Question #1 *Topic 1*

Which of the following are advantages of Network Intrusion Detection Systems (NIDS)?

A. B, C, and D

B. A, C, and E

C. B, D, and E

D. A, B, and C

E. Inexpensive to manage

Suggested Answer: *C*

ostorgaf 1 year, 5 months ago

Please update this question to:
Which of the following are advantages of Network Intrusion Detection Systems (NIDS)?
A. Analysis of encrypted traffic
B. Provide insight into network traffic
C. Detection of network operations problems
D. Provide logs of network traffic that can be used as part of other security measures.
E. Inexpensive to manage
A. B, C, and D
B. A, C, and E
C. B, D, and E
D. A, B, and C
Correct answer: C

upvoted 2 times

compgeek34 1 year, 8 months ago

I took the exam twice, and these questions were not even in the ball park for the GSEC

upvoted 2 times

shocdp 2 years, 7 months ago

This answer is missing some information.

upvoted 2 times

youngprinceton 2 years, 6 months ago

did you take exam yet? and how accurate are q from here

upvoted 1 times

Ron_Mistah 3 years, 9 months ago

was there missing on the given?

upvoted 3 times

Question #2 *Topic 1*

Which of the following protocols is used by a host that knows its own MAC (Media Access Control) address to query a server for its own IP address?

A. RARP

B. ARP

C. DNS

D. RDNS

Suggested Answer: *A*

compgeek34 1 year, 2 months ago

I took the exam twice, and these questions were not even in the ball park for the GSEC. A moderator may not show my coment here.

upvoted 1 times

arvkv 1 year, 4 months ago

The answer is A. RARP.

RARP (Reverse Address Resolution Protocol) is a protocol used by a host that knows its own MAC address to query a server for its own IP address. The RARP server maintains a table of MAC addresses and their corresponding IP addresses. When a host sends a RARP request, the RARP server responds with the host's IP address.

ARP (Address Resolution Protocol) is used by a host that knows its own IP address to query a server for the MAC address of a destination host. The ARP server maintains a table of IP addresses and their corresponding MAC addresses. When a host sends an ARP request, the ARP server responds with the destination host's MAC address.

DNS (Domain Name System) is used to translate domain names into IP addresses. It is not used to resolve MAC addresses to IP addresses.

RDNS (Reverse Domain Name System) is used to translate IP addresses into domain names. It is not used to resolve MAC addresses to IP addresses.

In conclusion, the RARP protocol is used by a host that knows its own MAC address to query a server for its own IP address.

upvoted 1 times

Question #3 *Topic 1*

What is the motivation behind SYN/FIN scanning?

A. The SYN/FIN combination is useful for signaling to certain Trojans.

B. SYN/FIN packets are commonly used to launch denial of service attacks against BSD hosts.

C. The crafted SYN/FIN packet sometimes gets past firewalls and filtering routers.

D. A SYN/FIN packet is used in session hijacking to take over a session.

Suggested Answer: *C*

Community vote distribution

C (100%)

Kuku55 Highly Voted 4 years, 1 month ago

Right answer is C.

upvoted 6 times

compgeek34 Most Recent 1 year, 2 months ago

I took the exam twice, and these questions were not even in the ballpark for the GSEC. A moderator may not show my comment here. These questions are ancient.

upvoted 3 times

arvkv 1 year, 4 months ago

A. The SYN/FIN combination is useful for signaling to certain Trojans. This is not correct, as the SYN/FIN combination is not generally used to communicate with Trojans.

B. SYN/FIN packets are commonly used to launch denial of service attacks against BSD hosts. This is not correct, SYN/FIN packets are not a common method for DoS attacks.

C. The crafted SYN/FIN packet sometimes gets past firewalls and filtering routers. This is correct. SYN/FIN scanning utilizes crafted packets with both the SYN and FIN flags set to bypass firewall rules.

D. A SYN/FIN packet is used in session hijacking to take over a session. This is not correct, session hijacking typically involves predicting TCP sequence numbers, not using SYN/FIN packets.

So the correct option is C.

upvoted 1 times

saucehozz 2 years, 10 months ago

Selected Answer: C

C senor

upvoted 3 times

director47 3 years, 2 months ago

C for this one

upvoted 4 times

Question #4 *Topic 1*

There is not universal agreement on the names of the layers in the TCP/IP networking model. Which of the following is one of the functions of the bottom layer which is sometimes called the Network Access or Link Layer?

A. Provides end-to-end data delivery service for user applications

B. Handles the routing of the data packets over the network

C. Manages IP addressing and encryption for data packets

D. Defines the procedures for interfacing with Ethernet devices

Suggested Answer: *D*

Praezin Highly Voted 2 years, 4 months ago

I would venture D

upvoted 5 times

compgeek34 Most Recent 1 year, 2 months ago

I took the exam twice, and these questions were not even in the ballpark for the GSEC. A moderator may not show my comment here. These questions are ancient.

upvoted 2 times

arvkv 1 year, 4 months ago

The TCP/IP model does not have universally agreed upon layer names, but the functions of each layer are well-defined.

Looking at the options:

A) End-to-end data delivery is a function of the Transport layer.

B) Routing of packets is a function of the Internet layer.

C) IP addressing and encryption happen at multiple layers, but are not specifically functions of the bottom layer.

D) Interfacing with actual physical network hardware like Ethernet is a function of the bottom Network Access or Link layer.

So the correct option is D

upvoted 1 times

Praezin 2 years, 4 months ago

Answer C

upvoted 1 times

Question #5 *Topic 1*

Which of the following is a private, RFC 1918 compliant IP address that would be assigned to a DHCP scope on a private LAN?

A. 127.0.0.100

B. 169.254.1.50

C. 10.254.1.50

D. 172.35.1.100

Suggested Answer: *C*

compgeek34 1 year, 2 months ago

I took the exam twice, and these questions were not even in the ballpark for the GSEC. A moderator may not show my comment here. These questions are ancient.

upvoted 3 times

arvkv 1 year, 4 months ago

Address ranges to be use by private networks are:

Class A: 10.0.0.0 to 10.255.255.255
Class B: 172.16.0.0 to 172.31.255.255
Class C: 192.168.0.0 to 192.168.255.255

All addresses outside these ranges are considered public.

A) 127.0.0.100 is in the 127.0.0.0/8 loopback range, which is used for loopback addresses and not assignable to physical interfaces.

B) 169.254.1.50 is in the 169.254.0.0/16 range used for link-local addresses, not RFC 1918 private addresses.

C) 10.254.1.50 is correct. 10.0.0.0/8 is a private RFC 1918 range commonly used for private LANs with DHCP.

D) 172.35.1.100 is not correct. This ip is outside of 172.16.0.0/12 range.

So the correct options is C.

upvoted 1 times

Ghost_0 3 years, 6 months ago

RFC1918 Subnets
The RFC1918 address space includes the following networks:
10.0.0.0 – 10.255.255.255 (10/8 prefix)
172.16.0.0 – 172.31.255.255 (172.16/12 prefix)
192.168.0.0 – 192.168.255.255 (192.168/16 prefix)

upvoted 2 times

Question #6 *Topic 1*

When using Pretty Good Privacy (PGP) to digitally sign a message, the signature is created in a two-step process. First, the message to be signed is submitted to
PGP's cryptographic hash algorithm. What is one of the hash algorithms used by PGP for this process?

A. Blowfish

B. DES

C. SHA-I

D. Cast

Suggested Answer: *C*

arvkv 1 year, 4 months ago

A) Blowfish - This is a symmetric encryption algorithm, not a hash.

B) DES - This is a symmetric encryption algorithm, not a hash.

C) SHA-1 - Correct. SHA-1 is a secure cryptographic hash algorithm used by PGP.

D) Cast - This is a symmetric encryption algorithm, not a commonly used hash.

Therefore, the correct option is C.

upvoted 2 times

Question #7 *Topic 1*

You are the security director for an off-shore banking site. From a business perspective, what is a major factor to consider before running your new vulnerability scanner against the company's business systems?

A. It may harm otherwise healthy systems.

B. It may produce false negative results.

C. It may generate false positive results.

D. It may not return enough benefit for the cost.

Suggested Answer: *C*

arvkv 1 year, 4 months ago

When deciding to run a vulnerability scanner against business systems, a major factor to consider from a business perspective is the potential for false positive results (option C).

False positives are results that incorrectly flag normal behavior as vulnerabilities. They can waste security team resources investigating issues that don't exist.

