

EXAM 312-50 TOPIC 2 QUESTION 11 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 11

Topic #: 2

[\[All 312-50 Questions\]](#)

When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

- A. Vulnerability scanning
- B. Social engineering **Most Voted**
- C. Application security testing
- D. Network sniffing

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [lau2123](#) at Feb. 21, 2023, 10:28 a.m.

Comments

  [greeklover84](#) 11 months, 3 weeks ago

Selected Answer: B

I suggest B
upvoted 1 times

  [lau2123](#) 2 years, 3 months ago

By conducting a social engineering test, an organization can assess the level of awareness and knowledge of employees with regard to security best practices, and identify areas where additional training may be needed.

Vulnerability scanning, application security testing, and network sniffing are all technical assessment methods that focus on identifying vulnerabilities in systems and networks, and do not directly measure the effectiveness of end-user security training. While these techniques are important for overall network security, they do not provide insight into the human factor of security. Therefore, social engineering is the most effective technique for assessing the effectiveness of end-user security training.

upvoted 4 times

EXAM 312-50 TOPIC 3 QUESTION 46 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 46

Topic #: 3

[\[All 312-50 Questions\]](#)

Which of the following business challenges could be solved by using a vulnerability scanner?

- A. Auditors want to discover if all systems are following a standard naming convention.
- B. A web server was compromised and management needs to know if any further systems were compromised.
- C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.
- D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

[Hide Answer](#)

Suggested Answer: D

by  **Hyrcane** at March 10, 2023, 12:11 p.m.

Comments

  **tlssy** 1 year ago

Its D, Makes more sense
upvoted 1 times

  **Hyrcane** 1 year, 2 months ago

B, come on
upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 31 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 31

Topic #: 1

[All 312-50v12 Questions]

John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to one of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation.

What is the type of vulnerability assessment tool employed by John in the above scenario?

A. Agent-based scanner Most Voted

B. Network-based scanner

C. Cluster scanner

D. Proxy scanner

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (66%)

B (34%)

by  eli117 at April 4, 2023, 3:46 p.m.

Comments

 **jeremy13** Highly Voted 2 years, 7 months ago

Selected Answer: A

A. Agent-based scanner

Module 05/P561 CEH bookV12

*Network-Based Scanner: Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.

*Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.

*Proxy Scanner: Proxy scanners are the network-based scanners that can scan networks from any machine on the network.

* Cluster scanner: Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network.

upvoted 23 times

 **eli117** Highly Voted 2 years, 7 months ago

Selected Answer: B

B. Network-based scanner

Explanation: In the given scenario, John employs a network-based scanner to identify vulnerabilities on the machines in the same network. A network-based scanner is a type of vulnerability assessment tool that scans the network for vulnerabilities and identifies security holes in the network devices and systems. It is a non-intrusive scanner that can detect vulnerabilities without accessing the system. It sends packets to the network and analyzes the response to identify vulnerabilities.

upvoted 6 times

 **best2000** 2 years, 7 months ago

you would have been right if the was no installing. the question said the scanner was installed on a machine. the right answer is A

upvoted 5 times

 **RobertVidal** Most Recent 10 months ago

Selected Answer: A

I think that it is answer A, because it says that the attacker installs the scanner on a single machine to scan other machines on the same network.
upvoted 2 times

👤 **Mann098** 11 months ago

Selected Answer: A

Agent-based scanner

upvoted 1 times

👤 **ametah** 1 year, 5 months ago

Selected Answer: A

Listed below are some of the location and data examination tools:

- o Network-Based Scanner: Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.
- o Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.
- o Proxy Scanner: Proxy scanners are the network-based scanners that can scan networks from any machine on the network.
- o Cluster scanner: Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network

upvoted 1 times

👤 **zarrzz** 1 year, 5 months ago

Selected Answer: B

The most appropriate choice is: B. Network-based scanner.

Explanation:

Agent-based scanner: This typically involves installing software agents on each target machine to perform vulnerability assessments. It doesn't fit the scenario where a scanner is installed on one machine and used to scan others.

Network-based scanner: This is a scanner that examines network traffic or directly probes other machines on the network to identify vulnerabilities. It matches the scenario where a scanner was installed on a machine and used to scan other machines on the same network.

Cluster scanner: This is less commonly referred to in the context of vulnerability assessment tools and usually pertains to managing and scanning clusters of machines, but not in the specific way described.

Proxy scanner: This typically involves using a proxy to scan web traffic, and is not relevant to the scenario described.

upvoted 4 times

👤 **zarrzz** 1 year, 5 months ago

The most appropriate choice is: B. Network-based scanner.

Explanation:

Agent-based scanner: This typically involves installing software agents on each target machine to perform vulnerability assessments. It doesn't fit the scenario where a scanner is installed on one machine and used to scan others.

Network-based scanner: This is a scanner that examines network traffic or directly probes other machines on the network to identify vulnerabilities. It matches the scenario where a scanner was installed on a machine and used to scan other machines on the same network.

Cluster scanner: This is less commonly referred to in the context of vulnerability assessment tools and usually pertains to managing and scanning clusters of machines, but not in the specific way described.

Proxy scanner: This typically involves using a proxy to scan web traffic, and is not relevant to the scenario described.

upvoted 2 times

👤 **Lost_Memo** 1 year, 6 months ago

Selected Answer: B

I Believe the answer is B as I understand how you are using the key word install, to run an agent-based scan all the machines involved need have the agent installed on them to do the scan, while network scan requires connectivity, and this scenario I do not think the attacker has access to any other device to install the agents.

upvoted 2 times

👤 **desertlotus1211** 1 year, 7 months ago

Though the scanner software was installed on a victim's machine... Actually a network-based scanner is being performed to identify vulnerabilities on the network and on the other machines.

Agent-based scanner would be installed on a machine BUT will send information about THAT machine to a central repo. This is not happening in this scenario.

upvoted 1 times

👤 **desertlotus1211** 1 year, 7 months ago

Agent-based scanning is a type of vulnerability scanning that involves installing a software agent on each system that needs to be scanned. The agent then monitors and reports on the system's status, enabling real-time data collection and analysis.

upvoted 2 times

👤 **jettguo** 1 year, 8 months ago

Selected Answer: B

My answer is network-based scanner.

Reason 1: although an "agent" is installed on a victim machine, there is no mention of using this scanner to scan for vulnerabilities on this victim machine.

Reason 2:

The "agent" was used to scan on machines within the network, this fits the signature of a "network-based scanner"

upvoted 1 times

✉  **sh4dali** 1 year, 8 months ago

Selected Answer: A

A. Agent based.

"installed a scanner on a machine" keyword is on a machine.

upvoted 1 times

✉  **barey** 1 year, 9 months ago

GPT4:

B. Network-based scanner

In the scenario described, the professional hacker is using a network-based scanner. This type of scanner is deployed on a network and scans multiple machines on that network to identify potential vulnerabilities without being installed on each individual machine. Network-based scanners are commonly used to assess security posture and identify vulnerabilities that could be exploited.

upvoted 1 times

✉  **yasso2023** 1 year, 10 months ago

Selected Answer: A

In the scenario described, where the hacker installed a scanner on a machine within the victim's network and scanned several machines on the same network, it aligns more closely with an Agent-Based Scanner. Agent-based scanners reside on a single machine but can scan several machines on the same network.

upvoted 1 times

✉  **yasso2023** 1 year, 10 months ago

In the scenario described, where the hacker installed a scanner on a machine within the victim's network and scanned several machines on the same network, it aligns more closely with an Agent-Based Scanner. Agent-based scanners reside on a single machine but can scan several machines on the same network.

upvoted 1 times

✉  **HetBeest** 1 year, 11 months ago

None-of-the-above would have been my answer. John didn't employ anything (himself).

upvoted 1 times

✉  **4MM449** 1 year, 11 months ago

Selected Answer: A

A. Agent-based scanner

upvoted 1 times

✉  **insaniunt** 2 years ago

Selected Answer: A

page 561 from CEH v12 book:

Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.

A. Agent-Based Scanner

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 101 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 101

Topic #: 1

[All 312-50v12 Questions]

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

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  eli117 at April 5, 2023, 1:26 p.m.

Comments

  **eli117**  2 years, 7 months ago

D. Bryan's public key; Alice's public key

Explanation:

Alice needs to send a confidential document to Bryan, and their company has public key infrastructure set up. In this scenario, Alice needs to encrypt the message using Bryan's public key, which ensures only Bryan can decrypt it using his private key. To ensure the authenticity of the message, Alice must digitally sign it using her private key, which can be verified by anyone who has access to Alice's public key, including Bryan. Therefore, Bryan uses Alice's public key to confirm the digital signature.

upvoted 5 times

  **a307962**  1 year, 4 months ago

Selected Answer: D

D. Bryan's public key; Alice's public key

upvoted 1 times

  **insaniunt** 1 year, 11 months ago

Selected Answer: D

D. Bryan's public key; Alice's public key

upvoted 1 times

  **Vincent_Lu** 2 years, 5 months ago

Selected Answer: D

D. Bryan's public key; Alice's public key

upvoted 1 times

  **victorfs** 2 years, 6 months ago

Selected Answer: D

D. Bryan's public key; Alice's public key

upvoted 1 times

  **eli117** 2 years, 7 months ago

Selected Answer: D

D. Bryan's public key; Alice's public key

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 111 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 111

Topic #: 1

[All 312-50v12 Questions]

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 Most Voted
- C. Elicitation
- D. Phishing

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (66%) C (34%)

by  eli117 at April 5, 2023, 1:44 p.m.

Comments

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

Selected Answer: C

A. Diversion theft: A technique involving distraction to commit theft or stealing.

B. Quid pro quo: An exchange where one party provides value in return for a benefit.

C. Elicitation: Gathering information through skilled questioning or social engineering.

D. Phishing: Fraudulent technique using deception to obtain sensitive information.

upvoted 11 times

 **fortinetmaster** Highly Voted 2 years, 7 months ago

Selected Answer: B

Correct B: Quid pro quo

CEH Book v12 Page 1341

Attackers call numerous random numbers within a company, claiming to be from technical support.

They offer their service to end users in exchange for confidential data or login credentials

upvoted 8 times

 **Carl.Chang** Most Recent 1 year ago

The social engineering technique employed by Johnson in the scenario you described is more aligned with ***Quid pro quo.***

In this context, the attacker pretends to be from a legitimate source (a technical support team) and offers a service (warning about an impending server compromise) in exchange for the victim taking specific actions (executing unusual commands and installing malicious files). This technique often involves an exchange where the attacker provides a benefit or service to the victim, who in turn provides sensitive information or access.

While "Elicitation" refers to techniques used to gather information without the victim realizing it, in this case, the direct exchange and manipulation for a specific action suggest that Quid pro quo is a better fit.

upvoted 2 times

 **Binx** 1 year, 3 months ago

B. Quid pro quo

In this scenario, Johnson pretends to be from a technical support team and warns the target about a supposed threat. He then instructs the target

to execute certain commands and install malicious files, offering the supposed benefit of preventing a server compromise. This exchange of providing help in return for the execution of malicious instructions is characteristic of quid pro quo in social engineering.

upvoted 1 times

✉  **ametah** 1 year, 5 months ago

Selected Answer: B

Quid Pro Quo Quid pro quo is a Latin phrase that means "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.

CEHv12 Module 09 Social Engineering Page 1348

upvoted 1 times

✉  **insaniunt** 1 year, 11 months ago

Selected Answer: B

B. Quid pro quo

upvoted 1 times

✉  **helloworlds** 2 years ago

Selected Answer: B

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

upvoted 1 times

✉  **IPconfig** 2 years, 1 month ago

Selected Answer: B

Quid Pro Quo

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 2 times

✉  **Attila777** 2 years, 1 month ago

definitely C.

elicitation: In requirements engineering, requirements elicitation is the practice of researching and discovering the requirements of a system from users, customers, and other stakeholders. The practice is also sometimes referred to as "requirement gathering".

upvoted 2 times

✉  **victorfs** 2 years, 6 months ago

Selected Answer: C

The correct option is C.

Elicitacion.

Steve uses persuasion and manipulation to extract sensitive information from the victim.

Where is the Quid pro quo? The victim don't get nothing!

upvoted 1 times

✉  **Tafulu** 2 years, 3 months ago

I believe the quid pro quo here is hey your server is going to die, I'm technical support and will help you prevent this. I just need you to download these files and update the system so that I can fix it.

upvoted 2 times

✉  **mikelpal** 1 year, 5 months ago

**Answer is B. "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."

upvoted 1 times

✉  **jeremy13** 2 years, 6 months ago

Selected Answer: B

same page as fortinetmaster => yeah we have the same book ;-)

upvoted 2 times

✉  **sausageman** 2 years, 7 months ago

Selected Answer: B

B. Quid pro quo

CEH Book v12 Module 09 Page 905

"Quid pro quo is a Latin phrase that means "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."

upvoted 4 times

✉  **eli117** 2 years, 7 months ago

Selected Answer: B

B. Quid pro quo. In this technique, the attacker offers something of value, in this case, a warning about a compromised server, in exchange for access or information. In this case, Johnson offered to help the victim prevent an attack in progress, but in reality, he was using the opportunity to install malware and steal sensitive information.

upvoted 4 times

EXAM 312-50V12 TOPIC 1 QUESTION 112 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 112

Topic #: 1

[All 312-50v12 Questions]

An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks.

Which of the following security scanners will help John perform the above task?

A. AlienVault® OSSIMTM

B. Syhunt Hybrid **Most Voted**

C. Saleae Logic Analyzer

D. Cisco ASA

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  eli117 at April 5, 2023, 1:45 p.m.

Comments

 **Vincent_Lu** **Highly Voted** 1 year, 11 months ago

Selected Answer: B

- A. AlienVault OSSIMTM: An open-source SIEM platform for security event and log data.
- B. Syhunt Hybrid: Web app security testing tool for finding vulnerabilities.
- C. Saleae Logic Analyzer: Hardware device for digital signal analysis.
- D. Cisco ASA: Network security device with firewall, VPN, and IPS features.

upvoted 5 times

 **insaniunt** **Most Recent** 1 year, 5 months ago

Selected Answer: B

- B. Syhunt Hybrid

upvoted 1 times

 **jeremy13** 2 years ago

Selected Answer: B

- B. Syhunt Hybrid
- Like Q380 V11
- CEH Book V12 Module 13 P1860

B. Syhunt Hybrid
from book :

The Syhunt Hybrid scanner automates web application security testing and guards the organization's web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory traversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Syhunt Hybrid creates signatures to detect application vulnerabilities and prevents logout. It analyzes JavaScript (JS), logs suspicious responses, and tests errors for review.

Figure

upvoted 2 times

 **eli117** 2 years, 1 month ago

Selected Answer: B

Syhunt Hybrid is a web application scanner that is specifically designed to detect and prevent web-application and web-server attacks. It can automatically test web applications for common vulnerabilities, including XSS, directory traversal, fault injection, SQL injection, command injection, and others. AlienVault® OSSIMTM is a unified security management platform that includes intrusion detection, asset management, vulnerability

assessment, and other security features, but it does not have a web application scanner. Saleae Logic Analyzer is a hardware tool used for analyzing digital signals, and Cisco ASA is a security appliance used for firewall, VPN, and intrusion prevention.

upvoted 2 times

EXAM 312-50 TOPIC 3 QUESTION 18 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 18

Topic #: 3

[\[All 312-50 Questions\]](#)

Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

- A. Microsoft Security Baseline Analyzer
- B. Retina
- C. Core Impact
- D. Microsoft Baseline Security Analyzer

[Hide Answer](#)

Suggested Answer: D

by  M4inB3nnY at April 19, 2023, 1:54 a.m.

Comments

  **NikoTomas** 1 year, 2 months ago

Okay, but just for info, MBSA is obsolete:

"MBSA was largely used in situations where Microsoft Update a local WSUS or Configuration Manager server wasn't available, or as a compliance tool to ensure that all security updates were deployed to a managed environment. While MBSA version 2.3 introduced support for Windows Server 2012 R2 and Windows 8.1, it has since been deprecated and no longer developed. MBSA 2.3 isn't updated to fully support Windows 10 and Windows Server 2016."

<https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/mbsa-removal-and-guidance>

upvoted 1 times

  **M4inB3nnY** 2 years, 1 month ago

the answer correct is D, MBSA.

<https://www.microsoft.com/en-us/security/blog/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/>

upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 51 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 51

Topic #: 3

[\[All 312-50 Questions\]](#)

An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

- A. Classified
- B. Overt
- C. Encrypted
- D. Covert Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  Novmejst at April 22, 2023, 5:14 p.m.

Comments

  **Novmejst** 1 year, 1 month ago

Selected Answer: D

The term "covert" generally refers to something that is concealed, hidden, or not easily detected or recognized. In the context of cybersecurity, covert techniques can refer to methods used by attackers to evade detection or hide their activities, such as using stealthy malware or encrypting their communication channels.

upvoted 1 times

EXAM 312-50 TOPIC 5 QUESTION 31 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 31

Topic #: 5

[\[All 312-50 Questions\]](#)

Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

- A. RSA 1024 bit strength
- B. AES 1024 bit strength
- C. RSA 512 bit strength
- D. AES 512 bit strength

[Hide Answer](#)

Suggested Answer: A

by  Novmejst at April 22, 2023, 10:15 p.m.

Comments

  **Novmejst** 1 year, 1 month ago

None of the listed options is correct.

Public Key Infrastructure (PKI) uses cryptographic algorithms at multiple levels to provide secure communication and trust among parties. At the core of PKI is the use of public key algorithms, also known as asymmetric cryptography, which use a pair of keys, a public key and a private key, for encryption and decryption.

Therefore, the correct answer is: PKI uses public key algorithms such as RSA (with key sizes of at least 2048-bit strength or higher), hash functions, and symmetric key algorithms such as AES (with key sizes of 128 bits or higher).

upvoted 1 times

EXAM 312-50 TOPIC 5 QUESTION 35 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 35

Topic #: 5

[\[All 312-50 Questions\]](#)

Which statement best describes a server type under an N-tier architecture?

- A. A group of servers at a specific layer
- B. A single server with a specific role
- C. A group of servers with a unique role Most Voted**
- D. A single server at a specific layer

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (100%)

by  [Novmejst](#) at April 22, 2023, 10:23 p.m.

Comments

  [Novmejst](#) 1 year, 1 month ago

Selected Answer: C

C. A group of servers with a unique role best describes a server type under an N-tier architecture. In an N-tier architecture, multiple servers can be used to perform a specific set of tasks or roles, and these servers are typically grouped together based on their function or responsibility in the application. Each server in the group may be responsible for a specific subset of tasks, but they work together to provide the necessary functionality to the layer or tier they belong to.

upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 48 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 48

Topic #: 3

[\[All 312-50 Questions\]](#)

A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the following:

Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably.

Another hour goes by and the log files have shrunk in size again.

Which of the following actions should the security administrator take?

- A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
- B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
- C. Run an anti-virus scan because it is likely the system is infected by malware.
- D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

[Hide Answer](#)

Suggested Answer: D

by  [AlbertDenmark](#) at May 12, 2023, 8:29 p.m.

Comments

  [AlbertDenmark](#) 1 year ago

Strange questions. Depends totally on the organization's structure. Not every organization has such a security policy - only perhaps in Utopia.
upvoted 3 times

EXAM 312-50 TOPIC 3 QUESTION 47 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 47

Topic #: 3

[\[All 312-50 Questions\]](#)

A security policy will be more accepted by employees if it is consistent and has the support of

- A. coworkers.
- B. executive management.
- C. the security officer.
- D. a supervisor.

[Hide Answer](#)

Suggested Answer: B

by  **AlbertDenmark** at May 12, 2023, 8:31 p.m.

Comments

 **AlbertDenmark** 1 year ago

Without involvement, you will never get commitment from coworkers. This has nothing to do with IT security but only with leadership.

upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 35 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 35

Topic #: 3

[\[All 312-50 Questions\]](#)

During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered.

Based on this response, which type of packet inspection is the firewall conducting?

- A. Host
- B. Stateful
- C. Stateless Most Voted
- D. Application

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (100%)

by  [thinkinconcept](#) at May 23, 2023, 7:58 p.m.

Comments

  [thinkinconcept](#) 1 year ago

Selected Answer: C

Filtered: Indicates that the probes were not received and the state could not be established. It also indicates that the probes are being dropped by some kind of filtering.

Unfiltered: Indicates that the probes were received but a state could not be established.

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 5 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 5

Topic #: 4

[\[All 312-50 Questions\]](#)

Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

A. Cain Most Voted

B. John the Ripper

C. Nikto

D. Hping

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [thinkinconcept](#) at May 23, 2023, 11:08 p.m.

Comments

  [thinkinconcept](#) 1 year ago

Selected Answer: A

<https://github.com/xchwarz/Cain>

Quote: "recording VoIP conversations"

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 11 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 11

Topic #: 4

[\[All 312-50 Questions\]](#)

An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

- A. g++ hackersExploit.cpp -o calc.exe Most Voted
- B. g++ hackersExploit.py -o calc.exe
- C. g++ -i hackersExploit.pl -o calc.exe
- D. g++ --compile -i hackersExploit.cpp -o calc.exe

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [thinkinconcept](#) at May 23, 2023, 11:15 p.m.

Comments

  [thinkinconcept](#) 1 year ago

Selected Answer: A

A. g++ hackersExploit.cpp -o calc.exe
g++ is a compiler
.cpp file extension is a c++ source code file
upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 24 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 24

Topic #: 4

[\[All 312-50 Questions\]](#)

A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

- A. Cupp
- B. Nessus
- C. Cain and Abel Most Voted
- D. John The Ripper Pro

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [thinkinconcept](#) at May 24, 2023, 4:07 p.m.

Comments

  [thinkinconcept](#) 1 year ago

Selected Answer: C

<https://resources.infosecinstitute.com/topic/password-cracking-using-cain-abel/>
upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 54 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 54

Topic #: 3

[All 312-50 Questions]

During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

- A. The web application does not have the secure flag set.
- B. The session cookies do not have the HttpOnly flag set. **Most Voted**
- C. The victim user should not have an endpoint security solution.
- D. The victim's browser must have ActiveX technology enabled. B

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  sardarji2u at Dec. 30, 2019, 8:13 a.m.