The other options are less of a concern:

A) Vulnerability scanners are designed not to harm systems when used properly.

B) False negatives (missing real vulnerabilities) are a security concern, but not as much of a business factor.

D) Cost/benefit is worth evaluating, but false positives directly reduce the scanner's benefit.

upvoted 1 times

Question #8 *Topic 1*

Which of the following is a benefit to utilizing Cygwin for Windows?

A. The ability to install a complete Red Hat operating system Install on Windows.

B. The ability to bring much more powerful scripting capabilities to Windows.

C. The ability to run a production Apache server.

D. The ability to install a complete Ubuntu operating system install on Windows.

Suggested Answer: *A*

Community vote distribution

B (100%)

urf 2 months, 1 week ago

Selected Answer: B

A key benefit of utilizing Cygwin for Windows is that it provides a Linux-like environment on Windows, allowing users to run Unix/Linux shell scripts and commands natively.

upvoted 1 times

arvkv 1 year, 4 months ago

The correct answer is: B. The ability to bring much more powerful scripting capabilities to Windows.

Cygwin is a collection of open-source tools that provides a Linux-like environment for Windows. It includes a large number of Unix utilities and libraries, as well as a Bash shell. This makes it possible to use powerful scripting languages like Perl, Python, and Ruby on Windows.

The other options are not correct:

Cygwin does not allow you to install a complete Red Hat or Ubuntu operating system on Windows.
While Cygwin can be used to run an Apache server, it is not typically used for production environments.

upvoted 2 times

MercyMe 2 years ago

Tricky. A and D are Linux based OS. Cygwin allows developers to migrate applications from Unix or Linux to Windows-based systems, making it easier to support their applications running on the Windows platform. I go with C.

upvoted 1 times

MercyMe 2 years ago

I mean B.

upvoted 1 times

youngprinceton 1 year, 11 months ago

did you take exam yet? and if no when do you take it and can you update if exam is exactly like exam topics

upvoted 1 times

RVR 2 years, 4 months ago

Shouldn't this be B?

upvoted 2 times

Question #9 *Topic 1*

What technical control provides the most critical layer of defense if an intruder is able to bypass all physical security controls and obtain tapes containing critical data?

A. Camera Recordings

B. Security guards

C. Encryption

D. Shredding

E. Corrective Controls

Suggested Answer: *C*

arvkv 1 year, 4 months ago

The correct answer is: C. Encryption

Encryption is the most critical layer of defense if an intruder is able to bypass all physical security controls and obtain tapes containing critical data. Encryption scrambles the data so that it is unreadable to anyone who does not have the encryption key. Even if an intruder is able to obtain the tapes, they will not be able to access the data without the key.

The other options are not as effective in protecting data from unauthorized access:

Camera recordings can be helpful in identifying and prosecuting intruders, but they cannot prevent them from accessing data.
Security guards can provide physical security, but they cannot prevent intruders from accessing data if they are able to bypass the physical security controls.
Shredding is an effective way to destroy data, but it is not possible to shred tapes after they have been stolen.
Corrective controls are actions taken to respond to and recover from a security incident. They are important, but they do not prevent the incident from happening in the first place.

upvoted 1 times

Question #10 *Topic 1*

Two clients connecting from the same public IP address (for example - behind the same NAT firewall) can connect simultaneously to the same web server on the
Internet, provided what condition is TRUE?

A. The server is not using a well-known port.

B. The server is on a different network.

C. The client-side source ports are different.

D. The clients are on different subnets.

Suggested Answer: *C*

arvkv 1 year, 4 months ago

The correct answer is: C. The client-side source ports are different.

When two clients connect to the same server from the same public IP address, the server needs to be able to distinguish between the two clients. This is done by using the client-side source port. The source port is a number that is randomly assigned to each outgoing connection. The server uses the source port to keep track of which client is sending which request.

The other options are not correct:

The server does not need to be using a well-known port. In fact, it is generally recommended to use non-well-known ports for security reasons.
The server does not need to be on a different network. The two clients and the server can all be on the same network.
The clients do not need to be on different subnets. The two clients can be on the same subnet.

upvoted 2 times

Question #11 *Topic 1*

Which of the following is a standard Unix command that would most likely be used to copy raw file system data for later forensic analysis?

A. dd

B. backup

C. cp

D. gzip

Suggested Answer: *A*

arvkv 1 year, 4 months ago

The correct answer is: A. dd

The dd command is a standard Unix command that can be used to copy raw file system data. It is often used for forensic analysis because it can create a bit-for-bit copy of the data, without making any modifications.

The other options are not as well-suited for forensic analysis:

The backup command is typically used to back up files and directories, not raw file system data.
The cp command can be used to copy files and directories, but it does not create a bit-for-bit copy of the data.
The gzip command is used to compress files, not copy them.

upvoted 1 times

exammer03 1 year, 7 months ago

dd, the disk/data duplicator (or, sometimes, disk destroyer) allows us to copy raw data from one source to another.

upvoted 1 times

Question #12 *Topic 1*

Which of the following is NOT a recommended best practice for securing Terminal Services and Remote Desktop?

A. Require TLS authentication and data encryption whenever possible.

B. Make sure to allow all TCP 3389 traffic through the external firewall.

C. Group Policy should be used to lock down the virtual desktops of thin-client users.

D. Consider using IPSec or a VPN in addition to the RDP encryption if you are concerned about future RDP vulnerabilities.

Suggested Answer: *B*

arvkv 1 year, 4 months ago

The correct answer is: B. Make sure to allow all TCP 3389 traffic through the external firewall.

Allowing all TCP 3389 traffic through the external firewall would make the Terminal Services and Remote Desktop environment more vulnerable to attack. Hackers could scan the internet for open RDP ports and then attempt to brute-force or exploit vulnerabilities in RDP to gain access to systems.

The other options are all recommended best practices for securing Terminal Services and Remote Desktop:

Requiring TLS authentication and data encryption helps to protect data from being intercepted and decrypted by attackers.
Using Group Policy to lock down the virtual desktops of thin-client users can help to prevent attackers from gaining access to systems, even if they are able to compromise the RDP connection.
Using IPSec or a VPN in addition to the RDP encryption can provide an extra layer of security and help to protect against future RDP vulnerabilities.

upvoted 1 times

Question #13 *Topic 1*

When an IIS filename extension is mapped, what does this mean?

A. Files with the mapped extensions cannot be interpreted by the web server.

B. The file and all the data from the browser's request are handed off to the mapped interpreter.

C. The files with the mapped extensions are interpreted by CMD.EXE.

D. The files with the mapped extensions are interpreted by the web browser.

Suggested Answer: *B*

Community vote distribution

B (100%)

newrose 9 months ago

Selected Answer: B

B is correct

upvoted 1 times

Question #14 *Topic 1*

Which Linux file lists every process that starts at boot time?

A. inetd

B. netsrv

C. initd

D. inittab

Suggested Answer: *D*

Community vote distribution

C (100%)

arvkv 1 year, 4 months ago

Answer: D (initiab) - When you boot the system or change run levels with the init or shutdown command, the init (init.d) daemon starts processes by reading information from the /etc/inittab file. This file defines three important items for the init process:

* The system's default run level
* What processes to start, monitor, and restart if they terminate
* What actions to take when the system enters a new run level

upvoted 1 times

RVR 2 years, 1 month ago

Selected Answer: C

INITD should be the answer

upvoted 1 times

T0m 2 years, 9 months ago

initd is the right answer

upvoted 2 times

Question #15 *Topic 1*

When trace route fails to get a timely response for a packet after three tries, which action will it take?

A. It will print '* * *' for the attempts and increase the maximum hop count by one.

B. It will exit gracefully, and indicate to the user that the destination is unreachable.

C. It will increase the timeout for the hop and resend the packets.

D. It will print '* * *' for the attempts, increment the TTL and try again until the maximum hop count.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

You are examining an IP packet with a header of 40 bytes in length and the value at byte 0 of the packet header is 6. Which of the following describes this packet?

A. This is an IPv4 packet; the protocol encapsulated in the payload is unspecified.

B. This is an IPv4 packet with a TCP payload.

C. This is an IPv6 packet; the protocol encapsulated in the payload is unspecified.

D. This is an IPv6 packet with a TCP payload.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Which of the following is a valid password for a system with the default "Password must meet complexity requirements" setting enabled as part of the GPO
Password policy requirements?

A. The Cat Chased its Tail All Night

B. disk ACCESS failed

C. SETI@HOME

D. SaNS2006

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

At what point in the Incident Handling process should an organization determine its approach to notifying law enforcement?

A. When performing analysis

B. When preparing policy

C. When recovering from the incident

D. When reacting to an incident

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Which of the following is TRUE regarding the ability of attackers to eavesdrop on wireless communications?

A. Eavesdropping attacks cannot be performed through concrete walls.

B. Eavesdropping attacks can take place from miles away.

C. Eavesdropping attacks are easily detected on wireless networks.

D. Eavesdropping attacks require expensive devices.

Suggested Answer: *B*

Praezin 1 year, 10 months ago

what kind of eaves dropping can be done from miles away?

upvoted 1 times

RVR 1 year, 7 months ago

Believe what it means is that eavesdropping attack, as a theft of information as it is transmitted over a unsecured network can be done from anywhere

upvoted 1 times

Question #20 *Topic 1*

An employee is currently logged into the corporate web server, without permission. You log into the web server as 'admin" and look for the employee's username:
"dmaul" using the "who" command. This is what you get back:

```
[user@localhost ~]$ who
admin :0 2010-09-11 06:49
dvader pts/3 2010-09-11 08:07 (localhost.localdomain)
hsolo pts/4 2010-09-11 08:14 (192.168.54.3)
cdooku pts/4 2010-09-11 08:14 (192.168.54.5)
```

A. The contents of the /var/log/messages file has been altered

B. The contents of the bash history file has been altered

C. The contents of the utmp file has been altered

D. The contents of the http logs have been altered

Suggested Answer: *B*

rincy Highly Voted 4 years ago

C is the correct answer, contents of utmp file is altered
upvoted 8 times

Question #21 *Topic 1*

What type of attack can be performed against a wireless network using the tool Kismet?

A. IP spoofing

B. Eavesdropping

C. Masquerading

D. Denial of Service

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which of the following is an Implementation of PKI?

A. SSL

B. 3DES

C. Kerberos

D. SHA-1

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Which of the following statements about policy is FALSE?

A. A well-written policy contains definitions relating to "what" to do.

B. A well-written policy states the specifics of "how" to do something.

C. Security policy establishes what must be done to protect information stored on computers.

D. Policy protects people who are trying to do the right thing.

Suggested Answer: *D*

E5_2699v4 Highly Voted 1 year, 7 months ago

Answer is B. See section policy vs procedure. Policy protects people that are trying to do the right thing and defines WHAT to do. Procedures define HOW to do it

upvoted 11 times

Question #24 *Topic 1*

You have reason to believe someone with a domain user account has been accessing and modifying sensitive spreadsheets on one of your application servers.
You decide to enable auditing for the files to see who is accessing and changing them. You enable the Audit Object Access policy on the files via Group Policy.
Two weeks later, when you check on the audit logs, you see they are empty. What is the most likely reason this has happened?

A. You cannot enable auditing on files, just folders

B. You did not enable auditing on the files

C. The person modifying the files turned off auditing

D. You did not save the change to the policy

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Which of the following BEST describes the two job functions of Microsoft Baseline Security Analyzer (MBSA)?

A. Vulnerability scanner and auditing tool

B. Auditing tool and alerting system

C. Configuration management and alerting system

D. Security patching and vulnerability scanner

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

How many bytes does it take to represent the hexadecimal value 0xFEDCBA?

A. 12

B. 2

C. 3

D. 6

Suggested Answer: *C*

Community vote distribution

C (100%)

JJAntoni 1 year ago

Selected Answer: C

The hexadecimal value
0xFEDCBA
0xFEDCBA represents a number in base 16. Each hexadecimal digit corresponds to 4 bits (half a byte). Let's calculate the number of bytes required to represent this value:

Count the number of hexadecimal digits in
0xFEDCBA
0xFEDCBA:
FEDCBA
FEDCBA has 6 hexadecimal digits.

Multiply the number of hexadecimal digits by 4 (to find the number of bits):
6
×
4
=
24
6×4=24 bits.

Convert bits to bytes (1 byte = 8 bits):
24
÷
8
=
3
24÷8=3 bytes.

Thus, it takes 3 bytes to represent
0xFEDCBA
0xFEDCBA.

upvoted 1 times

xzib 1 year, 7 months ago

The hexadecimal value 0xFEDCBA represents 32 bytes. Each hexadecimal character corresponds to 4 bits, and two hexadecimal characters together form a byte (8 bits) 1. So, 0xFEDCBA is equivalent to 32 bytes or 256 bits. The correct answer is D. 6.

upvoted 1 times

vilo24 2 years, 4 months ago

D, I think.

upvoted 1 times

Question #27 *Topic 1*

Which of the following choices accurately describes how PGP works when encrypting email?

A. PGP encrypts the message with the recipients public key, then encrypts this key with a random asymmetric key.

B. PGP creates a random asymmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key

C. PGP creates a random symmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key

D. PGP encrypts the message with the recipients public key, then encrypts this key with a random symmetric key.

Suggested Answer: *C*

Community vote distribution

C (100%)

Kushgod69420 Highly Voted 3 years, 1 month ago

Its C, Symmetric

upvoted 8 times

doggpark Most Recent 1 year, 2 months ago

Selected Answer: C

Symmetric then public key, why does it show as "B"?

upvoted 2 times

Qris 1 year, 9 months ago

Selected Answer: C

C, uses a symmetric encryption algorithm

upvoted 2 times

Jedisecure 2 years ago

It's C Symmetric

upvoted 4 times

Question #28 *Topic 1*

When designing wireless networks, one strategy to consider is implementing security mechanisms at all layers of the OSI model. Which of the following protection mechanisms would protect layer 1?

A. Hardening applications

B. Limit RF coverage

C. Employing firewalls

D. Enabling strong encryption

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

While building multiple virtual machines on a single host operating system, you have determined that each virtual machine needs to work on the network as a separate entity with its own unique IP address on the same logical subnet. You also need to limit each guest operating system to how much system resources it has access to. Which of the following correctly identifies steps that must be taken towards setting up these virtual environments?

A. The virtual machine software must define a separate virtual network Interface to each virtual machine and then define which unique logical hard drive partition should be available to the guest operating system.

B. The virtual machine software must define a separate virtual network interface since each system needs to have an IP address on the same logical subnet requiring they use the same physical interface on the host operating system.

C. The virtual machine software must define a separate virtual network interface to each virtual machine as well as how much RAM should be available to each virtual machine.

D. The virtual machine software establishes the existence of the guest operating systems and the physical system resources to be used by that system will be configured from within the guest operating system.

E. The virtual machine software must define a separate physical network interface to each virtual machine so that the guest operating systems can have unique

Suggested Answer: *E*

Kuku55 Highly Voted 1 year, 1 month ago

Correct answer is C

upvoted 8 times

Question #30 *Topic 1*

Which Windows event log would you look in if you wanted information about whether or not a specific diver was running at start up?

A. Application

B. System

C. Startup

D. Security

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

With regard to defense-in-depth, which of the following statements about network design principles is correct?

A. A secure network design requires that systems that have access to the Internet should not be accessible from the Internet and that systems accessible from the Internet should not have access to the Internet.

B. A secure network design requires that networks utilize VLAN (Virtual LAN) implementations to insure that private and semi-public systems are unable to reach each other without going through a firewall.

C. A secure network design will seek to provide an effective administrative structure by providing a single choke-point for the network from which all security controls and restrictions will be enforced.

D. A secure network design will seek to separate resources by providing a security boundary between systems that have different network security requirements.

Suggested Answer: *D*

arvkv 1 year, 3 months ago

The correct answer is: D. A secure network design will seek to separate resources by providing a security boundary between systems that have different network security requirements.

This is a fundamental principle of defence-in-depth, which is a security strategy that involves implementing multiple layers of security controls to protect a network. By separating systems with different security requirements, you can help to reduce the risk of a security breach spreading to other parts of the network.

upvoted 2 times

Question #32 *Topic 1*

Which of the following quantifies the effects of a potential disaster over a period of time?

A. Risk Assessment

B. Business Impact Analysis

C. Disaster Recovery Planning

D. Lessons Learned

Suggested Answer: *B*

arvkv 1 year, 3 months ago

The correct answer is: B. Business Impact Analysis

A business impact analysis (BIA) is a process that identifies and assesses the potential impacts of a disruption to a business's critical operations. It is used to develop a business continuity plan (BCP), which is a plan for how the business will recover from a disruption.