Comments

✉  thinkinconcept 1 year ago

Selected Answer: B

<https://owasp.org/www-community/HttpOnly>
upvoted 1 times

✉  Novmejst 1 year, 1 month ago

Selected Answer: B

HTTP Only flag je varnostni ukrep, ki preprečuje dostop do piškotkov s strani skriptov na strani odjemalca (npr. JavaScripta). Piškotki so majhne datoteke, ki jih spletni strežniki pošljejo brskalniku uporabnika, in se nato shranijo na uporabnikovem računalniku.
upvoted 1 times

✉  salei 1 year, 6 months ago

Selected Answer: B

<https://owasp.org/www-community/HttpOnly>
upvoted 1 times

✉  WZ1122 2 years, 2 months ago

The Secure flag is used to declare that the cookie may only be transmitted using a secure connection (SSL/HTTPS). If this cookie is set, the browser will never send the cookie if the connection is HTTP. This flag prevents cookie theft via man-in-the-middle attacks.

Note that this flag can only be set during an HTTPS connection. If it is set during an HTTP connection, the browser ignores it.
upvoted 1 times

✉  WZ1122 2 years, 2 months ago

Cross-site scripting (XSS) attacks are often aimed at stealing session cookies. In such an attack, the cookie value is accessed by a client-side script using JavaScript (`document.cookie`). However, in everyday use, web applications rarely need to access cookies via JavaScript. Therefore, a method of protecting cookies from such theft was devised: a flag that tells the web browser that the cookie can only be accessed through HTTP – the `HttpOnly` flag.
upvoted 1 times

✉  Marvelous 3 years, 7 months ago

Agree! The session cookies do not have the `HttpOnly` flag set.
upvoted 2 times

✉  Karzee 3 years, 8 months ago

yes b is the correct answer

upvoted 1 times

✉  **brider** 4 years, 1 month ago

B. The session cookies do not have the HttpOnly flag set.

upvoted 2 times

✉  **sardarji2u** 4 years, 5 months ago

Answer must be

The session cookies do not have the HttpOnly flag set.

upvoted 2 times

EXAM 312-50 TOPIC 4 QUESTION 2 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 2

Topic #: 4

[\[All 312-50 Questions\]](#)

Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

- A. Detective
- B. Passive **Most Voted**
- C. Intuitive
- D. Reactive B

[Hide Answer](#)

Suggested Answer: Explanation

Community vote distribution

 B (100%)

by  [sardarji2u](#) at Dec. 30, 2019, 9:09 a.m.

Comments

  **Novmejst** 1 year, 1 month ago

Selected Answer: B

B. Passive

upvoted 1 times

  **munoz** 2 years, 10 months ago

PASSIVE

upvoted 3 times

  **Karzee** 3 years, 8 months ago

passive

upvoted 2 times

  **brider** 4 years, 1 month ago

B. Passive

upvoted 2 times

  **sardarji2u** 4 years, 5 months ago

Passive

upvoted 2 times

EXAM 312-50 TOPIC 2 QUESTION 13 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 13

Topic #: 2

[\[All 312-50 Questions\]](#)

Which of the following techniques will identify if computer files have been changed?

- A. Network sniffing
- B. Permission sets
- C. Integrity checking hashes
- D. Firewall alerts

[Hide Answer](#)

Suggested Answer: C

by  [karthik_2003](#) at June 29, 2023, 8:28 a.m.

Comments

  [karthik_2003](#) 1 year, 5 months ago

Integrity checking hashes are used to verify the integrity of data sent through insecure channels.

upvoted 2 times

EXAM 312-50 TOPIC 2 QUESTION 26 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 26

Topic #: 2

[\[All 312-50 Questions\]](#)

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

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

[Hide Answer](#)

Suggested Answer: D

by  [karthik_2003](#) at June 29, 2023, 8:40 a.m.

Comments

  [karthik_2003](#) 1 year, 5 months ago

John the Ripper is a free password cracking software tool that supports many encryption technologies for Windows and Unix systems.

upvoted 3 times

EXAM 312-50V10 TOPIC 1 QUESTION 99 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 99

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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 Most Voted
- C. Traffic is Blocked on TCP Port 54
- D. Traffic is Blocked on UDP Port 80

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

B (100%)

by  [Jeremy95](#) at Jan. 4, 2020, 4:15 p.m.

Comments

 [BlackAdam](#) 1 year, 4 months ago

Selected Answer: B

B. Traffic is Blocked on TCP Port 80

The problem is likely that traffic is blocked on TCP port 80. TCP port 80 is the default port used for HTTP (Hypertext Transfer Protocol), which is the protocol used for web browsing. When you try to access websites using the URL (e.g., "http://www.example.com"), your browser communicates with the web server over TCP port 80 to retrieve the web pages.

Given that you can ping the servers and access them using their IP addresses, it indicates that the servers are reachable and responsive. However, the fact that you cannot access the websites using their URLs suggests that there may be an issue with the traffic on TCP port 80, which is used for regular web browsing.

upvoted 1 times

 [Jeremy95](#) 4 years, 10 months ago

choice of B and D is same

upvoted 2 times

 [me2](#) 4 years, 8 months ago

How is it the same? Because they are talking about the DNS not the website.

upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 99 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 99

Topic #: 8

[\[All 312-50 Questions\]](#)

The security concept of "separation of duties" is most similar to the operation of which type of security device?

- A. Firewall
- B. Bastion host **Most Voted**
- C. Intrusion Detection System
- D. Honeypot

[Hide Answer](#)

Suggested Answer: A

In most enterprises the engineer making a firewall change is also the one reviewing the firewall metrics for unauthorized changes. What if the firewall administrator wanted to hide something? How would anyone ever find out? This is where the separation of duties comes in to focus on the responsibilities of tasks within security.

References: <http://searchsecurity.techtarget.com/tip/Modern-security-management-strategy-requires-security-separation-of-duties>

Community vote distribution

 B (100%)

by  cannibalkorpo at July 25, 2023, 12:22 p.m.

Comments

  **cannibalkorpo** 1 year, 4 months ago

Selected Answer: B
As for me it is a bastion host - as a server especially hardened with only one responsibility.
upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 125 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 125

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following statements regarding ethical hacking is incorrect?

- A. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.
- B. Testing should be remotely performed offsite.
- C. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.
- D. Ethical hacking should not involve writing to or modifying the target systems.

[Hide Answer](#)

Suggested Answer: A

Ethical hackers use the same methods and techniques, including those that have the potential of exploiting vulnerabilities, to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.

References: <http://searchsecurity.techtarget.com/definition/ethical-hacker>

by  [aids00123](#) at Aug. 13, 2023, 9:58 a.m.

Comments

 [aids00123](#) 1 year, 3 months ago

Disagree. A states 'have the potential of exploiting vulnerabilities'. This suggests the attacker shouldn't try and run mimikatz just because it has the potential to get the hashes, which is the whole point of a pen test. D is correct - you shouldn't write or modify company systems that could cause changes in business continuity

upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 288 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 288

Topic #: 8

[\[All 312-50 Questions\]](#)

Study the log below and identify the scan type.

tcpdump -vv host 192.168.1.10

```
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)
```

tcpdump -vv -x host 192.168.1.10

```
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060)
4500 0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
```

A. nmap -sR 192.168.1.10

B. nmap -sS 192.168.1.10

C. nmap -sV 192.168.1.10

D. nmap -sO -T 192.168.1.10

[Hide Answer](#)

Suggested Answer: D

by  [aids00123](#) at Aug. 16, 2023, 10:43 a.m.

Comments

  [aids00123](#) 1 year, 3 months ago

Sorry, IP Protocol scan, my bad
upvoted 1 times

  [aids00123](#) 1 year, 3 months ago

How does this scan reveal the OS, as would be with D? Surely this is just a Syn Scan - B
upvoted 1 times

EXAM 312-50 TOPIC 5 QUESTION 7 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 7

Topic #: 5

[\[All 312-50 Questions\]](#)

When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

- A. The key entered is a symmetric key used to encrypt the wireless data. Most Voted
- B. The key entered is a hash that is used to prove the integrity of the wireless data.
- C. The key entered is based on the Diffie-Hellman method.
- D. The key is an RSA key used to encrypt the wireless data. A

[Hide Answer](#)

Suggested Answer: *Explanation*

Community vote distribution

A (100%)

by  [Jeremy95](#) at Jan. 21, 2020, 6:22 a.m.

Comments

  [dehamedah](#) 1 year, 4 months ago

Selected Answer: A

answer is A

upvoted 1 times

  [dorinh](#) 3 years, 6 months ago

WEP/WPA/WPA2 do not use RSA. Moreover, encryption (such as that of a wireless network) deals with confidentiality and not integrity. Finally, the "based on D-H" option is ruled out in that Diffie-Hellman is an asymmetric protocol, which RC4/TKIP/CCMP are not.

upvoted 2 times

  [brider](#) 5 years, 1 month ago

A. The key entered is a symmetric key used to encrypt the wireless data.

upvoted 3 times

  [Jeremy95](#) 5 years, 4 months ago

Answer is A

upvoted 2 times

EXAM 312-50 TOPIC 8 QUESTION 4 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 4

Topic #: 8

[\[All 312-50 Questions\]](#)

You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled.

Which port would you see listening on these Windows machines in the network?

A. 445

B. 3389

C. 161

D. 1433

[Hide Answer](#)

Suggested Answer: A

The following ports are associated with file sharing and server message block (SMB) communications:

- ⇒ Microsoft file sharing SMB: User Datagram Protocol (UDP) ports from 135 through 139 and Transmission Control Protocol (TCP) ports from 135 through 139.
- ⇒ Direct-hosted SMB traffic without a network basic input/output system (NetBIOS): port 445 (TCP and UDP).

References: <https://support.microsoft.com/en-us/kb/298804>

by  [y2mk1ng](#) at Dec. 20, 2023, 3:16 p.m.

Comments

  [y2mk1ng](#) 1 year, 5 months ago

Port 3389 is for remote access, e. g. RDP;

Port 161 is for SNMP;

Port 1433 is listened on TCP/IP for SQL Server Database Engine.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 130 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 130

Topic #: 1

[All 312-50v12 Questions]

In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with 'y' columns. Each table contains 'z' records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include 'UNION SELECT' statements and 'DBMS_XSLPROCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted 'E=xyz*u'. Assuming 'x=4', 'y=2', and varying 'z' and 'u', which situation is likely to result in the highest extracted data volume?

- A. z=600, u=2: The attacker devises 2 SQL payloads, each aimed at tables holding 600 records, affecting all columns across all tables.
- B. z=550, u=2: Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables.
- C. z=500, u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables.
- D. z=400, u=4: The attacker constructs 4 SQL payloads, each focusing on tables with 400 records, influencing all columns of all tables.

Most Voted

Hide Answer

Suggested Answer: D

Community vote distribution

D (100%)

by  smoce at Feb. 5, 2024, 1:50 p.m.

Comments

✉  insaniuont Highly Voted 1 year, 3 months ago

Selected Answer: D

E = (4 * 2 * z) * u

- A. E = (4 * 2 * 600) * 2 = 9600
- B. E = (4 * 2 * 550) * 2 = 8800
- C. E = (4 * 2 * 500) * 3 = 12000
- D. E = (4 * 2 * 400) * 4 = 12800

upvoted 5 times

✉  smoce Highly Voted 1 year, 3 months ago

Selected Answer: D

E=(xyz)*u

A. 9600

B. 8800

C. 12000

D. 12800

upvoted 5 times

✉  sosindi Most Recent 1 year, 3 months ago

Selected Answer: D

Answer is D

upvoted 1 times

✉  JR22craft 1 year, 3 months ago

Selected Answer: D

Answer is D

upvoted 1 times

✉  brrbrr 1 year, 3 months ago

Selected Answer: D

Answer is D

upvoted 1 times

 EXAM 312-50V12 TOPIC 1 QUESTION 145 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 145

Topic #: 1

[All 312-50v12 Questions]

As a Certified Ethical Hacker, you are conducting a footprinting and reconnaissance operation against a target organization. You discover a range of IP addresses associated with the target using the SecurityTrails tool. Now, you need to perform a reverse DNS lookup on these IP addresses to find the associated domain names, as well as determine the nameservers and mail exchange (MX) records. Which of the following DNSRecon commands would be most effective for this purpose?

- A. dnsrecon -r 192.168.1.0/24 -n ns1.example.com -t axfr
- B. dnsrecon -r 10.0.0.0/24 -n ns1.example.com -t zonewalk
- C. dnsrecon -r 162.241.216.0/24 -n ns1.example.com -t std Most Voted
- D. dnsrecon -r 162.241.216.0/24 -d example.com -t brt

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [smoce](#) at Feb. 5, 2024, 2:03 p.m.

Comments

  [smoce](#) Highly Voted 1 year, 3 months ago

Selected Answer: C

The std type is often used for standard enumeration, which includes fetching PTR, NS, and MX records.
upvoted 6 times

  [tow](#) Most Recent 1 year, 2 months ago

Selected Answer: C

The std type is often used for standard enumeration, which includes fetching PTR, NS, and MX records.C
upvoted 1 times

  [LeongCC](#) 1 year, 3 months ago

Selected Answer: C

Is C -std
upvoted 1 times

  [brrbrr](#) 1 year, 3 months ago

Selected Answer: C

-t TYPE, --type TYPE Type of enumeration to perform.
Possible types:
std: SOA, NS, A, AAAA, MX and SRV.
upvoted 1 times

  [przemyslaw1](#) 1 year, 3 months ago

Selected Answer: C

C. -t std
upvoted 2 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: C

C.
"-t std": Specifies the type of DNS query to perform. In this case, it's a standard query
upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 172 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 172

Topic #: 1

[All 312-50v12 Questions]

An IT company has just implemented new security controls to their network and system setup. As a Certified Ethical Hacker, your responsibility is to assess the possible vulnerabilities in the new setup. You are given the information that the network and system are adequately patched with the latest updates, and all employees have gone through recent cybersecurity awareness training. Considering the potential vulnerability sources, what is the best initial approach to vulnerability assessment?

- A. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information
- B. Checking for hardware and software misconfigurations to identify any possible loopholes **Most Voted**
- C. Evaluating the network for inherent technology weaknesses prone to specific types of attacks
- D. Investigating if any ex-employees still have access to the company's system and data

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by [cloudgangster](#) at Feb. 6, 2024, 8:14 a.m.

Comments

GK2205 1 year, 4 months ago

Selected Answer: B

The key to this question is "Best .. initial ..."
upvoted 1 times

LordXander 1 year, 8 months ago

Selected Answer: B

It's B because misconfiguration still can occur after proper patching and training
upvoted 2 times

qtygbapjpesdayazko 1 year, 8 months ago

Selected Answer: B

Keyword "new setup". Checking for hardware and software misconfigurations to identify any possible loopholes
upvoted 2 times

brrbrr 1 year, 9 months ago

Selected Answer: C

Given that the network and system are adequately patched, and employees have undergone recent cybersecurity awareness training, the best initial approach to vulnerability assessment would likely be:

C. Evaluating the network for inherent technology weaknesses prone to specific types of attacks.

While all the options are important aspects of a comprehensive vulnerability assessment, evaluating the network for inherent technology weaknesses helps identify potential vulnerabilities that may exist due to the configuration, design, or technology choices. This involves assessing the network for weaknesses that could be exploited by attackers, such as insecure protocols, open ports, or default configurations that may pose security risks. This step complements the information about the latest updates and cybersecurity awareness training by focusing on the technical aspects of the network's security posture.

upvoted 1 times

brrbrr 1 year, 9 months ago

actually, B is the correct answer.

upvoted 3 times

athicalacker 1 year, 9 months ago

The question mentions adequate patching, suggesting these weaknesses are likely addressed. So it can't be C.

The answer is option B. Even with patches and training, misconfigurations can introduce vulnerabilities. Checking for them first allows you to identify and address fundamental flaws before proceeding to more advanced testing.

upvoted 3 times

 **insaniunt** 1 year, 9 months ago

Selected Answer: B

B. Checking for hardware and software misconfigurations to identify any possible loopholes

upvoted 2 times

 **cloudgangster** 1 year, 9 months ago

Selected Answer: B

I'm not sure but i think B

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 218 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 218

Topic #: 1

[All 312-50v12 Questions]

An ethical hacker is testing the security of a website's database system against SQL Injection attacks. They discover that the IDS has a strong signature detection mechanism to detect typical SQL injection patterns. Which evasion technique can be most effectively used to bypass the IDS signature detection while performing a SQL Injection attack?

- A. Employ IP fragmentation to obscure the attack payload
- B. Implement case variation by altering the case of SQL statements
- C. Leverage string concatenation to break identifiable keywords
- D. Use Hex encoding to represent the SQL query string

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by [cloudgangster](#) at Feb. 6, 2024, 12:06 p.m.

Comments

✉ **Mos3ab** 9 months, 2 weeks ago

Selected Answer: C

When an IDS relies on fixed signatures to detect typical SQL injection patterns, using string concatenation to obfuscate SQL keywords (for example, writing "SEL" + "ECT" instead of "SELECT") can effectively bypass those signatures. This method alters the appearance of the SQL payload without affecting its functionality once processed by the database. In contrast, techniques like case variation are often normalized by the IDS, and hex encoding might be decoded during inspection. IP fragmentation is generally not effective for SQL injection payloads, as it is more suited for network-layer evasion.

upvoted 1 times

✉ **Lennin** 9 months, 3 weeks ago

Selected Answer: C

String concatenation is more effective because it splits up SQL keywords into multiple pieces that are much harder for an IDS to recognize as part of a known attack. For example, splitting SELECT into S + E + L + E + C + T makes it difficult for the IDS to match the attack pattern because the SQL keyword is now fragmented and unrecognizable to signature-based detection.

upvoted 1 times

✉ **7c4eac1** 1 year ago

Selected Answer: C

String concatenation effectively disrupts the recognizable structure of SQL keywords while ensuring the payload remains syntactically valid.

upvoted 1 times

✉ **49f4430** 1 year, 6 months ago

Ok D but why not C? it also evade IDS and chatGPT says is more easy to implement

upvoted 1 times

✉ **LordXander** 1 year, 8 months ago

Selected Answer: D

I would go with D because A is more specific with bypassing network traffic...

upvoted 1 times

✉ **LordXander** 1 year, 8 months ago

Also I really doubt the usage of "obscure" for the payload

upvoted 1 times

✉ **qtygbapjpesdayazko** 1 year, 8 months ago

Selected Answer: D

The most efective "D. Use Hex encoding to represent the SQL query string"

Hex encoding is an evasion technique that uses hexadecimal encoding to represent a string. Attackers use hex encoding to obfuscate the SQL query so that it will not be detected in the signatures of security measures, as most IDS do not recognize hex encodings. Attackers exploit such IDS to bypass their SQL injection crafted inputs. Hex encoding provides countless ways for attackers to obfuscate each URL.

upvoted 1 times

✉️ **Mos3ab** 9 months, 2 weeks ago

While hex encoding can obfuscate the payload, modern IDS are often equipped to decode such encodings during their inspection processes. This means that even if the payload is hex-encoded, the IDS may still recognize the malicious pattern after decoding it. Therefore, relying solely on hex encoding may not be sufficient to bypass IDS signature detection.

upvoted 2 times

✉️ **Spam_Protection** 1 year, 8 months ago

Selected Answer: D

D: Module 15, it has its own section.

upvoted 1 times

✉️ **Bobite** 1 year, 8 months ago

Selected Answer: D

Might be D because A can't be a good answer. The server IS sending to the bdd so can't be splitted

upvoted 1 times

✉️ **anarchyeagle** 1 year, 9 months ago

C. Leverage string concatenation to break identifiable keywords: String concatenation involves splitting SQL keywords and data within the injection payload, making it harder for signature-based IDS systems to match the payload against known SQL injection patterns. This technique can effectively obscure the malicious SQL code, making it less likely to be detected by signature-based detection mechanisms.

upvoted 1 times

✉️ **brrrrr** 1 year, 9 months ago

Selected Answer: D

D. Hex encoding involves representing characters in hexadecimal format, which can help obfuscate the SQL query string. By encoding the SQL injection payload in hexadecimal, an attacker can evade signature-based detection mechanisms that typically rely on detecting specific SQL injection patterns or keywords.

Its not A, because IP fragmentation is more related to evading network-based detection mechanisms, and it may not be as effective against signature-based detection focused on SQL injection patterns.

upvoted 1 times

✉️ **lukinno** 1 year, 9 months ago

Selected Answer: D

Options B (case variation) and D (Hex encoding) are the most effective strategies for bypassing IDS signature detection during SQL injection attacks.

If I have to choose one I vote D

upvoted 1 times

✉️ **qwerty100** 1 year, 9 months ago

Selected Answer: A

I think it's A:

(Module 15 Page 2334)

Evasion Technique: IP Fragmentation An attacker intentionally splits an IP packet to spread the packet across multiple small fragments. Attackers use this technique to evade an IDS or WAF. For an IDS or WAF to detect an attack, it must first reassemble the packet fragments. Usually, it is impossible to find a match between the attack string and a signature as each packet is checked individually. These small fragments can be further modified to complicate reassembly and detection of an attack payload.

upvoted 4 times

✉️ **Mos3ab** 9 months, 2 weeks ago

While IP fragmentation is a valid evasion technique at the network layer, it is not suitable for application-layer attacks like SQL injection. Employing string concatenation to obfuscate SQL keywords is a more effective strategy to bypass IDS signature detection in this context.

upvoted 1 times

✉️ **insaniunt** 1 year, 9 months ago

Selected Answer: D

D. Use Hex encoding to represent the SQL query string

upvoted 2 times

✉️ **cloudgangster** 1 year, 9 months ago

I think its D

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 132 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 132

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Your company has been receiving regular alerts from its IDS about potential intrusions. On further investigation, you notice that these alerts have been false positives triggered by certain goodware files. In response, you are planning to enhance the IDS with YARA rules, reducing these false positives while improving the detection of real threats. Based on the scenario and the principles of YARA and IDS, which of the following strategies would best serve your purpose?