A BIA should quantify the effects of a potential disaster over a period of time, including the financial and non-financial impacts. This information can be used to prioritize the business's recovery efforts and to make informed decisions about investing in disaster prevention and mitigation measures.

Risk assessment and disaster recovery planning are also important parts of business continuity management, but they do not quantify the effects of a potential disaster over a period of time. Lessons learned are the insights that are gained from past disruptions, and they can be used to improve the business's preparedness for future disruptions.

upvoted 1 times

Question #33 *Topic 1*

Which of the following statements about Microsoft's VPN client software is FALSE?

A. The VPN interface can be figured into the route table.

B. The VPN interface has the same IP address as the interface to the network it's been specified to protect.

C. The VPN client software is built into the Windows operating system.

D. The VPN tunnel appears as simply another adapter.

Suggested Answer: *B*

arvkv 1 year, 3 months ago

The correct answer is: B. The VPN interface has the same IP address as the interface to the network it's been specified to protect.

A VPN interface is a virtual network interface that is created by the VPN client software. It is used to tunnel traffic over the public internet to a remote network. The VPN interface has its own IP address, which is assigned by the remote network.

The other answer choices are correct:

A. The VPN interface can be configured in the route table. This is necessary to ensure that traffic destined for the remote network is routed through the VPN tunnel.
C. The VPN client software is built into the Windows operating system. The VPN client software is included in all versions of Windows 10 and later.
D. The VPN tunnel appears as simply another adapter. The VPN interface is displayed in the Network Connections window, just like any other network adapter.

upvoted 1 times

Question #34 *Topic 1*

Which common firewall feature can be utilized to generate a forensic trail of evidence and to identify attack trends against your network?

A. NAT

B. State Table

C. Logging

D. Content filtering

Suggested Answer: *C*

arvkv 1 year, 3 months ago

The correct answer is: C. Logging

Firewall logging is a feature that records all traffic that passes through the firewall. This information can be used to generate a forensic trail of evidence in the event of a security breach. It can also be used to identify attack trends against your network.

The other answer choices are incorrect:

A. NAT: NAT (Network Address Translation) is a technique that allows multiple devices to share a single public IP address. It does not generate a forensic trail of evidence.
B. State Table: The state table is a table that the firewall uses to track the status of all active connections. It does not generate a forensic trail of evidence.
D. Content filtering: Content filtering is a feature that blocks access to certain types of websites or content. It does not generate a forensic trail of evidence.

upvoted 2 times

Question #35 *Topic 1*

Your organization has broken its network into several sections/segments, which are separated by firewalls, ACLs and VLANs. The purpose is to defend segments of the network from potential attacks that originate in a different segment or that attempt to spread across segments.
This style of defense-in-depth protection is best described as which of the following?

A. Uniform protection

B. Protected enclaves

C. Vector-oriented

D. Information-centric

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Which of the following systems acts as a NAT device when utilizing VMware in NAT mode?

A. Guest system

B. Local gateway

C. Host system

D. Virtual system

Suggested Answer: *D*

Kuku55 Highly Voted 5 years, 1 month ago

Correct answer is C.

upvoted 6 times

xzib Most Recent 1 year, 7 months ago

When using VMware in NAT mode, the host system acts as the NAT device. It translates the address of virtual machines to its own address before forwarding packets to the external network. Additionally, the NAT device serves as a DNS proxy for virtual machines, forwarding DNS requests to a DNS server known by the host system1. So, the correct answer is C. Host system.

upvoted 1 times

arvkv 2 years, 3 months ago

The correct answer is: C. Host system

In VMware NAT mode, the host system acts as a NAT device. This means that the host system translates the IP addresses of the virtual machines on its network to its own IP address before sending traffic to the internet. This allows the virtual machines to share the host system's internet connection without having their own public IP addresses.

The other answer choices are incorrect:

A. Guest system: The guest system is a virtual machine. Guest systems do not act as NAT devices.
B. Local gateway: The local gateway is the router that connects the host system's network to the internet. The local gateway does not act as a NAT device.
D. Virtual system: A virtual system is a virtual machine. Virtual systems do not act as NAT devices.

upvoted 1 times

Question #37 *Topic 1*

Your organization is developing a network protection plan. No single aspect of your network seems more important than any other. You decide to avoid separating your network into segments or categorizing the systems on the network. Each device on the network is essentially protected in the same manner as all other devices.
This style of defense-in-depth protection is best described as which of the following?

A. Uniform protection

B. Threat-oriented

C. Information-centric

D. Protected enclaves

Suggested Answer: *A*

arvkv 1 year, 3 months ago
The correct answer is: A. Uniform protection

Uniform protection is a security approach that provides the same level of protection to all information assets. This approach is based on the assumption that all information assets are equally valuable and that all threats are equally dangerous.
upvoted 1 times

Question #38 *Topic 1*

When a packet leaving the network undergoes Network Address Translation (NAT), which of the following is changed?

A. TCP Sequence Number

B. Source address

C. Destination port

D. Destination address

Suggested Answer: *B*

arvkv 1 year, 3 months ago

The correct answer is: B. Source address

Network Address Translation (NAT) is a technique that allows multiple devices on a local network to share a single public IP address. NAT works by translating the IP addresses of the devices on the local network to the public IP address before sending traffic to the internet.

When a packet leaving the network undergoes NAT, the source address is changed to the public IP address of the NAT device. This allows all of the devices on the local network to share the same public IP address, even though they have different private IP addresses.

upvoted 1 times

Question #39 *Topic 1*

Which of the following elements is the most important requirement to ensuring the success of a business continuity plan?

A. Disaster Recover Plans

B. Anticipating all relevant threats

C. Executive buy-in

D. Clearly defining roles and responsibilities

E. Training

Suggested Answer: *C*

arvkv 1 year, 3 months ago

The correct answer is: C. Executive buy-in

Executive buy-in is the most important requirement to ensuring the success of a business continuity plan. Without executive buy-in, a business continuity plan is unlikely to be implemented or funded effectively.

Executives need to understand the importance of business continuity and be willing to invest in developing and maintaining a plan. They also need to be willing to support the plan during a disruption.

The other answer choices are also important, but they are less important than executive buy-in. Disaster recovery plans, anticipating all relevant threats, clearly defining roles and responsibilities, and training are all essential parts of a business continuity plan. However, if executives do not support the plan, it is unlikely to be successful.

upvoted 1 times

Question #40 *Topic 1*

Which of the following TCP dump output lines indicates the first step in the TCP 3-way handshake?

A. 07:09:43.368615 download.net 39904 > ftp.com.21: S 733381829:733381829(0) win 8760 <mss 1460> (DF)

B. 07:09:43.370302 ftp.com.21 > download.net.39904: S 1192930639:1192930639(0} ack 733381830 win 1024 <mss 1460> (DF)

C. 09:09:22.346383 ftp.com.21 > download.net.39904: , rst 1 win 2440(DF)

D. 07:09:43.370355 download.net.39904 > ftp.com.21: , ack 1 win

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

Users at the Marketing department are receiving their new Windows XP Professional workstations. They will need to maintain local work files in the first logical volume, and will use a second volume for the information shared between the area group. Which is the best file system design for these workstations?

A. Both volumes should be converted to NTFS at install time.

B. First volume should be FAT32 and second volume should be NTFS.

C. First volume should be EFS and second volume should be FAT32.

D. Both volumes should be converted to FAT32 with NTFS DACLs.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

Which of the following is a new Windows Server 2008 feature for the Remote Desktop Protocol (RDP)?

A. The ability to allow the administrator to choose a port other than the default RDP port (TCP 3389)

B. The ability to support connections from mobile devices like smart phones

C. The ability to allow clients to authenticate over TLS

D. The ability to allow clients to execute individual applications rather than using a terminal desktop

Suggested Answer: *D*

arvkv 1 year, 3 months ago

The correct answer is: D. The ability to allow clients to execute individual applications rather than using a terminal desktop

This feature is called RemoteApp. RemoteApp allows you to publish individual applications to users, who can then run those applications on their own devices without having to connect to a full remote desktop session. This can be useful for applications that require access to specific resources on the server, such as a database or a file share.

The other answer choices are also features of Windows Server 2008, but they are not new features:

A. The ability to allow the administrator to choose a port other than the default RDP port (TCP 3389): This feature has been available since Windows Server 2003.
B. The ability to support connections from mobile devices like smart phones: This feature was added to Windows Server 2008 R2, not Windows Server 2008.
C. The ability to allow clients to authenticate over TLS: This feature has been available since Windows Server 2003.

upvoted 1 times

Question #43 *Topic 1*

What is TRUE about Workgroups and Domain Controllers?

A. By default all computers running Windows 2008 can only form Domain Controllers not Workgroups

B. Workgroups are characterized by higher costs while Domain Controllers by lower costs

C. You cannot have stand-alone computers in the midst of other machines that are members of a domain

D. Workgroup computers cannot share resources, only computers running on the same domain can

E. You can have stand-alone computers in the midst of other machines that are members of a domain.

Suggested Answer: *E*

arvkv 1 year, 3 months ago

The correct answer is: E. You can have stand-alone computers in the midst of other machines that are members of a domain.

The other answer choices are incorrect:

A. By default, all computers running Windows 2008 can be either workgroup members or domain controllers.
B. Workgroups are typically lower in cost than domains, as domains require the purchase and maintenance of a domain controller.
C. This is not true. You can have standalone computers in the midst of other machines that are members of a domain.
D. Workgroup computers can share resources with each other, but they cannot access resources on a domain without being granted permission by the domain administrator.

upvoted 1 times

Question #44 *Topic 1*

What file instructs programs like Web spiders NOT to search certain areas of a site?

A. Robots.txt

B. Restricted.txt

C. Spider.txt

D. Search.txt

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

Which of the following is a benefit of using John the Ripper for auditing passwords?

A. John's Blowfish cracking routine uses a complex central computing loop that increases the cost of each hash computation.

B. John the Ripper is much slower for auditing passwords encrypted with MD5 and Blowfish.

C. John's MD5 cracking routine uses a simplified central computing loop that decreases the cost of each hash computation.

D. John cannot use the DES bit-slicing technique, so it is much slower than other tools, especially when used against DES-encrypted passwords.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

Which of the following is an advantage of a Host Intrusion Detection System (HIDS) versus a Network Intrusion Detection System (NIDS)?

A. Ability to detect malicious traffic after it has been decrypted by the host

B. Ability to decrypt network traffic

C. Ability to listen to network traffic at the perimeter

D. Ability to detect malicious traffic before it has been decrypted

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

Which of the following is more commonly used for establishing high-speed backbones that interconnect smaller networks and can carry signals over significant distances?

A. Bluetooth

B. Ethernet

C. Token ring

D. Asynchronous Transfer Mode (ATM)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

The Linux command to make the /etc/shadow file, already owned by root, readable only by root is which of the following?

A. chmod 444/etc/shadow

B. chown root: root/etc/shadow

C. chmod 400/etc/shadow

D. chown 400 /etc/shadow

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

What is the main reason that DES is faster than RSA?

A. DES is less secure.

B. DES is implemented in hardware and RSA is implemented in software.

C. Asymmetric cryptography is generally much faster than symmetric.

D. Symmetric cryptography is generally much faster than asymmetric.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

Which of the following statements would be seen in a Disaster Recovery Plan?

A. "Instructions for notification of the media can be found in Appendix A"

B. "The Emergency Response Plan should be executed in the case of any physical disaster listed on page 3."

C. "The target for restoration of business operations is 72 hours from the declaration of disaster."

D. "After arriving at the alternate site, utilize the server build checklist to rebuild all servers on the server rebuild list."

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

Your software developer comes to you with an application that controls a user device. The application monitors its own behavior and that of the device and creates log files. The log files are expected to grow steadily and rapidly. Your developer currently has the log files stored in the /bin folder with the application binary.
Where would you suggest that the developer store the log files?

A. /var/log

B. /etc/log

C. /usr/log

D. /tmp/log

E. /dev/log

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

Which of the following is an advantage of private circuits versus VPNs?

A. Flexibility

B. Performance guarantees

C. Cost

D. Time required to implement

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 1*

What would the following IP tables command do?
IP tables -I INPUT -s 99.23.45.1/32 -j DROP

A. Drop all packets from the source address

B. Input all packers to the source address

C. Log all packets to or from the specified address

D. Drop all packets to the specified address

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

What would the file permission example "rwsr-sr-x" translate to in absolute mode?

A. 1755

B. 6755

C. 6645

D. 1644

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 1*

Which of the following Unix syslog message priorities is the MOST severe?

A. err

B. emerg

C. crit

D. alert

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

During a scheduled evacuation training session the following events took place in this order:
1. Evacuation process began by triggering the building fire alarm.
2a. The meeting point leader arrived first at the designated meeting point and immediately began making note of who was and was not accounted for.
2b. Stairwell and door monitors made it to their designated position to leave behind a box of flashlights and prop the stairway doors open with a garbage can so employees can find exits and dispose of food and beverages.
2c. Special needs assistants performed their assigned responsibility to help employees out that require special assistance.
3. The safety warden communicated with the meeting point leader via walkie talkie to collect a list of missing personnel and communicated this information back to the searchers.
4. Searchers began checking each room and placing stick-it notes on the bottom of searched doors to designate which areas were cleared.
5. All special need assistants and their designated wards exited the building.
6. Searchers complete their assigned search pattern and exit with the Stairwell/door monitors.
Given this sequence of events, which role is in violation of its expected evacuation tasks?

A. Safety warden

B. Stairwell and door monitors

C. Meeting point leader

D. Searchers

E. Special needs assistants

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

What type of malware is a self-contained program that has the ability to copy itself without parasitically infecting other host code?

A. Trojans

B. Boot infectors

C. Viruses

D. Worms

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

An IT security manager is trying to quickly assess the risks associated with not implementing a corporate firewall system. What sort of risk assessment is most appropriate?

A. Annualized Risk Assessment

B. Qualitative risk assessment

C. Quantitative risk assessment

D. Technical Risk Assessment

E. Iterative Risk Assessment

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

In a /24 subnet, which of the following is a valid broadcast address?

A. 200.11.11.1

B. 221.10.10.10

C. 245.20.30.254

D. 192.10.10.255

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

Which of the following applications would be BEST implemented with UDP instead of TCP?

A. A multicast streaming application.

B. A web browser.

C. A DNS zone transfer.

D. A file transfer application.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 1*

One of your Linux systems was compromised last night. According to change management history and a recent vulnerability scan, the system's patches were up- to-date at the time of the attack. Which of the following statements is the Most Likely explanation?

A. It was a zero-day exploit.

B. It was a Trojan Horse exploit.

C. It was a worm exploit.

D. It was a man-in-middle exploit.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 1*

A folder D:\Files\Marketing has the following NTFS permissions:
Administrators: Full Control
Marketing: Change and Authenticated
Users: Read
It has been shared on the server as "MARKETING", with the following share permissions:
Full Control share permissions for the Marketing group
Which of the following effective permissions apply if a user from the Sales group accesses the \\FILESERVER\MARKETING shared folder?

A. No access

B. Full Control

C. Read

D. Change

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #63 *Topic 1*

Which of the following fields CANNOT be hashed by Authentication Header (AH) in transport mode?

A. Length

B. Source IP

C. TTL

D. Destination IP

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

Which of the following is an advantage of an Intrusion Detection System?

A. It is a mature technology.

B. It is the best network security.

C. It never needs patching.

D. It is a firewall replacement.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

If Linux server software is a requirement in your production environment which of the following should you NOT utilize?

A. Debian

B. Mandrake

C. Cygwin

D. Red Hat

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

Which of the following statements best describes where a border router is normally placed?

A. Between your firewall and your internal network

B. Between your firewall and DNS server

C. Between your ISP and DNS server

D. Between your ISP and your external firewall

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 1*

When a host on a remote network performs a DNS lookup of www.google.com, which of the following is likely to provide an Authoritative reply?

A. The local DNS server

B. The top-level DNS server for .com

C. The DNS server for google.com

D. The root DNS server

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

You are reviewing a packet capture file from your network intrusion detection system. In the packet stream, you come across a long series of "no operation" (NOP) commands. In addition to the NOP commands, there appears to be a malicious payload. Of the following, which is the most appropriate preventative measure for this type of attack?

A. Limits on the number of failed logins

B. Boundary checks on program inputs

C. Controls against time of check/time of use attacks

D. Restrictions on file permissions

Suggested Answer: *C*

xzib 1 year, 7 months ago

answer is B. Boundary checks on program inputs . It is buffer owerflow

upvoted 1 times

Question #69 *Topic 1*

When should you create the initial database for a Linux file integrity checker?

A. Before a system is patched

B. After a system has been compromised

C. Before a system has been compromised

D. During an attack

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #70 *Topic 1*

Validating which vulnerabilities in a network environment are able to be exploited by an attacker is called what?