- A. Writing YARA rules specifically to identify the goodware files triggering false positives Most Voted
- B. Implementing YARA rules that focus solely on known malware signatures
- C. Creating YARA rules to examine only the private database for intrusions
- D. Incorporating YARA rules to detect patterns in all files regardless of their nature

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [qtygbapjpesdayazko](#) 1 year, 2 months ago

Keyword "principles of YARA", so we create YARA rules with filters to filter false positives. A. Writing YARA rules specifically to identify the goodware files triggering false positives.

upvoted 1 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: A

A. Writing YARA rules specifically to identify the goodware files triggering false positives
Module 12 Page 1642

upvoted 3 times

  [cloudgangster](#) 1 year, 3 months ago

Selected Answer: A

A i think, others dont focus on the main objective
upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 135 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 135

Topic #: 1

[\[All 312-50v12 Questions\]](#)

As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data. However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

- A. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure.
- B. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay.
- C. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries. **Most Voted**
- D. The hacker alters his approach and injects a 'DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [insaniunt](#)  1 year, 3 months ago

Selected Answer: C

C - Encoding can work with the special character filter because the filter may not recognize the encoded input as a special character. For example, the filter may block the single quote character ('') but not the URL encoded version of it (%27). So the hacker can use the encoded input to trick the filter and still inject malicious SQL commands

upvoted 9 times

  [qtygbapjpesdayzko](#) 1 year, 2 months ago

this is the way

upvoted 1 times

  [lmourikis](#)  1 year, 3 months ago

The black-hat hacker tries to 'trick the login process into returning additional data'. Also, in the end it is mentioned that 'the hacker still intends to exploit this SQL Injection vulnerability'. So:

Not A - He/She does not ant the structure but the data

Not B - Delay will not say much about the data but rather whether a query is valid or not

Not D - Data loss is not what he/she seeks for.

It's B as encoding may allow to bypass the special characters filtering.

upvoted 2 times

 EXAM 312-50V12 TOPIC 1 QUESTION 136 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 136

Topic #: 1

[All 312-50v12 Questions]

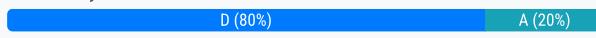
You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?

- A. UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables
 - B. ' OR username LIKE '%': This payload uses the LIKE operator to search for a specific pattern in a column
 - C. ' OR '1'='1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data
 - D. ' OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 insaniunt 1 year, 3 months ago

Selected Answer: D

The correct answer is D. This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss. This is the most significant impact because it can result in the deletion of an entire table from the database, which may contain sensitive customer data. The other payloads only allow the attacker to view or retrieve data, but not to modify or delete it. Therefore, they have less impact than D.

upvoted 8 times

 aklsjda Most Recent 1 year, 1 month ago

The question didn't specify if there is a back up of the database, logically B&C are eliminated cuz "BRO". and A is eliminated because the attacker doe not want other tables data, so D is the answer (if database is deleted+no backup=DOOM!)

upvoted 1 times

 calx5 1 year, 3 months ago

Selected Answer: A

A and C = data leakage; A with multiple-data leakage, big impact.

B = pattern only, not data

D = No data leakage, it is just data loss with backup as recovery.

upvoted 2 times

 Lalo 1 year, 2 months ago

Correct answer DDDDDDDDDDDDDDDDDDDDDDDDDDD.

Assuming that the other tables have critical information. However, what if they are temporary tables without critical information (the question does not clarify whether they are tables with important information or not). In this type of questions you have to check if they cover ALL possible options. In this situation, if we assume that it is unimportant data, the SQL injection attack with the most significant impact is D

upvoted 1 times

 insaniunt 1 year, 3 months ago

Payload D is indeed the most destructive among the options. It not only manipulates the WHERE clause for unauthorized data access but also includes a DROP TABLE statement, which can lead to the deletion of the "members" table, causing data loss.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 137 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 137

Topic #: 1

[All 312-50v12 Questions]

A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exhort the TGS tickets from memory for offline cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?

- A. Perform a system reboot to clear the memory
- B. Delete the compromised user's account
- C. Change the NTLM password hash used to encrypt the ST
- D. Invalidate the TGS the attacker acquired Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (52%) C (48%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [insaniunt](#) Highly Voted 1 year, 9 months ago

Selected Answer: D

D. Invalidate the TGS the attacker acquired: This is the best option among the four. Invalidating the TGS ticket will prevent the attacker from using it to access the network service, regardless of whether he cracks the password hash or not. This will effectively stop the Kerberoasting attack and protect the network from further compromise.

upvoted 6 times

 [kennels](#) Highly Voted 1 year, 9 months ago

Selected Answer: C

If the TGS ticket is disabled but the password is not changed, the attacker should be able to obtain the victim's password through offline cracking of the issued TGS and connect to the network entity, I think.

upvoted 6 times

 [KalingaDev](#) Most Recent 11 months, 2 weeks ago

Selected Answer: C

Changing the password will be more effective, otherwise, the same attack can happen.

upvoted 2 times

 [F4ll3n92](#) 1 year, 2 months ago

the question ask the immediate step to do...so, i think that the correct answer is D

upvoted 2 times

 [noyon2002](#) 1 year, 3 months ago

I Think C, the key word her is : But the attacker was stopped before he could complete his attack, that means he cannot access with the ticket acquired, and the after that the sentence said The system administrator needs to investigate and remediate the potential breach, so he should change the NTLM PWD hash used to encrypt the ST

upvoted 2 times

 [49f4430](#) 1 year, 6 months ago

Selected Answer: D

You Invalidate the ticket and after you change the password.

If you change the password the ticket is still valid...

The question ask for immediate action :

Action Nr.1 : Invalidate the ticket

upvoted 1 times

✉️ **dellalba** 1 year, 7 months ago

Selected Answer: D

The most insidious part about this attack is you can change the password for the KRBTGT account, but the authentication token is still valid. You can rebuild the DC, but that authentication token is still valid.

upvoted 1 times

✉️ **Oaf6dbd** 1 year, 7 months ago

Option C - Change the NTLM password hash used to encrypt the ST because the TGS is encrypted using the target service accounts' NTLM password hash

upvoted 2 times

✉️ **LordXander** 1 year, 8 months ago

Selected Answer: D

The correct answer would be C & D. That would be complete..however, the most correct answer would be D since this would stop the Cyber Killchain (exploitation)...but if I would have this question in the exam...toss a coin

upvoted 1 times

✉️ **Spam_Protection** 1 year, 8 months ago

Selected Answer: D

Module 4 P.416: To crack the ST, attackers export the TGS tickets from memory and save them offline to the local system. Furthermore, attackers use different NTLM hashes to crack the ST and, on successfully cracking it, the service account password can be discovered. Attackers use tools such as Kerberoast to perform Kerberoasting attacks on Kerberos authentication.

upvoted 1 times

✉️ **LeongCC** 1 year, 9 months ago

Selected Answer: C

ChatGPT checked C

upvoted 2 times

✉️ **przemyslaw1** 1 year, 9 months ago

Selected Answer: C

C. Change the NTLM password

upvoted 1 times

✉️ **przemyslaw1** 1 year, 9 months ago

C. Change the NTLM password hash used to encrypt the ST because the TGS is encrypted using the target service accounts' NTLM password hash

upvoted 3 times

✉️ **cloudgangster** 1 year, 9 months ago

Selected Answer: D

D is it.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 140 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 140

Topic #: 1

[All 312-50v12 Questions]

XYZ company recently discovered a potential vulnerability on their network, originating from misconfigurations. It was found that some of their host servers had enabled debugging functions and unknown users were granted administrative permissions. As a Certified Ethical Hacker, what would be the most potent risk associated with this misconfiguration?

- A. An attacker may be able to inject a malicious DLL into the current running process
- B. Weak encryption might be allowing man-in-the-middle attacks, leading to data tampering
- C. Unauthorized users may perform privilege escalation using unnecessarily created accounts Most Voted
- D. An attacker may carry out a Denial-of-Service assault draining the resources of the server in the process

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

lmourikis Highly Voted 1 year, 8 months ago

I believe it's not C, as unknown users have already been granted administrative permissions. Also, there is nowhere mentioned that unnecessarily accounts have been created. Also, not B or D, as these type of attacks do not require gaining admin permissions on a system. The problem with unknown users getting admin perms is that they can change the code the server is running, eg by injecting a malicious DLL. So, it's A.

upvoted 6 times

agelbahri Most Recent 8 months, 3 weeks ago

Selected Answer: C

CEH v12 page: 545

Host Misconfigurations

upvoted 1 times

yaolsaydi 10 months ago

Selected Answer: C

Option A (DLL injection) is not directly related to the described misconfiguration.

Option B (weak encryption) is not mentioned in the scenario.

Option D (Denial-of-Service) is possible but less likely to be the most potent risk given the specific misconfigurations described.

upvoted 1 times

Rami1996 10 months, 2 weeks ago

Selected Answer: A

An attacker may be able to inject a malicious DLL into the current running process

upvoted 1 times

jeejy 11 months, 1 week ago

It's C because, with administrative privileges, you can gain greater control over the network.

upvoted 1 times

blehbleh 1 year ago

Selected Answer: A

C doesn't make sense, unknown users were already granted access. C states "C. Unauthorized users may perform privilege escalation using unnecessarily created accounts". It states may perform privilege escalation, it's not may, the privileges are already there. There is no need for privilege escalation, it has already been granted. Additionally, it says using unnecessarily created accounts, nowhere in here does it say any accounts were created unnecessarily. B and D are both wrong. So I have to go with A.

upvoted 1 times

👤 **Binx** 1 year, 3 months ago

I believe the answer is A

Yes, it is possible for an attacker to inject a malicious DLL through a server debugging tool, especially if debugging functions are enabled and not properly secured. Here's how:

Exploiting Debugging Functions: Debugging tools often have elevated privileges and direct access to the system memory and processes. If an attacker gains access to these debugging functions, they can manipulate the system in various ways, including injecting malicious code.

DLL injection is a technique used to run malicious code within the address space of another process by loading a dynamic link library (DLL). If debugging functions are enabled, an attacker with access can use these tools to load their malicious DLL into a RUNNING PROCESS.

upvoted 1 times

👤 **f257c4e** 1 year, 6 months ago

I think Is A, why bother in priv esc if the user has already administrative account?!

upvoted 1 times

👤 **LordXander** 1 year, 8 months ago

Selected Answer: C

Why bother with A when you can already have system access by using C. Also AI says C, the book says A & C, and C makes more sense...so C

upvoted 1 times

👤 **qtygbapjpesdayazko** 1 year, 8 months ago

Selected Answer: A

Is C. Key words "unknown users were granted administrative permissions"

upvoted 2 times

👤 **qtygbapjpesdayazko** 1 year, 8 months ago

IS C!!!

upvoted 1 times

👤 **[Removed]** 1 year, 9 months ago

Could someone please validate this information

upvoted 1 times

👤 **insaniunt** 1 year, 9 months ago

Selected Answer: C

C. Unauthorized users may perform privilege escalation using unnecessarily created accounts

upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 143 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 143

Topic #: 1

[All 312-50v12 Questions]

A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

- A. The system failed to establish a connection due to an incorrect port number.
- B. The enumeration process was blocked by the target system's intrusion detection system.
- C. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation. **Most Voted**
- D. The Python version installed on the CEH's machine is incompatible with the ldap3 library.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **Spam_Protection** 1 year, 2 months ago

Selected Answer: C

3. As shown in the code given below, create a server object (server), specify the target IP address or hostname and port number. If the target server is listening on secure LDAP, specify use_ssl = True.

upvoted 2 times

 **insaniunt** 1 year, 3 months ago

Selected Answer: C

"The system is secured and accepts connections only on secure LDAP."

upvoted 3 times

 **qtygbapjpesdayazko** 1 year, 2 months ago

This is the way

upvoted 1 times

 **cloudgangster** 1 year, 3 months ago

Selected Answer: C

PG 434 CEH V12

upvoted 2 times

 **cloudgangster** 1 year, 3 months ago

C is the answer, CEH V12 PG434

upvoted 1 times

Exam 312-50v12 Topic 1 Question 144 Discussion

Actual exam question from ECCouncil's 312-50v12

Question #: 144

Topic #: 1

[All 312-50v12 Questions]

You are a cybersecurity consultant for a major airport that offers free Wi-Fi to travelers. The management is concerned about the possibility of "Evil Twin" attacks, where a malicious actor sets up a rogue access point that mimics the legitimate one. They are looking for a solution that would not significantly impact the user experience or require travelers to install additional software. What is the most effective security measure you could recommend that fits these constraints, considering the airport's unique operational environment?

- A. Regularly change the SSID of the airport's Wi-Fi network
- B. Use MAC address filtering on the airport's Wi-Fi network
- C. Implement WPA3 encryption for the airport's Wi-Fi network
- D. Display a captive portal page that warns users about the possibility of Evil Twin attacks Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

qwerty100 Highly Voted 1 year, 9 months ago

Selected Answer: C

C. Implement WPA3 encryption for the airport's Wi-Fi network

An evil twin can Display a captive portal page that warns users about the possibility of Evil Twin attacks
upvoted 5 times

JustAName Highly Voted 1 year, 9 months ago

Selected Answer: D

I'd go with D, while implementing WPA3 encryption is always good to strengthen the security of the wifi. But it only protect the actual airport's wifi and doesn't properly address the issue of possible evil twin attack. So D is the best answer available in my opinion.
upvoted 5 times

blehbleh Most Recent 1 year ago

Selected Answer: D

I have seen several stupid questions in this dump. This is one of them. I am assuming they want you to select C because WPA3 it talked about helping prevent evil twins. But in reality it can't protect against an evil twin, it can make your connection more secure if you are connected to a WPA3 connection but it can't negate or stop you from connecting to an evil twin which is why the real answer here should be D, but on the test I would probably answer C because if you do any research about WPA3 and its benefits compared to previous versions preventing evil twins in mentioned but it really doesn't do anything against an evil twin. I'm pretty sure I read about it in a SANS book as well about how WPA3 helps protect against evil twins.
upvoted 1 times

pboniface 1 year ago

Selected Answer: D

Answer is D,
If you use WPA3, how does it prevent an attacker from creating the same SSID and broadcasting it in the airport...
upvoted 1 times

pboniface 1 year, 1 month ago

Selected Answer: D

D is correct
upvoted 1 times

✉️  **yicx1** 1 year, 5 months ago

Selected Answer: D

C doesn't do anything to the evil twin use case
upvoted 1 times

✉️  **qtygbapjpesdayazko** 1 year, 8 months ago

Selected Answer: D

Is D, WPA3 with a open SSID do not protect to "Evil Twin" attacks,
<https://security.stackexchange.com/questions/188707/does-wpa3-owe-mean-the-return-of-evil-twins>
upvoted 1 times

✉️  **Spam_Protection** 1 year, 8 months ago

Selected Answer: C

WPA3 will keep people from being disconnected and possibly connected to Evil Twin. WPA3 focus on encryption not authentication(no open network provides auth). You still need to deploy rogue-AP detection or wireless intrusion prevention/detection systems to prevent wireless attacks.
upvoted 1 times

✉️  **anarchyeagle** 1 year, 9 months ago

Selected Answer: C

Chat GPT Response: The most effective and practical solution that fits the given constraints is Option C: Implement WPA3 encryption for the airport's Wi-Fi network. This approach enhances security without significantly impacting the user experience or requiring the installation of additional software. It directly addresses the vulnerability to "Evil Twin" attacks by ensuring that the connection between the user's device and the Wi-Fi network is securely encrypted, making it much more difficult for attackers to mimic or intercept communications.

upvoted 3 times

✉️  **[Removed]** 1 year, 9 months ago

Hey team can we double-check this response
upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 146 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 146

Topic #: 1

[All 312-50v12 Questions]

You are an ethical hacker tasked with conducting an enumeration of a company's network. Given a Windows system with NetBIOS enabled, port 139 open, and file and printer sharing active, you are about to run some nbtstat commands to enumerate NetBIOS names. The company uses IPv6 for its network. Which of the following actions should you take next?

- A. Switch to an enumeration tool that supports IPv6 Most Voted
- B. Use nbtstat -a followed by the IPv6 address of the target machine
- C. Use nbtstat -c to get the contents of the NetBIOS name cache
- D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (50%) D (29%) B (21%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [d02c2d5](#) 11 months, 3 weeks ago

Selected Answer: A

Which of the following actions should you take next? Next for what? for having more info on windows host with netbios e enabled D ; For discovering other host on network A. Clarify please!

upvoted 1 times

 [tyw82](#) 1 year, 1 month ago

Selected Answer: A

NetBIOS is not compatible with IPv6, as NetBIOS is an older protocol that was designed specifically for use in IPv4 networks. So you can't really enumerate the NetBIOS names. Therefore B,C and D are not correct. Note that the question starts with saying that your task is to enumerate the company's network, not NetBIOS per se.

upvoted 4 times

 [49f4430](#) 1 year, 6 months ago

Selected Answer: B

o'reilly:

Microsoft Windows uses an interface called Network Basic Input/Output System (NetBIOS), which relates names with workstations and is an upper-layer interface that requires a transport protocol—usually, TCP/IP. But IPv6 can be used as well. Deploying the nbtstat utility will achieve these three important things:

upvoted 1 times

 [qtygbapjpesdayzko](#) 1 year, 8 months ago

Selected Answer: D

Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration, nbtstat is not available for IPv6

upvoted 1 times

 [LordXander](#) 1 year, 8 months ago

Selected Answer: B

Guys...nbtstat is compatible with IPv6...so B? D could be but then you could run into some issues with NSE....this is a badluck question honestly

upvoted 2 times

 [broman](#) 1 year, 2 months ago

nbtstat -a <IPv6_address>

upvoted 1 times

✉ **qtygbapjpesdayazko** 1 year, 8 months ago

Selected Answer: D

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

upvoted 1 times

✉ **ethacker2** 1 year, 9 months ago

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

Nmap Scripting Engine (NSE) is used by attackers to discover NetBIOS shares on a network. Attackers can retrieve the target's NetBIOS names and MAC addresses using the NSE nbtstat script. By default, the script displays the computer's name and the currently logged-in user.

```
nmap -sV -v --script nbstat.nse <target IP address>
```

Reference: <https://github.com/mosse-security/mcsi-library/blob/main/docs/articles/2022/06/netbios-enumeration/netbios-enumeration.md>

upvoted 2 times

✉ **John07** 1 year, 8 months ago

```
C:\>nmap --script nbstat.nse 001:0000:130F:0000:0000:09C0:876A:130B Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-26 10:33 GMT
Standard Time 001:0000:130F:0000:0000:09C0:876A:130B looks like an IPv6 target specification -- you have to use the -6 option. WARNING: No targets were specified, so 0 hosts scanned. Nmap done: 0 IP addresses (0 hosts up) scanned in 0.09 seconds
```

upvoted 2 times

✉ **qwerty100** 1 year, 9 months ago

Selected Answer: A

I couldn't find any IPV6 NetBIOS enumeration script for NSE

I'm going to choose A

A. Switch to an enumeration tool that supports IPv6

upvoted 1 times

✉ **John07** 1 year, 8 months ago

```
C:\>nmap --script nbstat.nse 2001:0000:130F:0000:0000:09C0:876A:130B Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-26 10:35 GMT
Standard Time 2001:0000:130F:0000:0000:09C0:876A:130B looks like an IPv6 target specification -- you have to use the -6 option. WARNING: No targets were specified, so 0 hosts scanned. Nmap done: 0 IP addresses (0 hosts up) scanned in 0.10 seconds
```

upvoted 1 times

✉ **JR22craft** 1 year, 9 months ago

Selected Answer: D

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

upvoted 1 times

✉ **brrbrr** 1 year, 9 months ago

Selected Answer: A

B. Use nbtstat -a followed by the IPv6 address of the target machine

This command queries the specified IPv6 address for NetBIOS name information.

Option A is not necessary as nbtstat can still be used for NetBIOS enumeration even if IPv6 is in use.

Option C provides the contents of the NetBIOS name cache but does not directly enumerate NetBIOS names on a specific machine.

Option D suggests using Nmap Scripting Engine (NSE) for NetBIOS enumeration, which is an alternative but not necessary when nbtstat is available and suitable for the task.

upvoted 1 times

✉ **brrbrr** 1 year, 9 months ago

Actually correct answer is D

upvoted 2 times

✉ **Bobite** 1 year, 9 months ago

There is no name resolution for netbios IPV6 sp nbtstat -a wouldn't work.

The correct answer might be D

upvoted 1 times

✉ **Unr34l** 1 year, 9 months ago

I think that is the B

B. Use nbtstat -a followed by the IPv6 address of the target machine

Explanation:

Since the company uses IPv6 for its network and you want to enumerate NetBIOS names, you can use the following nbtstat command:

```
bash
```

Copy code

```
nbtstat -a [IPv6_address]
```

This command will attempt to query the NetBIOS names associated with the specified IPv6 address.

upvoted 2 times

✉️ **[Removed]** 1 year, 9 months ago

Hey friends can we make sure this is correct

upvoted 2 times

✉️ **insaniunt** 1 year, 9 months ago

Selected Answer: D

D.

Attackers use the Nmap Scripting Engine (NSE) for discovering NetBIOS shares on a network. The NSE nbstat script allows attackers to retrieve the target's NetBIOS names and MAC addresses. By default, the script displays the name of the computer and the logged-in user. However, if the verbosity is turned up, it displays all names related to that system. An attacker uses the following Nmap command to perform NetBIOS enumeration on a target host:

```
nmap -sV -v --script nbstat.nse <target IP address>
```

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 148 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 148

Topic #: 1

[All 312-50v12 Questions]

A large corporation is planning to implement preventive measures to counter a broad range of social engineering techniques. The organization has implemented a signature-based IDS, intrusion detection system, to detect known attack payloads and network flow analysis to monitor data entering and leaving the network. The organization is deliberating on the next step. Considering the information provided about various social engineering techniques, what should be the organization's next course of action?

- A. Implement endpoint detection and response solution to oversee endpoint activities
- B. Set up a honeypot to attract potential attackers into a controlled environment for analysis
- C. Deploy more security personnel to physically monitor key points of access
- D. Organize regular employee awareness training regarding social engineering techniques and preventive measures Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 **athicalacker** 1 year, 3 months ago

Selected Answer: D

Regular employee awareness training is crucial in combating social engineering attacks because many of these attacks rely on manipulating human behavior rather than exploiting technical vulnerabilities.

upvoted 2 times

 **qtygbapjpesdayazko** 1 year, 2 months ago

This is correct

upvoted 1 times

 **insaniunt** 1 year, 3 months ago

Selected Answer: D

D. Organize regular employee awareness training regarding social engineering techniques and preventive measures

upvoted 2 times

 **[Removed]** 1 year, 3 months ago

I'm unsure about the accuracy of this statement

upvoted 1 times

 **Spam_Protection** 1 year, 2 months ago

Instead of commenting this on every question. Help research or stfu.

upvoted 1 times

 **qtygbapjpesdayazko** 1 year, 2 months ago

do not spam and help with the question

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 149 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 149

Topic #: 1

[All 312-50v12 Questions]

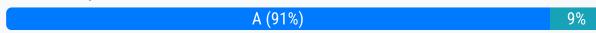
An audacious attacker is targeting a web server you oversee. He intends to perform a Slow HTTP POST attack, by manipulating 'a' HTTP connection. Each connection sends a byte of data every 'b' second, effectively holding up the connections for an extended period. Your server is designed to manage 'm' connections per second, but any connections exceeding this number tend to overwhelm the system. Given 'a=100' and variable 'm', along with the attacker's intention of maximizing the attack duration 'D=a*b', consider the following scenarios. Which is most likely to result in the longest duration of server unavailability?