A. Anomaly detection

B. Vulnerability scanning

C. Perimeter assessment

D. Penetration testing

Suggested Answer: *B*

Community vote distribution

D (100%)

Hemingway Highly Voted 4 years, 7 months ago

This should be D. Testing a network's security controls to determine actual, exploitable vulnerabilities is called penetration testing.

upvoted 7 times

Genesis777 Highly Voted 3 years, 11 months ago

This should be B - Notice the wording of the question - "Validating" you don't validate vulnerabilities by penetration testing. That's for Vulnerability scanning. The purpose of penetration testing is to determine if the security posture of the targets involved is robust and can withstand exploit attacks, if vulnerabilities are found then you exploit the vulnerabilities.

upvoted 5 times

xzib Most Recent 1 year, 7 months ago

Selected Answer: D

A vulnerability scan only uncovers weaknesses in your system, but a penetration test discovers weaknesses and attempts to exploit them. Often, a penetration test costs more than a vulnerability scan. answ B

upvoted 1 times

Question #71 *Topic 1*

Which of the following statements would describe the term "incident" when used in the branch of security known as Incident Handling?

A. A and C

B. A, B, and C

C. B and C

D. A and B

Suggested Answer: *D*

Community vote distribution

D (100%)

mmoghal Highly Voted 3 years, 3 months ago

Where are the statements?

upvoted 5 times

FaisalAmer77 Most Recent 1 year, 1 month ago

Selected Answer: D

options A and B are correct. violates an organization's security policies. the purpose of incident handling is to minimize damage and restore services. Option C is incorrect because neither containment nor mitigation is sufficient without detection and classification.

upvoted 1 times

Question #72 *Topic 1*

Which of the following is the FIRST step in performing an Operational Security (OP5EC) Vulnerabilities Assessment?

A. Assess the threat

B. Assess vulnerabilities of critical information to the threat

C. Conduct risk versus benefit analysis

D. Implement appropriate countermeasures

E. Identification of critical information

Suggested Answer: *E*

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 1*

Which of the following SIP methods is used to setup a new session and add a caller?

A. ACK

B. BYE

C. REGISTER

D. INVITE

E. CANCEL

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

You are an Intrusion Detection Analyst and the system has alerted you to an Event of Interest (EOI) that appears to be activity generated by a worm. You investigate and find that the network traffic was normal. How would this type of alert be categorized?

A. False Positive

B. True Negative

C. True Positive

D. False Negative

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 1*

Which aspect of UNIX systems was process accounting originally developed for?

A. Data warehouse

B. Time sharing

C. Process tracking

D. Real time

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #76 *Topic 1*

IPS devices that are classified as "In-line NIDS" devices use a combination of anomaly analysis, signature-based rules, and what else to identify malicious events on the network?

A. Firewall compatibility rules

B. Application analysis

C. ICMP and UDP active scanning

D. MAC address filtering

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #77 *Topic 1*

What is the name of the registry key that is used to manage remote registry share permissions for the whole registry?

A. regkey

B. regmng

C. winreg

D. rrsreg

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #78 *Topic 1*

Which layer of the TCP/IP Protocol Stack Is responsible for port numbers?

A. Network

B. Transport

C. Internet

D. Application

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #79 *Topic 1*

How are differences in configuration settings handled between Domain and Local Group Policy Objects (GPOs)?

A. Local and Domain GPOs control different configuration settings, so there will not be conflicts.

B. Settings in the domain-wide GPO override conflicting settings in the local GPO on each computer.

C. Settings in the local GPO override conflicting settings when the domain-wide GPO is applied.

D. Precedence depends on which GPO was updated first.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 1*

An attacker gained physical access to an internal computer to access company proprietary data. The facility is protected by a fingerprint biometric system that records both failed and successful entry attempts. No failures were logged during the time periods of the recent breach. The account used when the attacker entered the facility shortly before each incident belongs to an employee who was out of the area. With respect to the biometric entry system, which of the following actions will help mitigate unauthorized physical access to the facility?

A. Try raising the Crossover Error Rate (CER)

B. Try to lower the False Accept Rate (FAR)

C. Try setting the Equal Error Rate (EER) to zero

D. Try to set a lower False Reject Rate (FRR)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #81 *Topic 1*

Which of the following is a type of countermeasure that can be deployed to ensure that a threat vector does not meet a vulnerability?

A. Prevention controls

B. Detection controls

C. Monitoring controls

D. Subversive controls

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #82 *Topic 1*

What is the main problem with relying solely on firewalls to protect your company's sensitive data?

A. Their value is limited unless a full-featured Intrusion Detection System is used.

B. Their value is limited because they cannot be changed once they are configured.

C. Their value is limited because operating systems are now automatically patched.

D. Their value is limited because they can be bypassed by technical and non-technical means.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #83 *Topic 1*

Which of the following features of Windows 7 allows an administrator to both passively review installed software and configure policies to prevent out-of-date or insecure software from running?

A. Direct Access

B. Software Restriction Policies

C. App Locker

D. User Account Control

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #84 *Topic 1*

What does an attacker need to consider when attempting an IP spoofing attack that relies on guessing Initial Sequence Numbers (ISNs)?

A. These attacks work against relatively idle servers.

B. These attacks rely on a modified TCP/IP stack to function.

C. These attacks can be easily traced back to the source.

D. These attacks only work against Linux/Unix hosts.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #85 *Topic 1*

In preparation to do a vulnerability scan against your company's systems. You've taken the steps below:
You've notified users that there will be a system test.
You've priontized and selected your targets and subnets.
You've configured the system to do a deep scan.
You have a member of your team on call to answer questions.
Which of the following is a necessary step to take prior to starting the scan?

A. Placing the incident response team on call.

B. Clear relevant system log files.

C. Getting permission to run the scan.

D. Scheduling the scan to run before OS updates.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #86 *Topic 1*

There are three key factors in selecting a biometric mechanism. What are they?

A. Reliability, encryption strength, and cost

B. Encryption strength, authorization method, and cost

C. Reliability, user acceptance, and cost

D. User acceptance, encryption strength, and cost

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #87 *Topic 1*

What is the following sequence of packets demonstrating?

A. telnet.com.telnet > client.com.38060: F 4289:4289(0) ack 92 win 1024

B. client.com.38060 > telnet.com.telnet: .ack 4290 win 8760 (DF)

C. client.com.38060 > telnet.com.telnet: F 92:92(0) ack 4290 win 8760 (DF)

D. telnet.com.telnet > client.com.38060: .ack 93 win 1024

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #88 *Topic 1*

Which of the following is a Layer 3 device that will typically drop directed broadcast traffic?

A. Hubs

B. Bridges

C. Routers

D. Switches

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #89 *Topic 1*

Which of the following would be a valid reason to use a Windows workgroup?

A. Lower initial cost

B. Simplicity of single sign-on

C. Centralized control

D. Consistent permissions and rights

Suggested Answer: *D*

eroms Highly Voted 1 year, 4 months ago

lower cost A

upvoted 12 times

Question #90 *Topic 1*

Which Defense-in-Depth model involves identifying various means by which threats can become manifest and providing security mechanisms to shut them down?

A. Vector-oriented

B. Uniform protection

C. Information centric defense

D. Protected enclaves

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #91 *Topic 1*

Included below is the output from a resource kit utility run against local host.

```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ====== ================ ============ ============
System Idle Process              0 Console                    0         28 K
System                           4 Console                    0        244 K
smss.exe                       648 Console                    0        420 K
csrss.exe                      960 Console                    0      5,252 K
winlogon.exe                  1000 Console                    0      7,576 K
```

Which command could have produced this output?

A. Schtasks

B. Task kill

C. SC

D. Task list

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #92 *Topic 1*

How is a Distributed Denial of Service (DDOS) attack distinguished from a regular DOS attack?

A. DDOS attacks are perpetrated by many distributed hosts.

B. DDOS affects many distributed targets.

C. Regular DOS focuses on a single router.

D. DDOS affects the entire Internet.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #93 *Topic 1*

Regarding the UDP header below, what is the length in bytes of the UDP datagrarn?
04 1a 00 a1 00 55 db 51

A. 161

B. 81

C. 219

D. 85

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #94 *Topic 1*

A sensor that uses a light beam and a detecting plate to alarm if the light beam is obstructed is most commonly used to identify which of the following threats?

A. Power

B. Smoke

C. Natural Gas

D. Water

E. Toxins

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #95 *Topic 1*

What protocol is a WAN technology?