- A. m=90, b=15: The server can manage 90 connections per second, but the attacker's 100 connections exceed this, and with each connection held up for 15 seconds, the attack duration could be significant. **Most Voted**
- B. m=105, b=12: The server can manage 105 connections per second, more than the attacker's 100 connections, likely maintaining operation despite a moderate hold-up time.
- C. m=110, b=20: Despite the attacker sending 100 connections, the server can handle 110 connections per second, therefore likely staying operative, regardless of the hold-up time per connection.
- D. m=95, b=10: Here, the server can handle 95 connections per second, but it falls short against the attacker's 100 connections, albeit the hold-up time per connection is lower.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution



by DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

agelbahri 8 months, 3 weeks ago

Selected Answer: A

M < A and time: $100 * 15 = 1500$

upvoted 1 times

shubhi6 11 months, 3 weeks ago

Selected Answer: A

B & C can be exclude right away as the value of "m" is greater than "a" so can easily manage those request.

Now coming to option D which has m = 95 if we calculate the duration it would $100 * 10 = 1000$ also logically it would hold for less time as compared to the value m=90 for this also duration would be $15 * 100 = 1500$, hence Answer is A.

Hope it make sense.

upvoted 1 times

blehbleh 1 year ago

Selected Answer: A

This A and I am not understanding what other people are not understanding of how to solve this question. The question at the end wants to know which one will result in the most down time or something along those lines I cant view it with this discussion pulled up. Regardless option A the attacks are longer or more then what the server can manage that is easily viewable and the attacks are 15 seconds in duration, so with the server not being able to handle all the requests and the 15 seconds it makes it the longest duration attack. I think most of the other options the server can manage the requests because the requests are less of that then which the server can handle. Just because a time is larger does not mean the server could not handle the amount of requests.

upvoted 1 times

LordXander 1 year, 8 months ago

Selected Answer: A

Guys...it's A...I know people used AI for this question however, upon further questioning about the math is literally highlighted that A is the correct answer (checked from multiple sources).

In question regarding tools/numbers, ask for details about each option and you will see yourself the correct answer
upvoted 4 times

✉️👤 **anarchyeagle** 1 year, 9 months ago

Selected Answer: C

Chatgpt answer:

a=1500 seconds
b=1200 seconds
c=2000 seconds
d=1000 seconds

upvoted 1 times

✉️👤 **brrbrr** 1 year, 9 months ago

chatgpt is wrong, you need to always double-check the answer. Correct answer is A.
upvoted 1 times

✉️👤 **Unr34l** 1 year, 9 months ago

A
You need to analice the variable m, if m is lower than the connections of the attacker, it overload
upvoted 1 times

✉️👤 **[Removed]** 1 year, 9 months ago

Could anyone verify the correctness of this answer
upvoted 1 times

✉️👤 **insaniunt** 1 year, 9 months ago

Selected Answer: A

I think: A. Because the attacker sends more connections than the server can handle, and each connection lasts for the longest time among the options. The attack duration is $D = 100 * 15 = 1500$ seconds, which is the highest possible value.
upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 151 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 151

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Recently, the employees of a company have been receiving emails that seem to be from their colleagues, but with suspicious attachments. When opened, these attachments appear to install malware on their systems. The IT department suspects that this is a targeted malware attack. Which of the following measures would be the most effective in preventing such attacks?

- A. Disabling Autorun functionality on all drives
- B. Avoiding the use of outdated web browsers and email software
- C. Regularly scan systems for any new files and examine them
- D. Applying the latest patches and updating software programs

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [LordXander](#) 1 year, 1 month ago

Selected Answer: D

Can confirm, is D based on CEHv12 1187

upvoted 2 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: D

The most effective measure to prevent such attacks is D. Applying the latest patches and updating software programs is essential to keep the systems secure and protected from known vulnerabilities that attackers can exploit.

upvoted 4 times

  [insaniunt](#) 1 year, 3 months ago

Module 07 Page 1187

upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 154 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 154

Topic #: 1

[All 312-50v12 Questions]

A penetration tester is performing an enumeration on a client's network. The tester has acquired permission to perform enumeration activities. They have identified a remote inter-process communication (IPC) share and are trying to collect more information about it. The tester decides to use a common enumeration technique to collect the desired data. Which of the following techniques would be most appropriate for this scenario?

- A. Probe the IPC share by attempting to brute force admin credentials **Most Voted**
- B. Brute force Active Directory
- C. Extract usernames using email IDs
- D. Conduct a DNS zone transfer

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **duke_of_kamulu**  1 year, 3 months ago

ANS A pg 401 During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC\$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents.

upvoted 6 times

 **cloufgangster**  1 year, 3 months ago

Selected Answer: A
The answer is A, i can only answer what i know. pg 401 CEH V12
upvoted 5 times

 **LordXander**  1 year, 2 months ago

Selected Answer: A
So, it is A...however is a very...barbarian way of doing it.

Under normal circumstances, without the handbook I would've gone for D since this is authorised and a I simply ask to do a DNS zone transfer. But then we have the page 401...and we know EC likes to have their most correct answer, so...A

upvoted 1 times

 **insaniunt** 1 year, 3 months ago

Selected Answer: A
A. Probe the IPC share by attempting to brute force admin credentials
upvoted 3 times

 **insaniunt** 1 year, 3 months ago

During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC\$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents
upvoted 5 times

 EXAM 312-50V12 TOPIC 1 QUESTION 157 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 157

Topic #: 1

[All 312-50v12 Questions]

You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions. Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest. However, they are unsure of how to securely manage and distribute the symmetric keys to users. Which of the following strategies would you recommend to them?

- A. Use hash functions to distribute the keys.
- B. Use HTTPS protocol for secure key transfer.
- C. Use digital signatures to encrypt the symmetric keys.
- D. Implement the Diffie-Hellman protocol for secure key exchange. Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [LordXander](#) 1 year, 2 months ago

Selected Answer: D

Matter of fact is that...the only reason I would pick D is because the others are not valid.

A - this is just a oneway process, so you cannot use it to decrypt the data later
B - it could be...but then we have the "symmetric keys"
C - is only used for data integrity validation
D - very plausible as it's purpose is for symmetric keys.

So...D

upvoted 2 times

  [qtygbapjpesdayazko](#) 1 year, 2 months ago

Selected Answer: D

Key word "distribute the symmetric keys to users"

upvoted 1 times

  [brrbrr](#) 1 year, 3 months ago

Selected Answer: D

D is the right answer.

upvoted 2 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: D

D. Implement the Diffie-Hellman protocol for secure key exchange.

upvoted 4 times

  [multivolt](#) 1 year, 3 months ago

I'm unsure about the accuracy of this statement

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 159 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 159

Topic #: 1

[All 312-50v12 Questions]

A certified ethical hacker is conducting a Whois footprinting activity on a specific domain. The individual is leveraging various tools such as Batch IP Converter and Whois Analyzer Pro to retrieve vital details but is unable to gather complete Whois information from the registrar for a particular set of data. As the hacker, what might be the probable data model being utilized by the domain's registrar for storing and looking up Whois information?

- A. Thin Whois model working correctly **Most Voted**
- B. Thin Whois model with a malfunctioning server
- C. Thick Whois model with a malfunctioning server
- D. Thick Whois model working correctly

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (91%) 9%

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **Aalkinani** 4 months, 1 week ago

Selected Answer: C

Option	Model Type	Behavior	Fits Scenario?
A	Thin	Points to registrar who holds full info	 No, because the hacker couldn't retrieve info even after that
C	Thick	Registry holds all info; if broken, nothing can be retrieved	 Yes, perfectly fits the failure to get full data
upvoted 1 times

 **medithaperera** 1 year, 2 months ago

I is A " unable to gather complete Whois information" means it is a Thin Whois model working correctly Mos
upvoted 1 times

 **prasoonmk** 1 year, 5 months ago

Selected Answer: A
What is a Thin WHOIS lookup?

A thin WHOIS lookup provides limited technical data from the registry which would include identifying the sponsoring registrar, the status of the domain, along with the creation and expiration dates. The remaining data, that being the contact details, are stored directly at the holding registrar(OpenSRS). Examples of this would be .COM and .NET, which soon will be moving to thick WHOIS as per the articles above at ICANN.
What is a Thick WHOIS lookup?

A thick WHOIS lookup contains all the technical data with the registry, as such administrative and technical, owner contact details. In addition, the sponsoring registrar and registration status. With data handled directly at the registry level and not the registrar, there are limitations and restrictions to how the "domain lock" works, while making changes to contact details.

upvoted 1 times

 **LordXander** 1 year, 8 months ago

Selected Answer: A
It is actually A because the limited information is part of thin WHOIS
upvoted 2 times

 **qtygbapjpesdayazko** 1 year, 8 months ago

Selected Answer: A
Keyword "unable to gather complete Whois" Thin Whois model working correctly

upvoted 1 times

✉ **brrbrr** 1 year, 9 months ago

- Selected Answer: A**
- Thick WHOIS: information from all registrars for the specified set of data.
 - Thin WHOIS: limited information about the specified set of data.
- upvoted 2 times

✉ **duke_of_kamulu** 1 year, 9 months ago

A is the Answer

upvoted 1 times

✉ **duke_of_kamulu** 1 year, 9 months ago

pg 216 Thin Whois - Stores only the name of the Whois server of the registrar of a domain, which in turn holds complete details on the data being looked up.

upvoted 2 times

✉ **duke_of_kamulu** 1 year, 9 months ago

A Thin WHOIS lookup provides limited technical data from the registry

upvoted 1 times

✉ **insaniunt** 1 year, 9 months ago

Selected Answer: A

A. Thin Whois model working correctly

Thin Whois - Stores only the name of the Whois server of the registrar of a domain, which in turn holds complete details on the data being looked up.

upvoted 2 times

✉ **qwerty100** 1 year, 9 months ago

Selected Answer: A

I think it's : A. Thin Whois model working correctly

<https://domaincoco.com/thin-vs-thick-registry-whois>

upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 160 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 160

Topic #: 1

[All 312-50v12 Questions]

You are a cybersecurity professional managing cryptographic systems for a global corporation. The company uses a mix of Elliptic Curve Cryptography (ECC) for key exchange and symmetric encryption algorithms for data encryption. The time complexity of ECC key pair generation is $O(n^3)$, where 'n' is the size of the key. An advanced threat actor group has a quantum computer that can potentially break ECC with a time complexity of $O((\log n)^2)$. Given that the ECC key size is 'n=512' and varying symmetric encryption algorithms and key sizes, which scenario would provide the best balance of security and performance?

- A. Data encryption with AES-128: Provides moderate security and fast encryption, offering a balance between the two.
- B. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes. **Most Voted**
- C. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to 3DES's inherent inefficiencies.
- D. Data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

✉ milktea810182 1 year ago

Selected Answer: B

While AES-128 (Option A) does provide moderate security and fast encryption, its key size might be susceptible to potential advancements in computing power, including quantum computing. On the other hand, AES-256 offers a higher level of security due to its larger key size, making it more resistant to attacks, including those from quantum computers. Additionally, AES-256 still maintains reasonable performance, making it a suitable choice for data encryption in this scenario.

upvoted 1 times

✉ LordXander 1 year, 2 months ago

Selected Answer: B

I would go by elimination:
A - well, EC says at least 168/256
B - could be, as it respects the requirement of 168/256
C - improves the security but slower than AES256
D - a lot of security, no so much speed.

So the option would be B which checks with the handbook (3300 - 3500) and also with the AI

upvoted 1 times

✉ qtygbapjpesdayazko 1 year, 2 months ago

Selected Answer: A

Keyword "best balance of security and performance", AES-128 will do. <https://www.ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/>
upvoted 1 times

✉ qtygbapjpesdayazko 1 year, 2 months ago

Selected Answer: B

B. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.
upvoted 1 times

✉ Folken 1 year, 2 months ago

Selected Answer: B

Module 20, page 3460

Counter mesure of crypto atk : key size of 168/256 is preffered

upvoted 1 times

✉️ **dobarb** 1 year, 2 months ago

Answer B.

ECC 512 is RSA 15360 as key size. The smaller key/faster encryption. It askes about best balance security and performance. CEH page 3355

upvoted 1 times

✉️ **multivolt** 1 year, 3 months ago

Hey friends can we make sure this is correct

upvoted 1 times

✉️ **insaniunt** 1 year, 3 months ago

Selected Answer: B

B. Data encryption with AES-256: Provides high security with better performance than 3DES, and while it may not be as fast as some other AES key sizes, it offers a good compromise between security and performance

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 161 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 161

Topic #: 1

[\[All 312-50v12 Questions\]](#)

You are a security analyst for CloudSec, a company providing cloud security solutions. One of your clients, a financial institution, wants to shift its operations to a public cloud while maintaining a high level of security control. They want to ensure that they can monitor all their cloud resources continuously and receive real-time alerts about potential security threats. They also want to enforce their security policies consistently across all cloud workloads. Which of the following solutions would best meet these requirements?

- A. Implement a Virtual Private Network (VPN) for secure data transmission.
- B. Deploy a Cloud Access Security Broker (CASB). Most Voted
- C. Use multi-factor authentication for all cloud user accounts.
- D. Use client-side encryption for all stored data.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  **LordXander** 1 year, 2 months ago

Well, EC says CASB as posted by the colleague.

However, by elimination:

- A - doesn't provide the require information such as cloud resource monitor
 - B - does everything needed
 - C - again, doesn;t provide any sort of alert besides failed auth and no logging for resouces
 - D - again, resource management and alerts
- upvoted 2 times

  **multivolt** 1 year, 3 months ago

Hey team can we double-check this response

upvoted 1 times

  **insaniunt** 1 year, 3 months ago

Selected Answer: B

B. Deploy a Cloud Access Security Broker (CASB).

- module 19 page 3305 from ceh v12 book

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 167 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 167

Topic #: 1

[All 312-50v12 Questions]

A certified ethical hacker is carrying out an email footprinting exercise on a targeted organization using eMailTrackerPro. They want to map out detailed information about the recipient's activities after receiving the email. Which among the following pieces of information would NOT be directly obtained from eMailTrackerPro during this exercise?

- A. Geolocation of the recipient
- B. Type of device used to open the email
- C. The email accounts related to the domain of the organization Most Voted
- D. The time recipient spent reading the email

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

✉ **Aalkinani** 4 months, 1 week ago

Selected Answer: D

Answer D. The amount of time the recipient spent reading the email:

Information on the exact amount of time spent reading an email is usually not directly available through tools such as eMailTrackerPro. This type of detailed user interaction data may require more sophisticated tracking that monitors activity time in email content, which is usually beyond the capabilities of standard email tracking tools.

upvoted 1 times

✉ **e8bf1bd** 1 year, 4 months ago

Answer D. The amount of time the recipient spent reading the email:

Information on the exact amount of time spent reading an email is usually not directly available through tools such as eMailTrackerPro. This type of detailed user interaction data may require more sophisticated tracking that monitors activity time in email content, which is usually beyond the capabilities of standard email tracking tools.

upvoted 2 times

✉ **xavi79** 1 year, 6 months ago

C is correct Answer based on chatgpt

upvoted 1 times

✉ **LordXander** 1 year, 8 months ago

Selected Answer: C

Seems like C because it would be weird to be B...like common

And the EC handbooks says the same, but again common sense

upvoted 1 times

✉ **Spam_Protection** 1 year, 8 months ago

Selected Answer: C

Its C, Module 2 P141-142 on the digital book

upvoted 1 times

✉ **The_Lucifer** 1 year, 9 months ago

Selected Answer: C

pg 208-209

geolocation, device type, read duration

upvoted 2 times

✉️ **brrbrr** 1 year, 9 months ago

Selected Answer: C

C. The email accounts related to the domain of the organization.

While eMailTrackerPro may provide information about the geolocation of the recipient, the type of device used to open the email, and the time spent reading the email, it is less likely to directly provide details about email accounts related to the domain of the organization. This type of information may require additional reconnaissance and investigation using other tools or techniques.

upvoted 2 times

✉️ **qtygbapjpesdayazko** 1 year, 9 months ago

This is the way

upvoted 1 times

✉️ **hughnguyen** 1 year, 6 months ago

sounds like a chatgpt answer

upvoted 1 times

✉️ **przemyslaw1** 1 year, 9 months ago

Selected Answer: C

Information about the victim gathered using email tracking tools includes:

- Recipient's System IP address
- Geolocation
- Email Received and Read
- Read Duration
- Proxy Detection
- Links
- Operating System and Browser information
- Forward Email
- Device Type
- Path Travelled

upvoted 3 times

✉️ **insaniunt** 1 year, 9 months ago

Selected Answer: B

eMailTrackerPro can provide information such as geolocation, time spent reading the email, and other details. However, it may not directly provide information about the type of device used to open the email or the email accounts related to the domain of the organization...

idk, I think:

B. Type of device used to open the email

upvoted 1 times

✉️ **athicalacker** 1 year, 9 months ago

Not correct. Answer is C.

Point from the CEH textbook:

- Device Type: Provides information about the type of device used to open and read the email, e.g., desktop computer, mobile device, or laptop.
- Pg. 209

upvoted 1 times

✉️ **xbsumz** 1 year, 9 months ago

Hey ethical hacking team can we double-check this method

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 170 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 170

Topic #: 1

[All 312-50v12 Questions]

A large organization is investigating a possible identity theft case where an attacker has created a new identity by combining multiple pieces of information from different victims to open a new bank account. The attacker also managed to receive government benefits using a fraudulent identity. Given the circumstances, which type of identity theft is the organization dealing with?

- A. Identity Cloning and Concealment
- B. Child Identity Theft
- C. Social Identity Theft
- D. Synthetic Identity Theft Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [insaniunt](#) Highly Voted 1 year, 3 months ago

Selected Answer: D

D - Synthetic Identity Theft

This is one of the most sophisticated types of identity theft, where the perpetrator obtains information from different victims to create a new identity. Firstly, he steals a Social Security Number and uses it with a combination of fake names, date of birth, address, and other details required for creating a new identity. The perpetrator uses this new identity to open new accounts, loans, credit cards, phones, other goods, and services (Module 09 Page 1385)

upvoted 5 times

  [Spam_Protection](#) Most Recent 1 year, 2 months ago

Selected Answer: D

Its syn, you made a person using info from various sources.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 176 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 176

Topic #: 1

[All 312-50v12 Questions]

In an advanced digital security scenario, a multinational enterprise is being targeted with a complex series of assaults aimed to disrupt operations, manipulate data integrity, and cause serious financial damage. As the Lead Cybersecurity Analyst with CEH and CISSP certifications, your responsibility is to correctly identify the specific type of attack based on the following indicators:

The attacks are exploiting a vulnerability in the target system's hardware, inducing misprediction of future instructions in a program's control flow. The attackers are strategically inducing the victim process to speculatively execute instructions sequences that would not have been executed in the absence of the misprediction, leading to subtle side effects. These side effects, which are observable from the shared state, are then utilized to infer the values of in-flight data.

What type of attack best describes this scenario?

A. Rowhammer Attack

B. Watering Hole Attack

C. Side-Channel Attack Most Voted

D. Privilege Escalation Attack

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (75%)

A (25%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **insaniunt** Highly Voted 1 year, 9 months ago

Selected Answer: C

C. Side-Channel Attack

In this context, the attackers are exploiting a vulnerability in the target system's hardware to observe and infer information based on side-channel information. The side-channel information, in this case, is derived from subtle side effects caused by speculatively executed instructions and mispredictions in the program's control flow.

upvoted 5 times

 **Mos3ab** Most Recent 9 months, 2 weeks ago

Selected Answer: C

Explanation:

The scenario describes an attack that exploits vulnerabilities in hardware by manipulating speculative execution and observing subtle side effects in shared state to infer sensitive data. This is characteristic of a side-channel attack, specifically a speculative execution attack such as Spectre or Meltdown.

upvoted 1 times

 **yicx1** 1 year, 5 months ago

Selected Answer: A

- A: take advantage of side effect in DRAM hardware design
- B: induce victim to visit a malicious site
- C: gather extra information (such as timing information or power consumption), rather than directly exploit the target victim
- D: upgrade privilege to gain more access

So the answer should be A.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 178 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 178

Topic #: 1

[\[All 312-50v12 Questions\]](#)

In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings on a web server considered a security risk, and what would be the best initial step to mitigate this risk?

- A. Default settings allow unlimited login attempts; setup account lockout
- B. Default settings reveal server software type; change these settings Most Voted
- C. Default settings cause server malfunctions; simplify the settings
- D. Default settings enable auto-updates; disable and manually patch

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [LordXander](#) 1 year, 1 month ago

Selected Answer: B

B - because think of a default php.ini, mysql.conf and so on
upvoted 1 times

  [ryotan](#) 1 year, 3 months ago

Why A was incorrect?
upvoted 2 times

  [brrbrr](#) 1 year, 3 months ago

Option A suggests addressing the risk associated with default server settings by implementing an account lockout mechanism for unlimited login attempts. While implementing account lockout is a good security practice to protect against brute-force attacks, it may not directly address the broader issue of default settings on a web server.
upvoted 3 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: B

The best initial step to mitigate this risk is to:

B. Default settings reveal server software type; change these settings
upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 179 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 179

Topic #: 1

[All 312-50v12 Questions]

As a junior security analyst for a small business, you are tasked with setting up the company's first wireless network. The company wants to ensure the network is secure from potential attacks. Given that the company's workforce is relatively small and the need for simplicity in managing network security, which of the following measures would you consider a priority to protect the network?

- A. Hide the network SSID
- B. Enable WPA2 or WPA3 encryption on the wireless router Most Voted
- C. Implement a MAC address whitelist
- D. Establish a regular schedule for changing the network password

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [e020fdc](#) 6 months, 2 weeks ago

Selected Answer: B

B - enable encryption.

A - Hiding SSID is just annoying for the workers but doesn't protect the network.

C - MAC address filtering is more work, not simple to manage like the question asks.

D - Sure, you can change the passwords, but that doesn't offer the same level of protection as encryption. It is also a cumbersome task to do and have every device login with new password.

B is the way

upvoted 1 times

 [LordXander](#) 1 year, 1 month ago

Selected Answer: B

B because WPA3

upvoted 1 times

 [insaniunt](#) 1 year, 3 months ago

Selected Answer: B

B. Enable WPA2 or WPA3 encryption on the wireless router

upvoted 4 times

 EXAM 312-50V12 TOPIC 1 QUESTION 180 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 180

Topic #: 1

[All 312-50v12 Questions]

During a reconnaissance mission, an ethical hacker uses Maltego, a popular footprinting tool, to collect information about a target organization. The information includes the target's Internet infrastructure details (domains, DNS names, Netblocks, IP address information). The hacker decides to use social engineering techniques to gain further information. Which of the following would be the least likely method of social engineering to yield beneficial information based on the data collected?

- A. Dumpster diving in the target company's trash bins for valuable printouts
- B. Impersonating an ISP technical support agent to trick the target into providing further network details
- C. Shoulder surfing to observe sensitive credentials input on the target's computers Most Voted
- D. Eavesdropping on internal corporate conversations to understand key topics

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (50%) B (38%) 13%

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

  **Mos3ab** 9 months, 2 weeks ago

Selected Answer: C

During footprinting, the ethical hacker gathered technical information such as domains, DNS names, IP addresses, and Netblocks. This type of data is mostly network-related and does not directly involve user credentials or physical access. Social engineering is then used to gather additional information.

upvoted 1 times

  **94578de** 1 year, 5 months ago

Selected Answer: C

The correct answer is C because to perform shoulder surfing you have to be in the facility and stay behind an employee's shoulder
upvoted 2 times

  **LordXander** 1 year, 8 months ago

Selected Answer: A

Well, B is definitely not correct for one single reason: you already have the IP, so you know who the ISP is and you could definitely get some info.

C&D are more effective when you already have some information mapped...however quite questionable when you only have some IPs.

A...for A you don't need any prerequisites hence it makes a lot of sense to be A.

upvoted 1 times

  **qwerty100** 1 year, 9 months ago

Selected Answer: C

C. Shoulder surfing to observe sensitive credentials input on the target's computers

upvoted 1 times

  **insaniunt** 1 year, 9 months ago

Selected Answer: B

B. Impersonating an ISP technical support agent to trick the target into providing further network details

upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 181 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 181

Topic #: 1

[All 312-50v12 Questions]

An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the following tools would be the best choice for this purpose and why?

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files

Most Voted

B. Koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware

C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (80%)

D (20%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **LordXander** 1 year, 1 month ago

Selected Answer: A

A makes more sense for this specific case
upvoted 1 times

 **qtygbapjpjesdayazko** 1 year, 2 months ago

Selected Answer: A

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files
Is in the book
upvoted 1 times

 **brrbrr** 1 year, 3 months ago

Selected Answer: D

The most suitable tool for generating YARA rules, complementing the Snort rules, and reinforcing the intrusion detection process, based on the given options, would be:

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files.

AutoYara is designed to automate the generation of YARA rules by analyzing both malicious and benign files. It facilitates the creation of YARA rules based on patterns and characteristics found in the files, helping to identify and detect similar patterns in other files. This tool can be valuable for enhancing the rule-based approach of an Intrusion Detection System (IDS) by generating rules that are specific to the organization's threat landscape.

While other tools mentioned (yarGen, Koodous, YaraRET) also have their specific use cases, AutoYara is more aligned with the objective of automatically generating YARA rules from both malicious and benign files, which can be particularly useful for a comprehensive intrusion detection strategy.

upvoted 1 times

 **Lalo** 1 year, 2 months ago

Answer A

The choice between YARGen and AutoYARA depends on your specific use case and requirements. If your primary focus is on generating YARA rules specifically for malware samples, YARGen may be the better choice. However, if you need a more versatile tool that can generate rules

from various input sources and provide greater customization options, AutoYARA might be more suitable. Consider evaluating both tools based on your needs and preferences to determine which one best complements your Snort deployment.

upvoted 1 times

 **Lalo** 1 year, 2 months ago

In this case, the scenario is that the "best rule-based approach" is selected and not a flexible, customizable tool.

upvoted 1 times

 **insaniunt** 1 year, 3 months ago

Selected Answer: A

yarGen

yarGen is used for generating YARA rules from strings identified in malware files while removing all strings that also appear in goodware files

upvoted 1 times

 **insaniunt** 1 year, 3 months ago

Module 12 Page 1642

upvoted 4 times

 **qtygbapipesdayazko** 1 year, 2 months ago

this is the day

upvoted 1 times

 **qwerty100** 1 year, 3 months ago

Selected Answer: A

It's A

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files

A. yarGen: Generates YARA rules from malware and goodware strings to aid in malware detection.

B. Koodous: A collaborative platform for Android malware analysis and community-driven threat intelligence.

C. YaraRET: A tool for forensic analysis and reverse engineering, searching for patterns with YARA rules.

D. AutoYara: Automates YARA rule generation from malware samples for efficient threat detection.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 184 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 184

Topic #: 1

[All 312-50v12 Questions]

Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (CHDB) with an emphasis on VPN footprinting. Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

- A. location: This operator finds information for a specific location **Most Voted**
- B. inurl: This operator restricts the results to only the pages containing the specified word in the URL
- C. link: This operator searches websites or pages that contain links to the specified website or page
- D. intitle: This operator restricts results to only the pages containing the specified term in the title

Hide Answer

Suggested Answer: A

Community vote distribution

A (80%) C (20%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **prasoonmk** 1 year, 3 months ago

Selected Answer: A

The location: operator is the least useful in providing the attacker with sensitive VPN-related information, because it does not directly relate to VPN configuration, credentials, or vulnerabilities. The location: operator finds information for a specific location, such as a city, country, or region. For example, location:paris would return results related to Paris, France.

The intitle: operator restricts results to only the pages containing the specified term in the title. For example, intitle:vpn would return pages with VPN in their title, which may include VPN guides, manuals, or tutorials. The inurl: operator restricts the results to only the pages containing the specified word in the URL. For example, inurl:vpn would return pages with VPN in their URL, which may include VPN login portals, configuration files, or directories. The link: operator searches websites or pages that contain links to the specified website or page. For example, link:vpn.com would return pages that link to vpn.com, which may include VPN reviews, comparisons, or recommendations. Reference:

upvoted 2 times

 **LoveBug4** 1 year, 5 months ago

Selected Answer: C

We can use "location" to filter VPNs from a particular country

upvoted 1 times

 **LordXander** 1 year, 8 months ago

Selected Answer: A

It's A because D is the best and others make some sense

upvoted 1 times

 **DruSuperman** 1 year, 8 months ago

Selected Answer: A

I don't see location on the list in the book.

upvoted 1 times

 **LeongCC** 1 year, 9 months ago

Selected Answer: A

For this question , the A is more suitable.

upvoted 1 times

👤 **Lalo** 1 year, 8 months ago

ANSWER CCCCCCCCCCCCLLLLLLCCCCCCCC

If we are interested in finding VPNs based in the United States, we use:

site:*.com intitle:"VPN" location:"United States"

a dork that uses the location operator

However, the "link" operator would not be the most suitable option to directly search for VPN-related websites. It is more useful to use dorks that focus on the content of web pages.

upvoted 1 times

👤 **brrbrr** 1 year, 9 months ago

Selected Answer: C

C. link: This operator searches websites or pages that contain links to the specified website or page.

The "link:" operator is generally used to find pages that link to a specific website or page. It helps identify sites that reference or link to a given URL. While it might reveal some information about the online presence of a target, it is less likely to directly provide sensitive VPN-related information.

On the other hand, the other options (A, B, D) can potentially yield information related to VPNs:

A. location: This operator could be used to find information for a specific location, which might include details about VPN servers or network infrastructure in that location.

B. inurl: This operator restricts results to pages containing the specified word in the URL. Attackers might use this to identify pages with VPN-related keywords in the URL.

D. intitle: This operator restricts results to pages containing the specified term in the title. It can be used to find pages with titles indicating VPN-related content.

upvoted 1 times

👤 **duke_of_kamulu** 1 year, 8 months ago

you are very wrong answer is A location check courseware page 120 very clear on VPN hacking

upvoted 1 times

👤 **LoveBug4** 1 year, 5 months ago

I couldn't find "link" in that page. We can use "location" to search VPN from a specific location.

upvoted 1 times

👤 **qwerty100** 1 year, 9 months ago

Selected Answer: A

A. Location

The "location" operator in a Google search is used to refine search results based on a specific geographic location. By including this operator in a search query, users can prioritize or limit results to those that are more relevant to a particular city, region, or country. This is particularly useful for finding local news, businesses, services, or events.

upvoted 1 times

👤 **insaniunt** 1 year, 9 months ago

Selected Answer: A

A. Location: This operator finds information for a specific location. While it may be useful for other purposes, it is not directly related to sensitive information about VPNs.

upvoted 2 times

👤 **insaniunt** 1 year, 9 months ago

Module 02 Page 120

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 185 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 185

Topic #: 1

[\[All 312-50v12 Questions\]](#)

In a recent cyber-attack against a large corporation, an unknown adversary compromised the network and began escalating privileges and lateral movement. The security team identified that the adversary used a sophisticated set of techniques, specifically targeting zero-day vulnerabilities. As a Certified Ethical Hacker (CEH) hired to understand this attack and propose preventive measures, which of the following actions will be most crucial for your initial analysis?

- A. Identifying the specific tools used by the adversary for privilege escalation.
- B. Analyzing the initial exploitation methods, the adversary used. **Most Voted**
- C. Checking the persistence mechanisms used by the adversary in compromised systems.
- D. Investigating the data exfiltration methods used by the adversary.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  **brrbrr** 1 year, 3 months ago

Selected Answer: B

In the context of understanding and responding to a cyber-attack that involved zero-day vulnerabilities, the most crucial initial analysis would likely be:

B. Analyzing the initial exploitation methods the adversary used.

Understanding the initial exploitation methods is crucial because it provides insights into how the adversary gained access to the network.
upvoted 1 times

  **insaniunt** 1 year, 3 months ago

Selected Answer: B

B. Analyzing the initial exploitation methods, the adversary used.
upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 186 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 186

Topic #: 1

[All 312-50v12 Questions]

Jason, a certified ethical hacker, is hired by a major e-commerce company to evaluate their network's security. As part of his reconnaissance, Jason is trying to gain as much information as possible about the company's public-facing servers without arousing suspicion. His goal is to find potential points of entry and map out the network infrastructure for further examination. Which technique should Jason employ to gather this information without alerting the company's intrusion detection systems (IDS)?

- A. Jason should directly connect to each server and attempt to exploit known vulnerabilities.
- B. Jason should use passive reconnaissance techniques such as WHOIS lookups, NS lookups, and web research. **Most Voted**
- C. Jason should use a DNS zone transfer to gather information about the company's servers.
- D. Jason should perform a ping sweep to identify all the live hosts in the company's IP range.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **insaniunt** **Highly Voted** 1 year, 3 months ago

Selected Answer: B

B. Jason should use passive reconnaissance techniques such as WHOIS lookups, NS lookups, and web research.

Passive reconnaissance involves gathering information without directly interacting with the target system, minimizing the chances of detection by intrusion detection systems (IDS). WHOIS lookups, NS (Name Server) lookups, and web research are examples of passive techniques that provide valuable information about a company's public-facing servers, domain registration details, and other publicly available information without actively probing the systems.

upvoted 5 times

 **e020fdc** **Most Recent** 6 months, 2 weeks ago

Selected Answer: B

B is the only "quiet" answer. The others would all set off alarms.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 187 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 187

Topic #: 1

[All 312-50v12 Questions]

As the lead security engineer for a retail corporation, you are assessing the security of the wireless networks in the company's stores. One of your main concerns is the potential for "Wardriving" attacks, where attackers drive around with a Wi-Fi-enabled device to discover vulnerable wireless networks. Given the nature of the retail stores, you need to ensure that any security measures you implement do not interfere with customer experience, such as their ability to access in-store Wi-Fi. Taking into consideration these factors, which of the following would be the most suitable measure to mitigate the risk of Wardriving attacks?

- A. Limit the range of the store's wireless signals
- B. Implement MAC address filtering
- C. Disable SSID broadcasting
- D. Implement WPA3 encryption for the store's Wi-Fi network Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **insaniunt** Highly Voted  1 year, 3 months ago

Selected Answer: D

D. Implement WPA3 encryption for the store's Wi-Fi network

Implementing WPA3 encryption for the store's Wi-Fi network would be a suitable measure to mitigate the risk of Wardriving attacks. WPA3 is a robust security protocol that provides strong encryption and helps secure wireless communications. It ensures that even if an attacker is able to detect the Wi-Fi signals, the encrypted data transmitted over the network remains secure.

upvoted 5 times

 **e020fdc** Most Recent  6 months, 2 weeks ago

Selected Answer: D

This is the third question in the bank like this.

"How do you secure a WiFi network?"

(  ) Encrypt it

upvoted 1 times

 **qtygbapjpesdayzko** 1 year, 2 months ago

Selected Answer: D

D. Implement WPA3 encryption for the store's Wi-Fi network

B and C impact the customer, A is not effective or can impact also the customer.

D, we don't know if the SSID has a password, so it is the best option from the 4.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 188 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 188

Topic #: 1

[All 312-50v12 Questions]

A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?

- A. ICMP Timestamp Ping Scan
- B. ICMP ECHO Ping Scan
- C. TCP SYN Ping Scan
- D. UDP Ping Scan **Most Voted**

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

[insaniunt](#) **Highly Voted** 1 year, 9 months ago

Selected Answer: D

D. UDP Ping Scan

When dealing with strict TCP filtering rules on a firewall, a UDP Ping Scan can be an effective host discovery technique. Unlike ICMP or TCP SYN ping scans, UDP ping scans use UDP packets, which can sometimes bypass certain firewall restrictions.

upvoted 5 times

[insaniunt](#) 1 year, 9 months ago

module 3 page 286 from ceh v12 book

upvoted 4 times

[e020fdc](#) **Most Recent** 6 months, 2 weeks ago

Selected Answer: C

ChatGPT says C: In environments with strict TCP filtering rules on firewalls, traditional host discovery methods like ICMP pings are often blocked or ignored, making them unreliable for identifying live hosts. However, firewalls often allow traffic to certain TCP ports (e.g., port 80 for HTTP, 443 for HTTPS) to remain functional — and that's where a TCP SYN Ping Scan comes in.

TCP SYN Ping Scan (-PS in Nmap):

- Sends TCP SYN packets to specified ports (commonly allowed ones like 80, 443).
- If the host is alive and the port is open, it will respond with a SYN-ACK.
- Even if the port is closed, the host will send a RST, confirming it is up.
- Useful for bypassing ICMP and default ping blocking on firewalls.
- Faster and stealthier than full connection scans.

upvoted 1 times

[agelbahri](#) 8 months, 3 weeks ago

Selected Answer: A

strict TCP filtering rules on its firewall

upvoted 1 times

[7c4eac1](#) 1 year ago

Selected Answer: C

SYN packets are often permitted for legitimate connection attempts, making it an effective way to discover hosts in environments with restricted ICMP and UDP traffic.

upvoted 1 times

 **qtygbapjpesdayazko** 1 year, 8 months ago

Selected Answer: D

Is D.

Key word "strict TCP filtering rules on its firewall". so can not be ICMP and TCP related scans.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 189 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 189

Topic #: 1

[All 312-50v12 Questions]

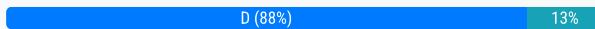
As part of a college project, you have set up a web server for hosting your team's application. Given your interest in cybersecurity, you have taken the lead in securing the server. You are aware that hackers often attempt to exploit server misconfigurations. Which of the following actions would best protect your web server from potential misconfiguration-based attacks?

- A. Regularly backing up server data
- B. Enabling multi-factor authentication for users
- C. Implementing a firewall to filter traffic
- D. Performing regular server configuration audits Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

[brrbrr](#) Highly Voted 1 year, 9 months ago

Selected Answer: D

While options like regularly backing up server data (option A), enabling multi-factor authentication (option B), and implementing a firewall to filter traffic (option C) are important security measures, they are not specifically focused on addressing misconfigurations. Regular configuration audits directly target the identification and correction of misconfigurations, making it a key practice for securing a web server against misconfiguration-based attacks.

upvoted 5 times

[asyik](#) Most Recent 1 year ago

Selected Answer: A

Backing up server data

upvoted 1 times

[insaniunt](#) 1 year, 9 months ago

Selected Answer: D

D. Performing regular server configuration audits

Performing regular server configuration audits is the best action to protect your web server from potential misconfiguration-based attacks. Regular audits involve reviewing and assessing the server configuration settings to identify any deviations from security best practices or unintended misconfigurations. This helps ensure that the server is configured securely and is less vulnerable to exploitation.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 192 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 192

Topic #: 1

[\[All 312-50v12 Questions\]](#)

A multinational organization has recently faced a severe information security breach. Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems. This knowledge was utilized to bypass security controls and corrupt valuable resources. Considering this event, the security team is contemplating the type of attack that occurred and the steps they could have taken to prevent it. Choose the most plausible type of attack and a countermeasure that the organization could have employed:

- A. Insider attacks and the organization should have implemented robust access control and monitoring. Most Voted
- B. Distribution attack and the organization could have ensured software and hardware integrity checks.
- C. Passive attack and the organization should have used encryption techniques.
- D. Active attack and the organization could have used network traffic analysis.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [e020fdc](#) 6 months, 1 week ago

Selected Answer: A

The know the layout and what is valuable. Sounds like an insider threat. Not much evidence given to support the other answers.
upvoted 1 times

 [GK2205](#) 1 year, 4 months ago

Selected Answer: A

The key to this question is in:
"Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems. This knowledge was utilized to bypass security controls and corrupt valuable resources"
Assumption: Encryption is part of security controls
Answer: A - Because only an insider can get to this level of understanding and access. (Acknowledging that there are some very good hacker out there, but one has to assume that that level of knowledge is very, very hard to gather externally).
upvoted 1 times

 [LordXander](#) 1 year, 8 months ago

Selected Answer: A

Everyone is saying A, and I'm inclined to agree, but we are talking about data corruption which in itself suggests lack of encryption.

Now, an insider threat could've used a passive attack for achieving its goal, hence it could be also C. My first thought of this was A, but thinking again, and again I can see C as plausible. In the exam I would've gone with A hence I will pick A
upvoted 1 times

 [DruSuperman](#) 1 year, 8 months ago

Selected Answer: A

Knowing internal processes, has to be A.
upvoted 1 times

 [ahmedalkibsy](#) 1 year, 9 months ago

A is correct
upvoted 1 times

 [anarchyeagle](#) 1 year, 9 months ago

Chat GPT:

Insider attacks occur when someone with authorized access to the organization's resources (an employee, contractor, or business partner) misuses their access to conduct malicious activities. The detailed knowledge of the organization's internal processes and systems, as described, suggests that the attacker was not an external party but rather someone with inside access or knowledge. Insider threats are challenging to detect because the attacker legitimately accesses the system, making their actions appear as normal activities.

upvoted 1 times

👤 **barey** 1 year, 9 months ago

GPT-4

A. Insider attacks and the organization should have implemented robust access control and monitoring.

The details of the breach indicating that the attacker had an in-depth understanding of the company's internal processes and systems suggest that this could have been an insider attack.

upvoted 1 times

👤 **LeongCC** 1 year, 9 months ago

Selected Answer: A

It's should be the A.

Already mentioned understanding of the organization's internal processes and systems.

upvoted 1 times

👤 **brrrrr** 1 year, 9 months ago

Selected Answer: A

Given that the attacker had a high degree of understanding of the organization's internal processes and systems, it suggests that the breach may have been facilitated by someone with insider knowledge or access.

upvoted 1 times

👤 **calx5** 1 year, 9 months ago

Selected Answer: A

Insider attacks, attacker with high degree of understanding

upvoted 1 times

👤 **insaniunt** 1 year, 9 months ago

Selected Answer: A

A. Insider attacks and the organization should have implemented robust access control and monitoring.

upvoted 1 times

👤 **JustAName** 1 year, 9 months ago

Should be A because "Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems." It is very likely that this attacker is within the organization, so insider threat.

upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 193 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 193

Topic #: 1

[\[All 312-50v12 Questions\]](#)

As a security analyst for SkySecure Inc., you are working with a client that uses a multi-cloud strategy, utilizing services from several cloud providers. The client wants to implement a system that will provide unified security management across all their cloud platforms. They need a solution that allows them to consistently enforce security policies, identify and respond to threats, and maintain visibility of all their cloud resources. Which of the following should you recommend as the best solution?

- A. Use a Cloud Access Security Broker (CASB). Most Voted
- B. Use a hardware-based firewall to secure all cloud resources.
- C. Implement separate security management tools for each cloud platform.
- D. Rely on the built-in security features of each cloud platform.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [e020fdc](#) 6 months, 1 week ago

Selected Answer: A

CASB for sure. The others are the opposite of what the client wants.

upvoted 1 times

  [LordXander](#) 1 year, 1 month ago

Selected Answer: A

The only one that makes sense

upvoted 1 times

  [duke_of_kamulu](#) 1 year, 3 months ago

NO 2ways about it CASB

upvoted 1 times

  [qwerty100](#) 1 year, 3 months ago

Selected Answer: A

A. Use a Cloud Access Security Broker (CASB).

upvoted 3 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: A

A. Use a Cloud Access Security Broker (CASB).

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 195 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 195

Topic #: 1

[All 312-50v12 Questions]

A Certified Ethical Hacker (CEH) is analyzing a target network. To do this, he decides to utilize an IDLE/IPID header scan using Nmap. The network analysis reveals that the IPID number increases by 2 after following the steps of an IDLE scan. Based on this information, what can the CEH conclude about the target network?