A. 802.11

B. 802.3

C. Ethernet

D. Frame Relay

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #96 *Topic 1*

Which of the following is a characteristic of hash operations?

A. Asymmetric

B. Non-reversible

C. Symmetric

D. Variable length output

Suggested Answer: *D*

eroms Highly Voted 1 year, 4 months ago

Non-reversible

upvoted 13 times

Question #97 *Topic 1*

The TTL can be found in which protocol header?

A. It is found in byte 8 of the ICMP header.

B. It is found in byte 8 of the IP header.

C. It is found in byte 8 of the TCP header.

D. It is found in byte 8 of the DNS header.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #98 *Topic 1*

Which of the following is a required component for successful 802.lx network authentication?

A. Supplicant

B. 3rd-party Certificate Authority

C. Ticket Granting Server (TGS)

D. IPSec

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #99 *Topic 1*

What is the name of the command-line tool for Windows that can be used to manage audit policies on remote systems?

A. SECEDTT.EXE

B. POLCLI.EXE

C. REMOTEAUDIT.EXE

D. AUDITPOL.EXE

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #100 *Topic 1*

Many IIS servers connect to Microsoft SQL databases. Which of the following statements about SQL server security is TRUE?

A. SQL Server patches are part of the operating system patches.

B. SQL Server should be installed on the same box as your IIS web server when they communicate as part of the web application.

C. It is good practice to never use integrated Windows authentication for SQL Server.

D. It is good practice to not allow users to send raw SQL commands to the SQL Server.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #101 *Topic 1*

You have an automated system for patching the operating systems of all your computers. All patches are supposedly current. Yet your automated vulnerability scanner has just reported vulnerabilities that you believe have been patched. Which of the actions below should you take next?

A. Check some systems manually.

B. Rerun the system patching routines.

C. Contact the incident response team.

D. Ignore the findings as false positives.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #102 *Topic 1*

You are doing some analysis of malware on a Unix computer in a closed test network. The IP address of the computer is 192.168.1.120. From a packet capture, you see the malware is attempting to do a DNS query for a server called iamabadserver.com so that it can connect to it. There is no DNS server on the test network to do name resolution. You have another computer, whose IP is 192.168.1.115, available on the test network that you would like for the malware connect to it instead. How do you get the malware to connect to that computer on the test network?

A. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com

B. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.115 iamabadserveriamabadserver.com

C. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com

D. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.115 iamabadserver

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #103 *Topic 1*

What type of formal document would include the following statement?
Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal application of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies, and if there is any uncertainty, employees should consult their supervisor or manager.

A. Company privacy statement

B. Remote access policy

C. Acceptable use policy

D. Non-disclosure agreement

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #104 *Topic 1*

What is the command-line tool for Windows XP and later that allows administrators the ability to get or set configuration data for a very wide variety of computer and user account settings?

A. IPCONFIG.EXE

B. NETSTAT.EXE

C. WMIC.EXE

D. C0NF1G.EXE

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #105 *Topic 1*

A US case involving malicious code is brought to trial. An employee had opened a helpdesk ticket to report specific instances of strange behavior on her system.
The IT helpdesk representative collected information by interviewing the user and escalated the ticket to the system administrators. As the user had regulated and sensitive data on her computer, the system administrators had the hard drive sent to the company's forensic consultant for analysis and configured a new hard drive for the user. Based on the recommendations from the forensic consultant and the company's legal department, the CEO decided to prosecute the author of the malicious code. During the court case, which of the following would be able to provide direct evidence?

A. The IT helpdesk representative

B. The company CEO

C. The user of the infected system

D. The system administrator who removed the hard drive

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #106 *Topic 1*

When you log into your Windows desktop what information does your Security Access Token (SAT) contain?

A. The Security ID numbers (SIDs) of all the groups to which you belong

B. A list of cached authentications

C. A list of your domain privileges

D. The Security ID numbers (SIDs) of all authenticated local users

Suggested Answer: *A*

Community vote distribution

A (100%)

MapelCarrot Highly Voted 2 years, 5 months ago

Maybe A, see book 5 Security ID numbers?

upvoted 6 times

FaisalAmer77 Most Recent 1 year, 1 month ago

Selected Answer: A

The correct answer is A. The Security ID numbers (SIDs) of all the groups to which you belong.

A Security Access Token (SAT) is a data structure that contains information about a user's identity and privileges. It is created when a user logs in to a Windows system, and it is used to control access to resources on the system.

The SAT contains the following information:

The user's Security ID (SID)
The SIDs of all the groups to which the user belongs
The user's privileges
The SAT is used to determine whether a user has permission to access a particular resource. For example, when a user tries to open a file, the system checks the user's SAT to see if the user has permission to access the file.

The SAT is also used to control access to other resources, such as printers and network shares.

The SAT is a critical part of the Windows security system. It is used to ensure that only authorized users can access resources on the system.

upvoted 3 times

doggpark 1 year, 8 months ago

Access tokens contain the following information:
The security identifier (SID) for the user's account
SIDs for the groups of which the user is a member
A logon SID that identifies the current logon session
A list of the privileges held by either the user or the user's groups
An owner SID
The SID for the primary group
The default DACL that the system uses when the user creates a securable object without specifying a security descriptor
The source of the access token
Whether the token is a primary or impersonation token
An optional list of restricting SIDs
Current impersonation levels
Other statistics

upvoted 2 times

Question #107 *Topic 1*

Which type of risk assessment results are typically categorized as low, medium, or high-risk events?

A. Technical

B. Qualitative

C. Management

D. Quantitative

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #108 *Topic 1*

What is the first thing that should be done during the containment step of incident handling?

A. Change all the passwords

B. Secure the area

C. Prepare the Jump bag

D. Notify management

E. Prepare a report

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #109 *Topic 1*

Which choice best describes the line below?
alert tcp any any -> 192.168.1.0/24 80 (content: /cgi-bin/test.cgi"; msg: "Attempted CGI-BIN Access!!";)

A. Tcpdump filter

B. IP tables rule

C. Wire shark filter

D. Snort rule

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #110 *Topic 1*

Which class of IDS events occur when the IDS fails to alert on malicious data?

A. True Negative

B. True Positive

C. False Positive

D. False Negative

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #111 *Topic 1*

Which of the following tools is also capable of static packet filtering?

A. netstat.exe

B. ipsecpol.exe

C. ipconfig.exe

D. net.exe

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #112 *Topic 1*

Which of the following best describes the level of risk associated with using proprietary crypto algorithms.?

A. Proprietary cryptographic algorithms are required by law to use shorter key lengths in the United States, so the risk is high.

B. Proprietary algorithms have not been subjected to public scrutiny, so they have been checked less throughly for vulnerabilities.

C. Proprietary algorithms are less likely be vulnerable than algorithms that have been publicly disclosed because of enhanced secrecy of the algorithm.

D. Proprietary algorithms are not known to generally be any more or less vulnerable than publicly scrutinized algorithms.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #113 *Topic 1*

What is the discipline of establishing a known baseline and managing that condition known as?

A. Condition deployment

B. Observation discipline

C. Security establishment

D. Configuration management

Suggested Answer: *C*

eroms Highly Voted 3 years, 10 months ago

Configuration Management

upvoted 8 times

cool45 Most Recent 1 year, 4 months ago

it is D

upvoted 1 times

Genesis777 2 years, 5 months ago

In the defense in depth book, word for word, it has Configuration Management. How come this question is C?

upvoted 3 times

Question #114 *Topic 1*

What is the name of the Windows XP/2003 tool that you can use to schedule commands to be executed on remote systems during off-peak hours?

A. SCHTASKS.EXE

B. SCHEDULETSKS.EXE

C. SCHEDULR.EXE

D. SCHRUN.EXE

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #115 *Topic 1*

Your IT security team is responding to a denial of service attack against your server. They have taken measures to block offending IP addresses. Which type of threat control is this?

A. Detective

B. Preventive

C. Responsive

D. Corrective

Suggested Answer: *D*

usopp 1 year, 3 months ago

Is this B instead?

upvoted 1 times

Question #116 *Topic 1*

What is the unnoticed theft of sensitive data from a laptop owned by an organization's CEO an example of in information warfare?

A. Non-zero sum game

B. Win-win situation

C. Zero-sum game

D. Symmetric warfare

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #117 *Topic 1*

Who is responsible for deciding the appropriate classification level for data within an organization?