- A. The ports on the target network are open **Most Voted**
- B. The target network has no firewall present
- C. The ports on the target network are closed
- D. The target network has a stateful firewall present

[Hide Answer](#)

Suggested Answer: A

Community vote distribution



by [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

[insaniunt](#) **Highly Voted** 1 year, 9 months ago

Selected Answer: A

Ok, I saw the ceh v12 book: Consequently, the IPID is increased by 2, which implies that the port on the target machine was open." - page 317
upvoted 6 times

[agelbahri](#) **Most Recent** 8 months, 3 weeks ago

Selected Answer: A

because of (after following the steps of an IDLE scan) which means using zompi
upvoted 1 times

[GK2205](#) 1 year, 4 months ago

Selected Answer: D

While A and D have merits, there is no mention of the use of a Zombie system to perform the testing, one has to assume the IDLE/IPID is being sent direct (Trusted CEH). Therefore the result (Which excludes the IPID incrementation of the Zombie)
is the response of a Stateful Firewall.
upvoted 1 times

[milktea810182](#) 1 year, 6 months ago

Selected Answer: D

Stateful firewalls maintain information about the state of active connections, including the IPID sequence numbers. When Nmap sends probes to closed ports, the firewall generates ICMP error messages in response to those probes. These ICMP error messages trigger changes in the IPID sequence number, causing it to increase by 2 for each probe. This behavior is a result of the firewall's response mechanism, indicating the presence of a stateful firewall on the target network.

Therefore, the correct conclusion the CEH can draw about the target network based on the observed behavior is that the target network has a stateful firewall present.
upvoted 1 times

[LordXander](#) 1 year, 8 months ago

Selected Answer: A

I would go with A as the documentation for Module 3, page 317 (not 217) says that. Also, reading the nmap documentation suggested A with some further insights in why it could be D
upvoted 1 times

[Spam_Protection](#) 1 year, 8 months ago

Selected Answer: A

Module 3 Page 217

Send a SYN+ACK packet to the zombie, and it responds with an RST packet containing the IPID. Assuming that the port on the target was open and that the zombie has already sent an RST packet to the target, the IPID number is increased by 1. Now, the zombie responds with an RST packet to the attacker using its next IPID, i.e., 31339 (X + 2). Consequently, the IPID is increased by 2, which implies that the port on the target machine was open. Thus, using an idle scan, an attacker can identify the open ports and services on the target machine by spoofing their IP address with a zombie's IP address.

upvoted 1 times

 **brrbrr** 1 year, 9 months ago

Selected Answer: D

The IDLE/IPID header scan is a technique used to identify the presence of a stateful firewall. In this scan, if the IPID number increases by 2 for each successive probe, it indicates that the system is using a stateful firewall.

upvoted 2 times

 **przemyslaw1** 1 year, 9 months ago

Selected Answer: A

An IPID increased by 2 will indicate an open port, whereas an IPID increased by 1 will indicate a closed port

upvoted 2 times

 **insaniunt** 1 year, 9 months ago

Selected Answer: D

D. The target network has a stateful firewall present

In an IDLE/IPID header scan using Nmap, the scanning technique relies on the behavior of the IPID (IP Identification) field in IP headers. In a normal scan, the IPID field typically increments by 1 for each packet sent. However, in the presence of a stateful firewall that performs packet normalization, the IPID might increase by a different value.

If the IPID number increases by 2 after performing the IDLE/IPID header scan, it suggests that the target network has a stateful firewall present. This behavior occurs because the firewall is manipulating the IPID field in a way that deviates from the normal incrementation observed in the absence of such a firewall.

upvoted 1 times

 **qwerty100** 1 year, 9 months ago

A. The ports on the target network are open

<https://nmap.org/book/idlescan.html>

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 197 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 197

Topic #: 1

[All 312-50v12 Questions]

An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?

A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing

Most Voted

B. Implementing sophisticated matches such as "OR john' = 'john" in place of classical matches like "OR 1=1"

C. Manipulating white spaces in SQL queries to bypass signature detection

D. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (64%)

C (27%)

9%

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **e020fdc** 6 months, 1 week ago

Selected Answer: A

I think A and so does ChatGPT. Here's why:

Using functions like CHAR() (in SQL Server) or equivalents like CHR() (in Oracle) to construct strings from character codes (decimal or hexadecimal) is a common and advanced evasion technique.

This bypasses literal string detection, since the payload isn't written out in a recognizable form.

Here's why the others were a no:

B. Implementing "OR john' = 'john": This is a known evasion but not particularly advanced. IDS systems often already detect variations of logical tautologies.

C. Manipulating white spaces: Basic evasion, and many signature-based IDS tools normalize input to detect this.

D. Using URL encoding: Another basic and well-known evasion. Modern IDS systems often decode input before analysis.

upvoted 1 times

 **ba1dd4b** 9 months, 1 week ago

Selected Answer: A

A, B, C and D. All of them. I think some questions have multiple answers. All choices are listed in Module 15, page 2322. A is the second in the list in thais page.

upvoted 1 times

 **LordXander** 1 year, 1 month ago

I would definitely say A.

B - boolean based SQL, is part of pretty much any decent IDS

C - plausible but personally, I saw that usage of custom characters might get it bypassed for a WAF.

D - is like A but you need something that can be read by SQL engine

upvoted 1 times

 **DIINESSH** 1 year, 1 month ago

Selected Answer: B

ChatGPT says : B. Implementing sophisticated matches such as "OR 'john'='john'" allows the hacker to bypass signature-based detection systems that may only be looking for classical SQL injection patterns like "OR 1=1". By using more complex and varied syntax, the hacker can evade detection.

upvoted 1 times

✉ **qtygbapjpesdayazko** 1 year, 2 months ago

Selected Answer: A

Utilizing the char encoding function to convert hexadecimal and decimal values into characters

upvoted 1 times

✉ **przemyslaw1** 1 year, 3 months ago

Selected Answer: A

A. Utilizing the char encoding...

upvoted 2 times

✉ **insaniunt** 1 year, 3 months ago

Selected Answer: A

Char Encoding: an attacker can encode a common injection variable present in the input string to avoid detection in the signature of network security measures. This char() function converts hexadecimal and decimal values into characters that can easily pass through SQL engine parsing. The char() function can be used for SQL injection into MySQL without double quotes - Module 15 Page 2324

upvoted 2 times

✉ **Nopez** 1 year, 3 months ago

Selected Answer: C

C. Manipulating white spaces in SQL queries to bypass signature detection

upvoted 3 times

✉ **Lalo** 1 year, 2 months ago

Answer AAAAAAAA

Since only a signature-based IDS system is used, the best form of attack would be to use the technique that is least likely to be detected by the IDS signatures. In this case, the most effective method would probably be to use the CHAR encoding function to convert hexadecimal and decimal values into characters that pass the SQL engine's analysis.

The main reason is that signature-based IDS systems tend to look for specific known patterns associated with known attacks. If the IDS is not configured to recognize CHAR encoding as an indicator of possible SQL injection, the attack is more likely to go undetected.

Additionally, whitespace manipulation in SQL queries might be more easily detected by the IDS if it is configured to look for unusual whitespace patterns in SQL queries.

Therefore, in this scenario, using the CHAR encoding feature would be the best option to evade IDS detection and succeed in the attack.

upvoted 2 times

✉ **xbsumz** 1 year, 3 months ago

I'm not certain about this ethical hacking concept

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 198 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 198

Topic #: 1

[All 312-50v12 Questions]

As the Chief Information Security Officer (CISO) at a large university, you are responsible for the security of a campus-wide Wi-Fi network that serves thousands of students, faculty, and staff. Recently, there has been a rise in reports of unauthorized network access, and you suspect that some users are sharing their login credentials. You are considering deploying an additional layer of security that could effectively mitigate this issue. What would be the most suitable measure to implement in this context?

- A. Implement network segmentation
- B. Deploy a VPN for the entire campus
- C. Enforce a policy of regularly changing Wi-Fi passwords
- D. Implement 802.1X authentication Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [LordXander](#) 1 year, 1 month ago

Selected Answer: D

As it is the only one that makes sense
upvoted 2 times

 [anarchyeagle](#) 1 year, 3 months ago

Selected Answer: D

Chat GPT:

Implement 802.1X authentication: 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. By implementing 802.1X, the university can enforce strong authentication methods that go beyond just a username and password, potentially incorporating certificates or a two-factor authentication system. This can significantly reduce the risk of unauthorized access due to credential sharing, as each user's device would need to be authenticated individually. It also allows for greater control over network access on a per-user basis, making it easier to manage access rights and monitor network usage.

upvoted 1 times

 [qwerty100](#) 1 year, 3 months ago

Selected Answer: D

D. Implement 802.1X authentication
upvoted 1 times

 [insaniunt](#) 1 year, 3 months ago

Selected Answer: D

D. Implement 802.1X authentication
upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 199 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 199

Topic #: 1

[\[All 312-50v12 Questions\]](#)

An ethical hacker is scanning a target network. They initiate a TCP connection by sending an SYN packet to a target machine and receiving a SYN/ACK packet in response. But instead of completing the three-way handshake with an ACK packet, they send an RST packet. What kind of scan is the ethical hacker likely performing and what is their goal?

- A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection. Most Voted
- B. They are performing a network scan to identify live hosts and their IP addresses.
- C. They are performing a TCP connect scan to identify open ports on the target machine.
- D. They are performing a vulnerability scan to identify any weaknesses in the target system.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [e020fdc](#) 6 months, 1 week ago

Selected Answer: A

A makes the most sense

upvoted 1 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: A

A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection.

upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 200 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 200

Topic #: 1

[\[All 312-50v12 Questions\]](#)

In the process of setting up a lab for malware analysis, a cybersecurity analyst is tasked to establish a secure environment using a sheep dip computer. The analyst must prepare the testbed while adhering to best practices. Which of the following steps should the analyst avoid when configuring the environment?

- A. Installing malware analysis tools on the guest OS
- B. Connecting the system to the production network during the malware analysis Most Voted
- C. Simulating Internet services using tools such as INetSim
- D. Installing multiple guest operating systems on the virtual machine(s)

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [e020fdc](#) 6 months, 1 week ago

Selected Answer: B

Now that I looked up what the heck "sheep dip computer" means, B makes the most sense for sure.

In IT security, a "sheep dip" computer refers to a dedicated system used to scan removable media (like USB drives) for malware before they are connected to other computers. It's essentially a safety net that minimizes the risk of introducing viruses or other malicious software into a network from external sources

upvoted 1 times

  [LordXander](#) 1 year, 1 month ago

Selected Answer: B

B - the only one that makes sense

But I would love to see a forensics lab connected to production :D

upvoted 2 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: B

B. Connecting the system to the production network during the malware analysis

When configuring a sheep dip computer for malware analysis, one should avoid connecting the system to the production network. The purpose of a sheep dip computer is to provide a controlled and isolated environment for analyzing potentially malicious software. Connecting it to the production network poses a significant security risk, as it could potentially expose the network to the analyzed malware or compromise the integrity of the production environment.

upvoted 4 times

EXAM 312-50V12 TOPIC 1 QUESTION 201 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 201

Topic #: 1

[All 312-50v12 Questions]

A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

- A. Inference-based assessment solution
- B. Tree-based assessment approach
- C. Product-based solution installed on a private network
- D. Service-based solution offered by an auditing firm **Most Voted**

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

✉ **e020fdc** 6 months, 1 week ago

Selected Answer: D

I D and so does ChatGPT because it does the most to meet the stated requirements. Why the others are not as suitable:

A. Inference-based assessment solution: While this mentions one key feature (inference-based testing), it doesn't address automation, attacker perspective, or multi-network support. It's a method, not a comprehensive solution.

B. Tree-based assessment approach: This is a structured decision-making or modeling technique, not a full-featured vulnerability assessment solution.

C. Product-based solution installed on a private network: This would provide an internal perspective, not mimicking the external attacker's view. It might not scale easily across multiple networks or reflect external threats as well as a service-based solution.

upvoted 1 times

✉ **AtuJay** 7 months, 3 weeks ago

Selected Answer: D

Page 558 v12

upvoted 1 times

✉ **LordXander** 1 year, 1 month ago

Selected Answer: D

I would have said A but the outside view pretty much says that it has to be a 3rd party

upvoted 1 times

✉ **sosindi** 1 year, 3 months ago

Service - based solution. - 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.

upvoted 1 times

✉ **przemyslaw1** 1 year, 3 months ago

Selected Answer: D

D. Service-based solution offered by an auditing firm

upvoted 1 times

 **brrbrr** 1 year, 3 months ago

Selected Answer: D

A service-based solution provided by an auditing firm often includes external vulnerability assessments that mimic the perspective of an outside attacker. These services typically involve experienced security professionals who perform thorough and well-organized testing, utilize continuously updated databases of vulnerabilities, and can adapt to multiple network environments
upvoted 1 times

 **insaniunt** 1 year, 3 months ago

Selected Answer: D

I was wrong...
D. Service-based solution offered by an auditing firm

A service-based solution offered by an auditing firm, especially if hosted outside the organization's network, can provide an external perspective that imitates the outside view of attackers. Auditing firms often perform well-organized inference-based testing, continuously update their databases with the latest threat intelligence, and can support assessments across multiple networks.

upvoted 2 times

 **insaniunt** 1 year, 3 months ago

Selected Answer: A

A. Inference-based assessment solution
upvoted 1 times

 **qwerty100** 1 year, 3 months ago

Selected Answer: D
I think it's D
(Module 05 Page 558)
D. Service-based solution offered by an auditing firm
upvoted 4 times

 **qtygbapjpesdayazko** 1 year, 2 months ago

This is the way.

Can not be "A. Inference-based" as the scan need to be done from outside, not from the inside the host.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 202 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 202

Topic #: 1

[\[All 312-50v12 Questions\]](#)

During a penetration testing assignment, a Certified Ethical Hacker (CEH) used a set of scanning tools to create a profile of the target organization. The CEH wanted to scan for live hosts, open ports, and services on a target network. He used Nmap for network inventory and Hping3 for network security auditing. However, he wanted to spoof IP addresses for anonymity during probing. Which command should the CEH use to perform this task?

- A. Hping3 -1 10.0.0.25 -ICMP
- B. Hping3 -2 10.0.0.25-p 80
- C. Nmap -sS -Pn -n -vv --packet-trace -p- --script discovery -T4
- D. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [e020fdc](#) 6 months, 1 week ago

Selected Answer: D

Chat GPT says D and breaks down the command:

-S: Sends a SYN packet (used in TCP port scanning)

192.168.1.1: Target IP address

-a 192.168.1.254: Spoofs the source IP address to appear as 192.168.1.254

-p 22: Target port (SSH in this case)

--flood: Sends packets as fast as possible, useful in stress testing or noisy scans
upvoted 1 times

 [e020fdc](#) 6 months, 1 week ago

Reasons why the others are not correct:

A. Hping3 -1 10.0.0.25 -ICMP

Uses ICMP (-1), but the -ICMP flag is invalid. Also, it does not spoof IP addresses.

B. Hping3 -2 10.0.0.25 -p 80

Uses UDP mode (-2) to port 80 (usually TCP), which is unusual and doesn't spoof IP addresses.

C. Nmap -sS -Pn -n -vv --packet-trace -p- --script discovery -T4

A detailed Nmap command for scanning all ports (-p-), disabling ping (-Pn), and including scripting. However, Nmap does not support IP spoofing in the same flexible way as Hping3. It can spoof MACs or perform decoy scans, but not raw IP spoofing like Hping3.
upvoted 1 times

 [qtygbapjpesdayazko](#) 1 year, 2 months ago

Is D-

"-a" is to spoof the IP 192.168.1.254

upvoted 2 times

 **JustAName** 1 year, 3 months ago

Selected Answer: D

D "--flood" syntax is used for sphttps://www.examtopics.com/exams/eccouncil/312-50v12/view/41/#oofing ip address when performing scans
upvoted 2 times

 **xbsumz** 1 year, 3 months ago

I'm a bit hesitant about the effectiveness of this CEH technique
upvoted 1 times

 **insaniunt** 1 year, 3 months ago

Selected Answer: D

D. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood
upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 205 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 205

Topic #: 1

[\[All 312-50v12 Questions\]](#)

As a cybersecurity consultant, you are working with a client who wants to migrate their data to a Software as a Service (SaaS) cloud environment. They are particularly concerned about maintaining the privacy of their sensitive data, even from the cloud service provider. Which of the following strategies would best ensure the privacy of their data in the SaaS environment?

- A. Implement a Virtual Private Network (VPN) for accessing the SaaS applications.
- B. Rely on the cloud service provider's built-in security features.
- C. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently. Most Voted**
- D. Use multi-factor authentication for all user accounts accessing the SaaS applications

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 **qwerty100** 1 year, 3 months ago

Selected Answer: C

C. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.

upvoted 1 times

 **Unr34l** 1 year, 3 months ago

C. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.

Encrypting the data client-side before uploading it to the SaaS environment and managing encryption keys independently provides an additional layer of security and privacy. This approach ensures that even if the data is stored in the cloud, it remains encrypted, and the client retains control over the encryption keys. This way, the cloud service provider has limited visibility into the actual content of the data, enhancing the privacy and security of sensitive information.

upvoted 3 times

 **xbsumz** 1 year, 3 months ago

Team can you confirm if this is accurate

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 206 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 206

Topic #: 1

[All 312-50v12 Questions]

An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure. During the scan, he discovers an active host with multiple open ports running various services. The hacker uses TCP communication flags to establish a connection with the host and starts communicating with it. He sends a SYN packet to a port on the host and receives a SYN/ACK packet back. He then sends an ACK packet for the received SYN/ACK packet, which triggers an open connection. Which of the following actions should the ethical hacker perform next?

- A. Send a PSH packet to inform the receiving application about the buffered data.
- B. Conduct a vulnerability scan on the open port to identify any potential weaknesses. Most Voted
- C. Scan another port on the same host using the SYN, ACK, and RST flags.
- D. Send a FIN or RST packet to close the connection.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

e020fdc 6 months, 1 week ago

Selected Answer: B

You're hired to assess the security of the network. If you've already connected to the port, have a look at what vulnerabilities are there. Scanning for them doesn't mean you'll exploit what you find. Gather notes on whatever is there and move on.

upvoted 1 times

agelbahri 8 months, 3 weeks ago

Selected Answer: B

B. Conduct a vulnerability scan on the open port to identify any potential weaknesses

upvoted 1 times

KalingaDev 11 months, 2 weeks ago

Selected Answer: B

Since this is an ethical hacking operation, the hacker should proceed with scanning for vulns. for those who chose 'D', this would be making since if this operation is being conducted illegally.

upvoted 1 times

blehbleh 12 months ago

Selected Answer: B

I'm pretty sure this is B as an ethical hacker you need to see if there are any vulnerabilities. You can't just tell them at the end of the pentest that they had open ports but without validation as to if it is a security concern or not. You would not be doing your job as the pentester. You would just be scanning a network without any knowledge of if anything is vulnerable or not.

upvoted 1 times

azdan 1 year, 2 months ago

Selected Answer: D

Keyword is the ethical hacker perform next.

upvoted 1 times

kevin403 1 year, 3 months ago

Selected Answer: D

Key sentence " An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure" his role here didn't mention anything about scanning for vuln nor having permission to do so. Hence he RST and move on.

Ethical hacking is all about getting the permission from the owner to do a specific task, in this case. Network scan only
upvoted 1 times

✉️ **GK2205** 1 year, 4 months ago

Selected Answer: D

Another one that is tricky because of nuance: The Ethical Hacker is performing a network scan and not necessarily a vulnerability scan. Network scans do not traverse into vulnerability scans although if required we would do so. The context of the question is key here IMHO. One thing is very clear throughout the program, as a CEH your job is to do no harm and not to compromise. i.e. When you gain access to a sensitive database you are to report on it, not enter and potentially exploit it. Similarly here, your scope is a network scan, not a vulnerability scan. So RST and move on.
upvoted 2 times

✉️ **Truth_Seeker** 1 year, 4 months ago

I think the correct answer is D

it is a common practice across various network scanning tools to ensure that connections are properly managed and closed. Therefore, the conclusion about closing connections with a FIN or RST packet after a scan is applicable to most network scanners, not just Nmap
upvoted 1 times

✉️ **MustafaDDD** 1 year, 9 months ago

Selected Answer: B

I am just thinking, the question says, "An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure", why would the hacker close the session?
upvoted 3 times

✉️ **qwerty100** 1 year, 9 months ago

Selected Answer: B

B. Conduct a vulnerability scan on the open port to identify any potential weaknesses.
upvoted 3 times

✉️ **qtygbapjpesdayazko** 1 year, 8 months ago

This is the way.

He starts the connection on the port, why do a reset? so scan the port for vulns.

upvoted 1 times

✉️ **qwerty100** 1 year, 9 months ago

B. Conduct a vulnerability scan on the open port to identify any potential weaknesses.
upvoted 3 times

✉️ **insaniunt** 1 year, 9 months ago

Selected Answer: D

D, I think
The ethical hacker must send a FIN or RST packet to terminate the connection
upvoted 2 times

✉️ **xbsumz** 1 year, 9 months ago

Could someone help me confirm the validity of this ethical hacking technique
upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 207 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 207

Topic #: 1

[\[All 312-50v12 Questions\]](#)

A multinational corporation's computer system was infiltrated by an advanced persistent threat (APT). During forensic analysis, it was discovered that the malware was utilizing a blend of two highly sophisticated techniques to stay undetected and continue its operations.

Firstly, the malware was embedding its harmful code into the actual binary or executable part of genuine system files rather than appending or prepending itself to the files. This made it exceptionally difficult to detect and eradicate, as doing so risked damaging the system files themselves.

Secondly, the malware exhibited characteristics of a type of malware that changes its code as it propagates, making signature-based detection approaches nearly impossible.

On top of these, the malware maintained a persistent presence by installing itself in the registry, making it able to survive system reboots.

Given these distinctive characteristics, which two types of malware techniques does this malware most closely embody?

- A. Polymorphic and Metamorphic malware
- B. Polymorphic and Macro malware
- C. Macro and Rootkit malware
- D. Metamorphic and Rootkit malware

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (64%)

A (36%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [e020fdc](#) 6 months, 1 week ago

Selected Answer: D

Changes its code = metamorphic

Installs itself in the registry to survive reboots = rootkit

upvoted 1 times

 [agelbahri](#) 8 months, 3 weeks ago

Selected Answer: A

the key focus of the question lies in its advanced evasion methods through code alteration. Rootkits don't inherently alter their code like Polymorphic or Metamorphic malware do.

upvoted 1 times

 [skorek31](#) 9 months, 4 weeks ago

Selected Answer: D

Metamorphic → evades detection by rewriting its own code with every iteration, making it new and unique from its previous code. This malware doesn't use any encryption keys

Polymorphic → continually changes its features using dynamic encryption keys, making each iteration appear different, malware in the question doesn't use encryption keys

upvoted 1 times

 [49f4430](#) 1 year ago

Selected Answer: A

For mw chat GPT say A, i will go for A
upvoted 1 times

✉️ **LordXander** 1 year, 1 month ago

Selected Answer: A

Guys...it's A for the following reasons:

Polymorphic as it hides as a genuine executable (polymorphic capabilities)
Metamorphic - the malware changes its code.

It could've been C if it mentioned that it was not seen by antivirus solutions as rootkits would run at a lower lever (higher privileges) than antivirus and would be undetectable.

upvoted 2 times

✉️ **LordXander** 1 year, 1 month ago

It's actually D, because it is not polymorphic if it is just embedding into a file; metamorphic capabilities (changing its code as it propagates) and rootkit capabilities (registry install)

upvoted 3 times

✉️ **anarchyeagle** 1 year, 3 months ago

ChatGPT Why not D:

D. Metamorphic and Rootkit malware: While the malware does exhibit metamorphic characteristics, and its persistence could be seen as rootkit-like, the description focuses more on the malware's ability to change its code and embed itself in system files, which are hallmarks of polymorphic and metamorphic malware. Rootkits primarily focus on hiding the presence of malware, which, while possibly a feature of this malware, is not explicitly described in the scenario.

upvoted 1 times

✉️ **qwertyst100** 1 year, 3 months ago

Selected Answer: D
D. Metamorphic and Rootkit malware
upvoted 4 times

✉️ **qtygbapjpesdayazko** 1 year, 2 months ago

This is the way is a Metamorphic and a Rootkit malware
upvoted 1 times

✉️ **xbsumz** 1 year, 3 months ago

Ethical hacking experts can you verify this procedure
upvoted 2 times

✉️ **insaniunt** 1 year, 3 months ago

Selected Answer: D
Polymorphic: The malware changes its code as it propagates, making signature-based detection approaches nearly impossible. This aligns with the characteristics of polymorphic malware.

Rootkit: The malware installs itself in the registry, ensuring a persistent presence and the ability to survive system reboots. This behavior is typical of rootkit malware, which often hides its presence and maintains control over the compromised system by integrating itself deeply into the operating system, often in the registry or kernel level.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 210 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 210

Topic #: 1

[All 312-50v12 Questions]

During a red team engagement, an ethical hacker is tasked with testing the security measures of an organization's wireless network. The hacker needs to select an appropriate tool to carry out a session hijacking attack. Which of the following tools should the hacker use to effectively perform session hijacking and subsequent security analysis, given that the target wireless network has the Wi-Fi Protected Access-pre-shared key (WPA-PSK) security protocol in place?

- A. Hetty
- B. bettercap **Most Voted**
- C. DroidSheep
- D. FaceNiff

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

kinaj 1 year, 4 months ago

A. Hetty: is primarily used for HTTP and HTTPS proxy and session manipulation, but it is not specifically designed for session hijacking in wireless networks.
B. bettercap: is a comprehensive and flexible network attack and monitoring tool that supports a wide range of attacks. It is well-suited for performing attacks on various network protocols and can be used to capture and manipulate traffic, making it effective for session hijacking in a WPA-PSK network.
C. DroidSheep: is an Android application used for session hijacking on unencrypted Wi-Fi networks.
D. FaceNiff: is another tool designed for session hijacking but is specifically tailored for capturing sessions over unsecured (HTTP) networks.
upvoted 1 times

GK2205 1 year, 4 months ago

Selected Answer: B

The difference here is between trying to compromise the network or devices on the network. Bettercap is for the network, most others here are for compromising devices.
upvoted 1 times

GK2205 1 year, 4 months ago

BTW - Bettercap does do hijacking also (HID, Bluetooth). Failed to highlight that fact in my original comment. it also does IP v4 / v6 MITM.
upvoted 1 times

LordXander 1 year, 8 months ago

Selected Answer: B

I would go with B, because it is in the labs and EC likes to put questions about the tools they talk in detail about
upvoted 1 times

mossj 1 year, 8 months ago

Selected Answer: B

B. bettercap

CEHv12. 1026

bettercap is a portable framework written in Go that allows security researchers, red teamers, and reverse engineers to perform reconnaissance and various attacks on Wi-Fi networks, Bluetooth low energy devices, wireless HID devices, and IPv4/IPv6 networks.

key here is and subsequent security analysis
upvoted 1 times

✉  **anarchyeagle** 1 year, 9 months ago

ChatGPT:

B. bettercap

Explanation:

bettercap: is a powerful, flexible, and portable tool designed for network attacks and monitoring. It is well-suited for a wide range of network attack scenarios, including session hijacking on wireless networks. bettercap is capable of performing Man-in-the-Middle (MitM) attacks, which are essential for session hijacking. It can sniff network traffic, capture cookies, and exploit various network protocols to hijack sessions. Its capabilities make it a suitable choice for attacking networks with WPA-PSK security, as it can work after gaining access to the network or when conducting attacks within the network perimeter.

upvoted 1 times

✉  **Miro009900** 1 year, 6 months ago

Stop using ChatGPT all the time. Its mostly wrong.

upvoted 1 times

✉  **sosindi** 1 year, 9 months ago

Bettercap - is a comprehensive network attack and monitoring framework suitable for various types of attacks, including session hijacking, on wireless networks with WPA-PSK security protocols.

Hetty is a tool for wireless network analysis and auditing but does not specialize in session hijacking attacks.

DroidSheep and FaceNiff are Android applications designed for session hijacking attacks targeting mobile devices, specifically over Wi-Fi networks.

upvoted 1 times

✉  **brrbrr** 1 year, 9 months ago

Selected Answer: B

B. bettercap

upvoted 1 times

✉  **duke_of_kamulu** 1 year, 9 months ago

i think the key WORD is SESSION HIJACKING -The DroidSheep tool is used for session hijacking on Android devices connected to a common wireless network. It obtains the session ID of active users on the Wi-Fi network and uses it to access a website as an authorized user. A DroidSheep user can easily observe the activities of authorized users on websites. It can also hijack social accounts by obtaining the session ID.

upvoted 1 times

✉  **sosindi** 1 year, 9 months ago

Selected Answer: C

DroidSheep

upvoted 1 times

✉  **przemyslaw1** 1 year, 9 months ago

Selected Answer: D

FaceNiff is an Android app that allows a user to sniff and intercept web-session profiles over the WiFi network that the user's mobile device is connected to. Although FaceNiff can hijack sessions only when the WiFi network does not use the Extensible Authentication Protocol (EAP), it works on any private network, including open, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access-pre-shared key (WPA-PSK), and WPA2-PSK networks.

upvoted 1 times

✉  **przemyslaw1** 1 year, 9 months ago

Selected Answer: C

DroidSheep is a simple Android tool for web session hijacking

upvoted 1 times

✉  **przemyslaw1** 1 year, 9 months ago

DroidSheep can capture sessions using the libpcap library and it supports OPEN networks, WEP encrypted networks, and WPA and WPA2 (PSK only) encrypted networks.

upvoted 1 times

✉  **xbsumz** 1 year, 9 months ago

Could someone help me confirm the accuracy of this data

upvoted 1 times

✉  **insaniunt** 1 year, 9 months ago

Selected Answer: B

B. bettercap

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 211 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 211

Topic #: 1

[All 312-50v12 Questions]

As a certified ethical hacker, you are tasked with gaining information about an enterprise's internal network. You are permitted to test the network's security using enumeration techniques. You successfully obtain a list of usernames using email IDs and execute a DNS Zone Transfer. Which enumeration technique would be most effective for your next move given that you have identified open TCP ports 25 (SMTP) and 139 (NetBIOS Session Service)?

- A. Perform a brute force attack on Microsoft Active Directory to extract valid usernames
- B. Exploit the NetBIOS Session Service on TCP port 139 to gain unauthorized access to the file system Most Voted
- C. Use SNMP to extract usernames given the community strings
- D. Exploit the NFS protocol on TCP port 2049 to gain control over a remote system

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

[przemyslaw1](#) Highly Voted 1 year, 9 months ago

Selected Answer: B

B. Exploit the NetBIOS
SNMP uses UDP ports 161 and 162
upvoted 11 times

[qtygbapjpesdayazko](#) 1 year, 8 months ago

Base on ports available is B NetBIOS
upvoted 1 times

[John07](#) 1 year, 7 months ago

Exploit the NetBIOS Session Service on TCP port 139 to gain unauthorized access to the file system - it's not an enumeration techniques. Correct answer is C.
upvoted 1 times

[Mos3ab](#) 9 months, 2 weeks ago

While the wording "exploit" might imply active abuse, in the context of a red team engagement it often encompasses benign enumeration techniques that interact with the NetBIOS service to extract useful information (e.g., available shared directories, NetBIOS names, and associated details). Therefore, using the NetBIOS Session Service as a vector for enumeration is the most effective next move given the open port and context.
upvoted 1 times

[agelbahri](#) Most Recent 8 months, 3 weeks ago

Selected Answer: B

CEH v12 page : 411
NetBIOS is considered first for enumeration because it extracts a large amount of sensitive information about the target network, such as users and network shares.
upvoted 1 times

[noyon2002](#) 1 year, 3 months ago

A Brute force active directory, it is the 3rd step in techniques for enumeration :
CEH V12 Module 4 Page 403
upvoted 1 times

 **noyon2002** 1 year, 3 months ago

My bad miss read the question, it is mentioned Port 25 SMTP, so it is C the , 6th step in enumeration CEH V12 Module 5 Page 403
upvoted 1 times

 **49f4430** 1 year, 6 months ago

Selected Answer: A

A

Nothing about 161 and 162, B is a attack..that leave us with A :validate the usernames
upvoted 1 times

 **pranav10** 1 year, 6 months ago

Selected Answer: C

CEHv12 page number 404
upvoted 1 times

 **jrbobson** 1 year, 7 months ago

Selected Answer: C

Enumeration is the key - C
upvoted 1 times

 **Rafael_Fontana** 1 year, 7 months ago

Selected Answer: B

You already have usernames so.... Am I missing something?
upvoted 1 times

 **duke_of_kamulu** 1 year, 8 months ago

GUYS AGAIN i repeat answers is C go to page 403,404 and check you will find its clear the steps they are six
upvoted 2 times

 **Spam_Protection** 1 year, 8 months ago

Selected Answer: A

You need to validate your usernames. You can do this brute forcing Active Directory.
Module 4: Techniques for Enumeration section - • Brute force Active Directory Microsoft Active Directory is susceptible to username enumeration at the time of user-supplied input verification. This is a design error in the Microsoft Active Directory implementation. If a user enables the "logon hours" feature, then all the attempts at service authentication result in different error messages. Attackers take advantage of this to enumerate valid usernames. An attacker who succeeds in extracting valid usernames can conduct a brute-force attack to crack the respective passwords.
upvoted 1 times

 **sosindi** 1 year, 9 months ago

A,
We already extracted emails usernames- "successfully obtained a list of usernames using email IDs and execute a DNS Zone Transfer" the next would be A now to exploit netbios.
upvoted 2 times

 **duke_of_kamulu** 1 year, 9 months ago

according to CEHv12 they follow systematic flow shown clearly on the table pg 403 1-6 so C get Techniques for Enumeration step six last step is Extract usernames using SNMP
upvoted 1 times

 **JustAName** 1 year, 9 months ago

Selected Answer: C

I'd choose C because exploitation and brute force attacks are typically considered post-enumeration activities and consider too invasive to be "enumeration" activity
upvoted 1 times

 **insaniunt** 1 year, 9 months ago

Selected Answer: C

just pay attention, the question asking for "Which enumeration technique", not about perform attack or exploit something
upvoted 3 times

 **sosindi** 1 year, 9 months ago

We already extracted emails usernames- "successfully obtained a list of usernames using email IDs and execute a DNS Zone Transfer" the next would be A now to exploit netbios.
upvoted 1 times

 **cloudgangster** 1 year, 9 months ago

Selected Answer: C

c, check ceh v12 pg 403
upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 212 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 212

Topic #: 1

[\[All 312-50v12 Questions\]](#)

A large corporate network is being subjected to repeated sniffing attacks. To increase security, the company's IT department decides to implement a combination of several security measures. They permanently add the MAC address of the gateway to the ARP cache, switch to using IPv6 instead of IPv4, implement the use of encrypted sessions such as SSH instead of Telnet, and use Secure File Transfer Protocol instead of FTP. However, they are still faced with the threat of sniffing. Considering the countermeasures, what should be their next step to enhance network security?

- A. Use HTTP instead of HTTPS for protecting usernames and passwords
- B. Implement network scanning and monitoring tools Most Voted
- C. Enable network identification broadcasts
- D. Retrieve MAC addresses from the OS

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **JCSundaes** 11 months, 3 weeks ago

Selected Answer: B

A, C, and D are wrong, because:

- A. Use HTTPS not HTTP
- C. Disable network identification broadcasts, not enable.
- D. Retrieve MAC addresses from the NIC, not the OS.

upvoted 1 times

 **duke_of_kamulu** 1 year, 9 months ago

ANSWER IS A because threat is all about sniffing so even one gets those packets are encripted

upvoted 1 times

 **qwerty100** 1 year, 9 months ago

pay attention it says HTTP not https

upvoted 4 times

 **duke_of_kamulu** 1 year, 9 months ago

wah you saved me big time thnx thnx it not see that ANSWER is B

upvoted 1 times

 **insaniunt** 1 year, 9 months ago

Selected Answer: B

B. Implement network scanning and monitoring tools.

Network scanning and monitoring tools can help detect and identify suspicious activities, including sniffing attacks.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 214 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 214

Topic #: 1

[\[All 312-50v12 Questions\]](#)

A cyber attacker has initiated a series of activities against a high-profile organization following the Cyber Kill Chain Methodology. The attacker is presently in the "Delivery" stage. As an Ethical Hacker, you are trying to anticipate the adversary's next move. What is the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology?

- A. The attacker will attempt to escalate privileges to gain complete control of the compromised system.
- B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold. Most Voted
- C. The attacker will initiate an active connection to the target system to gather more data.
- D. The attacker will start reconnaissance to gather as much information as possible about the target.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [e020fdc](#) 6 months, 1 week ago

Selected Answer: B

You got the payload there, now time to set that thing off babyyy
upvoted 1 times

 [LordXander](#) 1 year, 1 month ago

Selected Answer: B

Because...long live cyber kill chain (I will not miss it from CTIA)
upvoted 1 times

 [qtygbapjpesdayazko](#) 1 year, 2 months ago

Selected Answer: B

Is B.

B then A
upvoted 1 times

 [insaniunt](#) 1 year, 3 months ago

Selected Answer: B

B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.
upvoted 4 times

EXAM 312-50V12 TOPIC 1 QUESTION 216 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 216

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Your company, Encryptor Corp, is developing a new application that will handle highly sensitive user information. As a cybersecurity specialist, you want to ensure this data is securely stored. The development team proposes a method where data is hashed and then encrypted before storage. However, you want an added layer of security to verify the integrity of the data upon retrieval. Which of the following cryptographic concepts should you propose to the team?

- A. Switch to elliptic curve cryptography.
- B. Implement a block cipher mode of operation.
- C. Apply a digital signature mechanism. Most Voted
- D. Suggest using salt with hashing.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [Mos3ab](#) 9 months, 2 weeks ago

Selected Answer: C

A digital signature allows you to verify the integrity and authenticity of the data. By signing the data (or its hash) with a private key, you can later verify that the data has not been altered by using the corresponding public key. This added layer ensures that upon retrieval, any unauthorized changes can be detected.

upvoted 1 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: C

C. Apply a digital signature mechanism.

To ensure the integrity of the data upon retrieval, a digital signature mechanism can be employed. Digital signatures provide a way to verify the authenticity and integrity of data by using asymmetric cryptography.

upvoted 4 times

EXAM 312-50V12 TOPIC 1 QUESTION 220 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 220

Topic #: 1

[All 312-50v12 Questions]

A sophisticated attacker targets your web server with the intent to execute a Denial of Service (DoS) attack. His strategy involves a unique mixture of TCP SYN, UDP, and ICMP floods, using ' r ' packets per second. Your server, reinforced with advanced security measures, can handle ' h ' packets per second before it starts showing signs of strain. If ' r ' surpasses ' h ', it overwhelms the server, causing it to become unresponsive. In a peculiar pattern, the attacker selects ' r ' as a composite number and ' h ' as a prime number, making the attack detection more challenging. Considering ' $r=2010$ ' and different values for ' h ', which of the following scenarios would potentially cause the server to falter?

- A. $h=1987$ (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness. Most Voted
- B. $h=1999$ (prime): Despite the attacker's packet flood, the server can handle these requests, remaining responsive.
- C. $h=1993$ (prime): Despite being less than ' r ', the server's prime number capacity keeps it barely operational, but the risk of falling is imminent.
- D. $h=2003$ (prime): The server can manage more packets than the attacker is sending, hence it stays operational.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

✉  sumanroy 11 months ago

Selected Answer: A

Bruh it was simple enough XD, what will overwhelm the server most? the one with less resource right?
upvoted 1 times

✉  49f4430 1 year ago

common ECC all this question for telling us A > B
upvoted 1 times

✉  qwerty100 1 year, 3 months ago

Selected Answer: A

A. $h=1987$ (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness.
upvoted 1 times

✉  Nopez 1 year, 3 months ago

Selected Answer: A

A. If ' r ' surpasses ' h ', it'll overwhelm. That means if 2010 surpasses 1987 (it does), it'll cause problems.
upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 221 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 221

Topic #: 1

[\[All 312-50v12 Questions\]](#)

An IT security team is conducting an internal review of security protocols in their organization to identify potential vulnerabilities. During their investigation, they encounter a suspicious program running on several computers. Further examination reveals that the program has been logging all user keystrokes. How can the security team confirm the type of program and what countermeasures should be taken to ensure the same attack does not occur in the future?

- A. The program is spyware; the team should use password managers and encrypt sensitive data.
- B. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software. Most Voted
- C. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups.
- D. The program is a Trojan; the team should regularly update antivirus software and install a reliable firewall.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [insaniunt](#) 1 year, 3 months ago

Selected Answer: B

B. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software.
upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 222 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 222

Topic #: 1

[All 312-50v12 Questions]

Being a Certified Ethical Hacker (CEH), a company has brought you on board to evaluate the safety measures in place for their network system. The company uses a network time protocol server in the demilitarized zone. During your enumeration, you decide to run a `ntptrace` command. Given the syntax: `ntptrace [-n] [-m maxhosts] [servername/IP_address]`, which command usage would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network?

- A. `ntptrace -n -m 5192.168.1.1`
- B. `ntptrace -m 5192.168.1.1`
- C. `ntptrace -n localhost`
- D. `ntptrace 192.168.1.1` Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

[3936e29](#) 8 months, 1 week ago

Selected Answer: D

The default value for maxhosts is 99, by using -m 5 you effectively limit tracing to 5 hops. Which may not result in finished trace.

The correct answer is D - `ntptrace` with no parameters.
upvoted 1 times

[Mos3ab](#) 9 months, 2 weeks ago

Selected Answer: D

The `ntptrace` command traces a chain of Network Time Protocol (NTP) servers back to their master time source. By default, running `ntptrace` without any arguments starts the trace from the localhost. However, to trace the NTP servers for a specific server, you should provide its hostname or IP address as an argument. In this case, `ntptrace 192.168.1.1` will trace the NTP server chain starting from the server at 192.168.1.1.

The -n option disables the resolution of hostnames, displaying IP addresses instead. The -m option sets the maximum number of levels to trace. While these options can be useful, they are not necessary for the basic functionality of tracing the NTP server chain. Therefore, the simplest and most direct command to achieve your objective is `ntptrace 192.168.1.1`.

upvoted 1 times

[MPA3333](#) 1 year ago

It's A, there is a typo with a " " missing between 5 and the IP address.
upvoted 1 times

[noyon2002](#) 1 year, 3 months ago

I am confused in the book CEH V12 Module 4 Page it is clearly mentioned A, and most of people are answering D
upvoted 1 times

[noyon2002](#) 1 year, 3 months ago

Page 446

upvoted 2 times

[g_man_rap](#) 1 year, 7 months ago

A. `ntptrace -n -m 5192.168.1.1`

This usage is incorrect because -m expects a numerical argument that specifies the maximum number of hosts to trace, not an IP address.

B. ntptrace -m 5192.168.1.1

Similar to option A, this is a misuse of the -m option. It wrongly places an IP address where a number should be, indicating the depth of the trace.

C. ntptrace -n localhost

This command will start tracing from the local host, and the -n option will ensure that the output remains numerical (IP addresses only), which might not be as informative if you're unfamiliar with the IPs but does provide clean data output.

D. ntptrace 192.168.1.1

This is the basic form of the command and correctly targets an NTP server by IP address. It lacks any specific options for depth of trace (-m) or format (-n), but correctly initiates a trace to the specified server.

upvoted 1 times

✉ **Spam_Protection** 1 year, 8 months ago

Selected Answer: D

It's D.

A &B: You're not trying to find max host but trace source of time.

C: you use the -n command which means it should give you IP of local host(127.0.0.1) instead of local host , host name.

upvoted 2 times

✉ **qtygbapjpesdayazko** 1 year, 8 months ago

Selected Answer: D

D. ntptrace 192.168.1.1

upvoted 1 times

✉ **qtygbapjpesdayazko** 1 year, 8 months ago

A and B are note valid, missing a space and parameter N and M are optional.

And the NTP server is not localhost.

upvoted 1 times

✉ **athicalacker** 1 year, 9 months ago

Selected Answer: D

The -n option is not necessary unless you prefer to see IP addresses instead of hostnames, and the -m option is not necessary unless you want to limit the number of hosts traced. Option C would only be correct if you were running the command on the NTP server itself and you wanted to see IP addresses instead of hostnames. So, the correct answer is option D, ntptrace 192.168.1.1.

upvoted 3 times

✉ **LeongCC** 1 year, 9 months ago

Selected Answer: A

I think A is more suitable

upvoted 1 times

✉ **duke_of_kamulu** 1 year, 9 months ago

CEHv12 pg 446 CORRECT ANSWER is A ntptrace This command determines where the NTP server obtains the time from and follows the chain of NTP servers back to its primary time source. Attackers use this command to trace the list of NTP servers connected to the network. Its syntax is as follows: ntptrace [-n] [-m maxhosts] [servername/IP_address]

upvoted 1 times

✉ **qwerty100** 1 year, 9 months ago

I think is D. ntptrace 192.168.1.1

-m and -n are optional

upvoted 4 times

✉ **athicalacker** 1 year, 9 months ago

Exactly!

upvoted 2 times

✉ **insaniunt** 1 year, 9 months ago

5192.168.1.1?

if: B. ntptrace -m 192.168.1.1 thats correct

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 223 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 223

Topic #: 1

[All 312-50v12 Questions]

A Certified Ethical Hacker is attempting to gather information about a target organization's network structure through network footprinting. During the operation, they encounter ICMP blocking by the target system's firewall. The hacker wants to ascertain the path that packets take to the host system from a source, using an alternative protocol. Which of the following actions should the hacker consider next?