A. Data custodian

B. Security auditor

C. End user

D. Data owner

Suggested Answer: *B*

xzib 1 year, 7 months ago

answr. D

upvoted 2 times

Question #118 *Topic 1*

Which of the following protocols describes the operation of security In H.323?

A. H.239

B. H.245

C. H.235

D. H.225

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #119 *Topic 1*

If a DNS client wants to look up the IP address for good.news.com and does not receive an authoritative reply from its local DNS server, which name server is most likely to provide an authoritative reply?

A. The news.com domain name server

B. The .com (top-level) domain name server

C. The .(root-level) domain name server

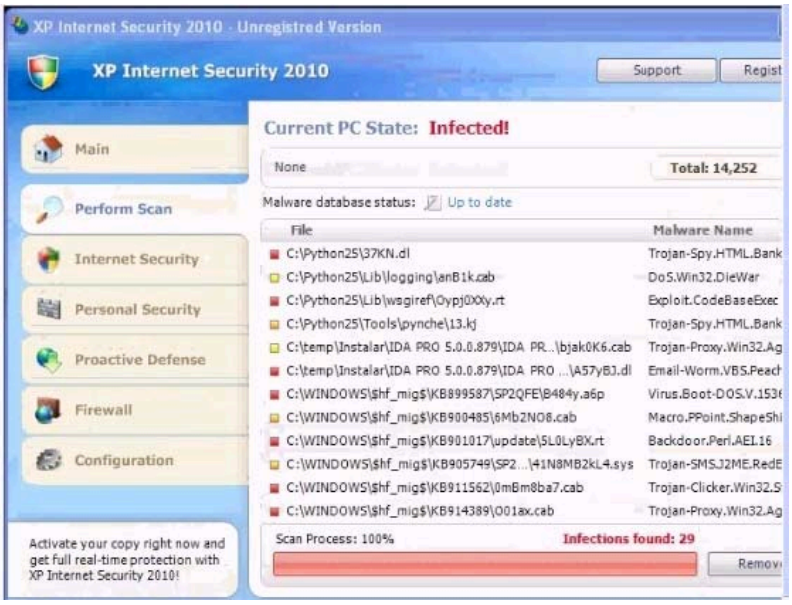
D. The .gov (top-level) domain name server

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #120 *Topic 1*

Analyze the screenshot below. What is the purpose of this message?



A. To gather non-specific vulnerability information

B. To get the user to download malicious software

C. To test the browser plugins for compatibility

D. To alert the user to infected software on the computer.

Suggested Answer: *B*

Community vote distribution

B (100%)

xzib 1 year, 7 months ago

Selected Answer: B

answr B

upvoted 2 times

elegantpete 2 years, 5 months ago

Selected Answer: B

it's classic fake infection notification, convincing the victim to download malware disguised as AV, it's B.

upvoted 1 times

Question #121 *Topic 1*

Why would someone use port 80 for deployment of unauthorized services?

A. Google will detect the service listing on port 80 and post a link, so that people all over the world will surf to the rogue service.

B. If someone were to randomly browse to the rogue port 80 service they could be compromised.

C. This is a technique commonly used to perform a denial of service on the local web server.

D. HTTP traffic is usually allowed outbound to port 80 through the firewall in most environments.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #122 *Topic 1*

Which of the below choices should an organization start with when implementing an effective risk management process?

A. Implement an incident response plan

B. Define security policy requirements

C. Conduct periodic reviews

D. Design controls and develop standards for each technology you plan to deploy

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #123 *Topic 1*

In trace route results, what is the significance of an * result?

A. A listening port was identified.

B. A reply was returned in less than a second.

C. The target host was successfully reached.

D. No reply was received for a particular hop.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #124 *Topic 1*

You have set up a local area network for your company. Your firewall separates your network into several sections: a DMZ with semi-public servers (web, dns, email) and an intranet with private servers. A penetration tester gains access to both sections and installs sniffers in each. He is able to capture network traffic for all the devices in the private section but only for one device (the device with the sniffer) in the DMZ. What can be inferred about the design of the system?

A. You installed a router in the private section and a switch in the DMZ

B. You installed a hub in the private section and a switch in the DMZ

C. You installed a switch in the private section and a hub in the DMZ

D. You installed a switch in the private section and a router in the DMZ

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #125 *Topic 1*

The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?
STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.
STEP 2 - Do a binary backup if data is being collected.
STEP 3 - Deliver collected evidence to law enforcement officials.

A. Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic bag.

B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody.

C. Take photographs of all persons who have had access to the computer.

D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #126 *Topic 1*

Which Defense-in-Depth principle starts with an awareness of the value of each section of information within an organization?

A. Information centric defense

B. Uniform information protection

C. General information protection

D. Perimeter layering

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #127 *Topic 1*

Which of the following Linux commands can change both the username and group name a file belongs to?

A. chown

B. chgrp

C. chmod

D. newgrp

Suggested Answer: *B*

eroms Highly Voted 1 year, 4 months ago

A. Chown

upvoted 7 times

Question #128 *Topic 1*

Which of the following is a backup strategy?

A. Differential

B. Integrational

C. Recursive

D. Supplemental

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #129 *Topic 1*

The Return on Investment (ROI) measurement used in Information Technology and Information Security fields is typically calculated with which formula?

A. ROI = (gain - expenditure)/(expenditure) X 100%

B. ROI = (gain + expenditure)/(expenditure) X 100%

C. ROI = (loss + expenditure)/(expenditure) X 100%

D. ROI = (loss - expenditure)/(expenditure) X 100%

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #130 *Topic 1*

What database can provide contact information for Internet domains?

A. dig

B. who

C. who is

D. ns look up

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #131 *Topic 1*

During which of the following steps is the public/private key-pair generated for Public Key Infrastructure (PKI)?

A. Key Recovery

B. Initialization

C. Registration

D. Certification

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #132 *Topic 1*

What is the process of simultaneously installing an operating system and a Service Pack called?

A. Synchronous Update

B. Slipstreaming

C. Simultaneous Update

D. Synchronizing

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #133 *Topic 1*

Which of the following is an UDP based protocol?

A. telnet

B. SNMP

C. IMAP

D. LDAP

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #134 *Topic 1*

What is the function of the TTL (Time to Live) field in IPv4 and the Hop Limit field in IPv6 In an IP Packet header?

A. These fields are decremented each time a packet is retransmitted to minimize the possibility of routing loops.

B. These fields are initialized to an initial value to prevent packet fragmentation and fragmentation attacks.

C. These fields are recalculated based on the required time for a packet to arrive at its destination.

D. These fields are incremented each time a packet is transmitted to indicate the number of routers that an IP packet has traversed.

Suggested Answer: *A*

username8527 1 year, 3 months ago

A is the correct answer. TTL is decremented and not incremented.

upvoted 2 times

eroms 3 years, 10 months ago

D. These fields are incremented each time a packet is transmitted to indicate the number of routers that an IP packet has traversed.

upvoted 2 times

Kuku55 3 years, 7 months ago

A is right. Its Time to Live

upvoted 7 times

Question #135 *Topic 1*

When discussing access controls, which of the following terms describes the process of determining the activities or functions that an Individual is permitted to perform?

A. Authentication

B. Identification

C. Authorization

D. Validation

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #136 *Topic 1*

Which command would allow an administrator to determine if a RPM package was already installed?

A. rpm -s

B. rpm -q

C. rpm -a

D. rpm -t

Suggested Answer: *B*

tifgif 1 year, 5 months ago

def rpm -a

from the RPM man page

-a, --all

Query all installed packages.

upvoted 1 times

Question #137 *Topic 1*

A new data center is being built where customer credit information will be processed and stored. Which of the following actions will help maintain the confidentiality of the data?

A. Environmental sensors in the server room

B. Access control system for physical building

C. Automated fire detection and control systems

D. Frequent off-site backup of critical databases

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #138 *Topic 1*

In order to capture traffic for analysis, Network Intrusion Detection Systems (NIDS) operate with network cards in what mode?

A. Discrete

B. Reporting

C. Promiscuous

D. Alert

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #139 *Topic 1*

A Host-based Intrusion Prevention System (HIPS) software vendor records how the Firefox Web browser interacts with the operating system and other applications, and identifies all areas of Firefox functionality. After collecting all the data about how Firefox should work, a database is created with this information, and it is fed into the HIPS software. The HIPS then monitors Firefox whenever it's in use. What feature of HIPS is being described in this scenario?

A. Signature Matching

B. Application Behavior Monitoring

C. Host Based Sniffing

D. Application Action Modeling

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!