- A. Use UDP Traceroute in the Linux operating system by executing the 'traceroute' command with the destination IP or domain name.
Most Voted
- B. Use the ICMP Traceroute on the Windows operating system as it is the default utility.
- C. Use the ARIN Whois database search tool to find the network range of the target network.
- D. Utilize the Path Analyzer Pro to trace the route from the source to the destination target systems.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 e020fdc 6 months, 1 week ago

Selected Answer: A

Reason why A is correct is explained by others below (not LordXander tho).

ChatGPT says for the others:

B. ICMP Traceroute on Windows:

Windows uses ICMP Echo Request for traceroute, which is ineffective if ICMP is blocked.

C. ARIN Whois database search:

Useful for identifying IP address ownership and ranges, but not for tracing packet paths.

D. Path Analyzer Pro:

A commercial tool that can be useful, but it's an additional utility, and the question suggests the need for a protocol-level workaround.

Also, its effectiveness still depends on how it performs traceroute (may still be blocked if it uses ICMP).

upvoted 1 times

 Mos3ab 9 months, 2 weeks ago

Selected Answer: A

The traceroute utility in Linux, by default, sends UDP packets to high-numbered ports (starting at 33434) and listens for ICMP "port unreachable" messages from the destination. This method can bypass ICMP blocking since it doesn't rely on ICMP echo requests for its operation. By executing traceroute [destination IP/domain], you can trace the route packets take to the target system.

upvoted 1 times

 LordXander 1 year, 1 month ago

Selected Answer: A

UDP..because most defences are not configured for UDP (don't ask how I know that)

upvoted 2 times

 insaniumt 1 year, 3 months ago

Selected Answer: A

A. Use UDP Traceroute in the Linux operating system by executing the 'traceroute' command with the destination IP or domain name.

When ICMP is blocked by a firewall, you can use alternative protocols like UDP for tracerouting. In Linux, the 'traceroute' command allows you to specify the UDP protocol using the '-U' option.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 227 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 227

Topic #: 1

[\[All 312-50v12 Questions\]](#)

A penetration tester is conducting an assessment of a web application for a financial institution. The application uses form-based authentication and does not implement account lockout policies after multiple failed login attempts. Interestingly, the application displays detailed error messages that disclose whether the username or password entered is incorrect. The tester also notices that the application uses HTTP headers to prevent clickjacking attacks but does not implement Content Security Policy (CSP). With these observations, which of the following attack methods would likely be the most effective for the penetration tester to exploit these vulnerabilities and attempt unauthorized access?

- A. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database.
- B. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials. **Most Voted**
- C. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack.
- D. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [LordXander](#) 1 year, 1 month ago

Selected Answer: B

Because there's no account lockout mechanism and have detailed information whatever the username or password is wrong, the brute force method makes the most sense

B

upvoted 1 times

  [xbsumz](#) 1 year, 3 months ago

Could someone confirm the accuracy of this CEH technique

upvoted 1 times

  [Lalo](#) 1 year, 2 months ago

1.- It is not an exclusive technique of CEH, it is a general technique to crack passwords
2.- When reading the scenario it indicates ...does not implement account lockout policies after multiple failed login attempts...
Therefore the correct option is option b.
3.- If you read the scenario carefully and know a little about security, you come to this conclusion

upvoted 1 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: B

B. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 230 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 230

Topic #: 1

[All 312-50v12 Questions]

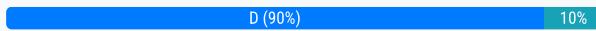
Consider a scenario where a Certified Ethical Hacker is attempting to infiltrate a company's network without being detected. The hacker intends to use a stealth scan on a BSD-derived TCP/IP stack, but he suspects that the network security devices may be able to detect SYN packets. Based on this information, which of the following methods should he use to bypass the detection mechanisms and why?

- A. Maimon Scan, because it is very similar to NULL, FIN, and Xmas scans, but the probe used here is FIN/ACK
- B. Xmas Scan, because it can pass through filters undetected, depending on the security mechanisms installed
- C. TCP Connect/Full-Open Scan, because it completes a three-way handshake with the target machine
- D. ACK Flag Probe Scan, because it exploits the vulnerabilities within the BSD-derived TCP/IP stack Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

✉ [agelbahri](#) 8 months, 3 weeks ago

Selected Answer: D

CEH v12 pages: 311-313

upvoted 2 times

✉ [NikeshMaharaj](#) 1 year, 2 months ago

i think its option A:

To bypass detection mechanisms on a BSD-derived TCP/IP stack, the Certified Ethical Hacker should use:

A. Maimon Scan, because it is very similar to NULL, FIN, and Xmas scans, but the probe used here is FIN/ACK

The Maimon Scan is effective because it sends a FIN/ACK probe, which can exploit certain vulnerabilities in the TCP/IP stack of BSD-derived systems. This type of scan is less likely to be detected by network security devices that are configured to detect SYN packets, making it a suitable choice for stealth scanning.

upvoted 3 times

✉ [g_man_rap](#) 1 year, 7 months ago

Option D, ACK Flag Probe Scan, is the most appropriate choice. This scan can provide insights into the network's filtering behavior without the usual risks of detection associated with opening a full connection or sending irregular flag combinations, making it a more discreet option for initial reconnaissance, especially in environments that are sensitive to SYN packets.

upvoted 1 times

✉ [qtygbapipesdayazko](#) 1 year, 8 months ago

Selected Answer: D

The correct is D. Keyword "BSD-derived TCP/IP stack", BSD have a limitation in TCP/IP stack.

ACK Flag Probe Scan

Attackers send TCP probe packets with the ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of the received RST packets to find out if the port is open or closed. The ACK flag probe scan exploits the vulnerabilities within the BSD-derived TCP/IP stack. Thus, such scanning is effective only on those OSs and platforms on which the BSD derives TCP/IP stacks.

Module 03 Page 312

upvoted 3 times

✉ [przemyslaw1](#) 1 year, 9 months ago

Selected Answer: D

Attackers send TCP probe packets with the ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of the received RST packets to find out if the port is open or closed. The ACK flag probe scan exploits the vulnerabilities within the BSD-derived TCP/IP stack. Thus, such scanning is effective only on those OSs and platforms on which the BSD derives TCP/IP stacks.

upvoted 2 times

 **Nopez** 1 year, 9 months ago

Selected Answer: D

D. via research

upvoted 1 times

 **insaniunt** 1 year, 9 months ago

Selected Answer: B

B. Xmas Scan, because it can pass through filters undetected, depending on the security mechanisms installed.

A Xmas Scan is a type of TCP port scan where the attacker sends TCP packets with the FIN, URG, and PSH flags set to target a specific range of ports. This scan is designed to evade detection mechanisms that may be configured to detect SYN packets or other standard scanning techniques.

upvoted 1 times

 **insaniunt** 1 year, 9 months ago

Module 03 Page 308 and 309

upvoted 1 times

 **qwerty100** 1 year, 9 months ago

Selected Answer: D

I am not very sure, but I think it's D

(Module 03 Page 311and 312)

ACK Flag Probe Scan Attackers send TCP probe packets with the ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of the received RST packets to find out if the port is open or closed. The ACK flag probe scan exploits the vulnerabilities within the BSD-derived TCP/IP stack. Thus, such scanning is effective only on those OSs and platforms on which the BSD derives TCP/IP stacks.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 231 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 231

Topic #: 1

[\[All 312-50v12 Questions\]](#)

While performing a security audit of a web application, an ethical hacker discovers a potential vulnerability. The application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. The ethical hacker decides to exploit this vulnerability further. Which type of SQL Injection attack is the ethical hacker likely to use?

- A. UNION SQL Injection
- B. Error-based SQL Injection Most Voted
- C. In-band SQL Injection
- D. Blind/Inferential SQL Injection

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  **LordXander** 1 year, 1 month ago

Selected Answer: B

CEH 2218 - error based sql injection - B

upvoted 2 times

  **insaniunt** 1 year, 3 months ago

Selected Answer: B

B. Error-based SQL Injection

In an Error-based SQL Injection attack, the attacker intentionally injects malicious SQL code into user input fields to provoke an error in the database. The application, if not properly secured, may then reveal detailed error messages that expose information about the underlying database structure

upvoted 2 times

  **rorahir** 1 year, 3 months ago

Im unsure about the accuracy of this statement"

upvoted 1 times

 EXAM 312-50V12 TOPIC 1 QUESTION 233 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 233

Topic #: 1

[All 312-50v12 Questions]

Martin, a Certified Ethical Hacker (CEH), is conducting a penetration test on a large enterprise network. He suspects that sensitive information might be leaking out of the network. Martin decides to use network sniffing as part of his testing methodology. Which of the following sniffing techniques should Martin employ to get a comprehensive understanding of the data flowing across the network?

A. Raw Sniffing **Most Voted**

B. MAC Flooding

C. ARP Poisoning

D. DNS Poisoning

[Hide Answer](#)

Suggested Answer: A

Community vote distribution



by DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

Aalkinani 4 months, 1 week ago

Selected Answer: C

This allows the attacker to position themselves as a man-in-the-middle (MITM) by associating their MAC address with the IP of another host (like the gateway). It's a stealthy and effective way to sniff traffic on a switched LAN.

upvoted 1 times

ba1dd4b 9 months, 1 week ago

Selected Answer: B

Module 8, page 1214

upvoted 1 times

qtygbapjpesdayazko 1 year, 1 month ago

Selected Answer: A

keyword "network sniffing", Raw Sniffing, all other will cause problems.

upvoted 1 times

brrbrr 1 year, 3 months ago

Selected Answer: A

Raw sniffing involves capturing and analyzing network traffic at the raw data link layer, allowing an analyst to inspect the actual content of packets. Moreover, this is the only sniffing technique proposed here, other options are considered as sniffing attacks.

upvoted 4 times

insaniunt 1 year, 3 months ago

Selected Answer: A

A. Raw Sniffing

upvoted 1 times

rorahir 1 year, 3 months ago

Team is this ethical hacking approach correct"

upvoted 1 times

 EXAM 312-50V12 TOPIC 1 QUESTION 234 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 234

Topic #: 1

[All 312-50v12 Questions]

As a cybersecurity consultant for SafePath Corp, you have been tasked with implementing a system for secure email communication. The key requirement is to ensure both confidentiality and non-repudiation. While considering various encryption methods, you are inclined towards using a combination of symmetric and asymmetric cryptography. However, you are unsure which cryptographic technique would best serve the purpose. Which of the following options would you choose to meet these requirements?

- A. Apply asymmetric encryption with RSA and use the private key for signing. Most Voted
- B. Use the Diffie-Hellman protocol for key exchange and encryption.
- C. Apply asymmetric encryption with RSA and use the public key for encryption.
- D. Use symmetric encryption with the AES algorithm.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **milktea810182** 1 year ago

Selected Answer: A

This option utilizes asymmetric encryption with RSA, which ensures confidentiality through encryption using the recipient's public key and utilizes the sender's private key for digital signing to achieve non-repudiation. By signing the email with the sender's private key, it ensures that the sender cannot later deny sending the message, providing a form of non-repudiation. This approach offers a robust solution for secure email communication meeting the specified requirements.

upvoted 2 times

 **qtygbapjpesdayazko** 1 year, 2 months ago

Selected Answer: A

Apply asymmetric encryption with RSA and use the private key for signing.

upvoted 1 times

 **brrbrr** 1 year, 3 months ago

Selected Answer: A

A - Apply asymmetric encryption with RSA and use the private key for signing:

Asymmetric encryption with RSA is suitable for confidentiality (encryption) when combined with the public key. Using the private key for signing ensures that the sender is authentic, providing non-repudiation.

upvoted 2 times

 **insaniunt** 1 year, 3 months ago

Selected Answer: A

To meet the requirements of both confidentiality and non-repudiation in secure email communication, a combination of symmetric and asymmetric cryptography is commonly employed. Based on the options provided, the most suitable choice would be:

A. Apply asymmetric encryption with RSA and use the private key for signing.

upvoted 1 times

 **rorahir** 1 year, 3 months ago

"Im a bit hesitant about the effectiveness of this ethical hacking approach"

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 235 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 235

Topic #: 1

[\[All 312-50v12 Questions\]](#)

As a cybersecurity analyst for SecureNet, you are performing a security assessment of a new mobile payment application. One of your primary concerns is the secure storage of customer data on the device. The application stores sensitive information such as credit card details and personal identification numbers (PINs) on the device. Which of the following measures would best ensure the security of this data?

- A. Enable GPS tracking for all devices using the app.
- B. Regularly update the app to the latest version.
- C. Encrypt all sensitive data stored on the device. Most Voted
- D. Implement biometric authentication for app access.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [qwerty100](#) 1 year, 3 months ago

Selected Answer: C

C. Encrypt all sensitive data stored on the device.

upvoted 3 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: C

C. Encrypt all sensitive data stored on the device.

To ensure the security of sensitive data stored on a mobile device, especially credit card details and PINs, the most effective measure is to encrypt the data.

upvoted 2 times

  [rorahir](#) 1 year, 3 months ago

I'm unsure about the accuracy of this statement"

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 236 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 236

Topic #: 1

[\[All 312-50v12 Questions\]](#)

A large multinational corporation is in the process of evaluating its security infrastructure to identify potential vulnerabilities. After a comprehensive analysis, they found multiple areas of concern, including time of check/time of use (TOC/TOU) errors, improper input handling, and poor patch management. Which of the following approaches will best help the organization mitigate the vulnerability associated with TOC/TOU errors?

- A. Regular patching of servers, firmware, operating system, and applications
- B. Ensuring atomicity of operations between checking and using data resources Most Voted
- C. Frequently updating firewall configurations to prevent intrusion attempts
- D. Implementing stronger encryption algorithms for all data transfers

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [LordXander](#) 1 year, 1 month ago

Selected Answer: B

CEH 547 - It's a race condition more or less, hence B
upvoted 2 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: B

B. Ensuring atomicity of operations between checking and using data resources

Time of Check/Time of Use (TOC/TOU) errors, also known as race conditions, occur when a system checks the status of a resource at one point in time and then uses that resource at a later point in time without proper synchronization. This time gap between checking and using the resource can lead to security vulnerabilities.

upvoted 4 times

  [rorahir](#) 1 year, 3 months ago

Could someone confirm the accuracy of this CEH technique"

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 237 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 237

Topic #: 1

[\[All 312-50v12 Questions\]](#)

A security analyst is preparing to analyze a potentially malicious program believed to have infiltrated an organization's network. To ensure the safety and integrity of the production environment, the analyst decided to use a sheep dip computer for the analysis. Before initiating the analysis, what key step should the analyst take?

- A. Install the potentially malicious program on the sheep dip computer.
- B. Store the potentially malicious program on an external medium, such as a CD-ROM. Most Voted
- C. Run the potentially malicious program on the sheep dip computer to determine its behavior.
- D. Connect the sheep dip computer to the organization's internal network.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

 [a68d338](#) 9 months, 3 weeks ago

Selected Answer: B

The user isolate the sheep dip computer from others computer on the network to block any malware entering in the system. Before performing this process it is important to save all downloaded programs on external media such as CD ROMS and DVD.
CEH v12 Module 7 page 1085

upvoted 3 times

 [qtygbapjpesdayazko](#) 1 year, 1 month ago

keyword "Before initiating the analysis", store the malware in a CD-ROM.
upvoted 1 times

 [LordXander](#) 1 year, 1 month ago

Selected Answer: B

I mean, none of the other option make sense (even B is questionable but is the least questionable one)
upvoted 2 times

 [qwerty100](#) 1 year, 3 months ago

Selected Answer: B

B. Store the potentially malicious program on an external medium, such as a CD-ROM.
upvoted 2 times

 [insaniunt](#) 1 year, 3 months ago

B. Store the potentially malicious program on an external medium, such as a CD-ROM.
- Module 07 Page 1085
upvoted 3 times

 [rorahir](#) 1 year, 3 months ago

Team can you confirm if this is accurate"
upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 239 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 239

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However, you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?

- A. Switching all data transmission to the HTTPS protocol.
- B. Implementing SSL certificates on your company's web servers.
- C. Utilizing SSH for secure remote logins to the servers.
- D. Applying the Diffie-Hellman protocol to exchange the symmetric key. Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [LordXander](#) 1 year, 1 month ago

Selected Answer: D

'However, you must also ensure the secure exchange of the symmetric key' -the only one applicable is D
upvoted 2 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: D

D. Applying the Diffie-Hellman protocol to exchange the symmetric key.

The Diffie-Hellman key exchange protocol is specifically designed for securely exchanging cryptographic keys over an untrusted communication channel

upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 240 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 240

Topic #: 1

[\[All 312-50v12 Questions\]](#)

As an IT intern, you have been asked to help set up a secure Wi-Fi network for a local coffee shop. The owners want to provide free Wi-Fi to their customers, but they are concerned about potential security risks. They are looking for a simple yet effective solution that would not require a lot of technical knowledge to manage. Which of the following security measures would be the most suitable in this context?

- A. Disable the network's SSID broadcast
- B. Enable MAC address filtering
- C. Require customers to use VPN when connected to the Wi-Fi
- D. Implement WPA2 or WPA3 encryption

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [LordXander](#) 1 year, 1 month ago

Selected Answer: D

Again, ease of use and limited technical capabilities - D

upvoted 1 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: D

D. Implement WPA2 or WPA3 encryption

upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 241 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 241

Topic #: 1

[\[All 312-50v12 Questions\]](#)

During a penetration test, an ethical hacker is exploring the security of a complex web application. The application heavily relies on JavaScript for client-side input sanitization, with an apparent assumption that this alone is adequate to prevent injection attacks. During the investigation, the ethical hacker also notices that the application utilizes cookies to manage user sessions but does not enable the HttpOnly flag. This lack of flag potentially exposes the cookies to client-side scripts. Given these identified vulnerabilities, what would be the most effective strategy for the ethical hacker to exploit this application?

- A. Instigate a Distributed Denial of Service (DDoS) attack to overload the server, capitalizing on potential weak server-side security.
- B. Implement an SQL Injection attack to take advantage of potential unvalidated input and gain unauthorized database access.
- C. Employ a brute-force attack to decipher user credentials, considering the lack of server-side validation.
- D. Launch a Cross-Site Scripting (XSS) attack, aiming to bypass the client-side sanitization and exploit the exposure of session cookies.

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  [LordXander](#) 1 year, 1 month ago

Selected Answer: D

D - because if there's lack of HttpOnly & validation via JavaScript, this opens the possibility for a XSS to exploit the cookies
upvoted 1 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: D

D. Launch a Cross-Site Scripting (XSS) attack, aiming to bypass the client-side sanitization and exploit the exposure of session cookies.
upvoted 4 times

EXAM 312-50V12 TOPIC 1 QUESTION 242 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 242

Topic #: 1

[\[All 312-50v12 Questions\]](#)

In the process of footprinting a target website, an ethical hacker utilized various tools to gather critical information. The hacker encountered a target site where standard web spiders were ineffective due to a specific file in its root directory. However, they managed to uncover all the files and web pages on the target site, monitoring the resulting incoming and outgoing traffic while browsing the website manually. What technique did the hacker likely employ to achieve this?

- A. Using the Netcraft tool to gather website information
- B. Examining HTML source code and cookies
- C. Using Photon to retrieve archived URLs of the target website from archive.org
- D. User-directed spidering with tools like Burp Suite and WebScarab

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:38 p.m.

Comments

  **LordXander** 1 year, 1 month ago

Selected Answer: D

D - because Burp Suite is very good at spidering a website
upvoted 1 times

  **insaniunt** 1 year, 3 months ago

Selected Answer: D

D. User-directed spidering with tools like Burp Suite and WebScarab.
upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 244 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 244

Topic #: 1

[All 312-50v12 Questions]

As a budding cybersecurity enthusiast, you have set up a small lab at home to learn more about wireless network security. While experimenting with your home Wi-Fi network, you decide to use a well-known hacking tool to capture network traffic and attempt to crack the Wi-Fi password. However, despite many attempts, you have been unsuccessful. Your home Wi-Fi network uses WPA2 Personal with AES encryption. Why are you finding it difficult to crack the Wi-Fi password?

- A. Your hacking tool is outdated.
- B. The Wi-Fi password is too complex and long. **Most Voted**
- C. The network is using an uncrackable encryption method.
- D. The network is using MAC address filtering.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **njasanjs** 1 year, 4 months ago

Selected Answer: B

WPA2 with AES is not uncrackable, but it is very secure when used with a strong passphrase. It can be cracked if the password is weak or if certain vulnerabilities are exploited, but this is not the case here.

upvoted 1 times

 **g_man_rap** 1 year, 7 months ago

C. WPA2 Personal with AES is widely used. If it would be simple to crack would not be used at large scale.

upvoted 1 times

 **anarchyeagle** 1 year, 9 months ago

Selected Answer: B

ChatGPT:

B. The Wi-Fi password is too complex and long.

Here's why this option is the most plausible:

WPA2 Personal with AES encryption is currently considered secure for home and personal use, provided a strong, complex, and long password is used. AES (Advanced Encryption Standard) is a symmetric encryption algorithm widely regarded as unbreakable with current computing technology when implemented correctly. The security of a WPA2 network largely depends on the password's strength. A complex and long password (typically 12 characters or more, including numbers, symbols, and upper and lower case letters) significantly increases the time and computational power required to crack it through brute-force attacks.

upvoted 1 times

 **insaniunt** 1 year, 9 months ago

Selected Answer: B

C. The network is using an uncrackable encryption method

upvoted 1 times

 **sogbe** 1 year, 9 months ago

The issue here is

A. The hacking tool is outdated

The question suggests that you're using a well known hack which involves capturing network traffic to get into the wifi network, this is how the IV attack worked on WEP, by picking up enough packets from the air to be able to figure out which key is in use. That doesn't work with WPA2

though, WPA2 is vulnerable to KRACK which attacks the network by abusing the 3 way handshake authentication method.

Besides look at the suggested answer, nothing is uncrackable, especially not WiFi, even something like AES256 bit is breakable... it would just take a billion years to do it. But KRACK will break through WPA2.

upvoted 1 times

 **przemyslaw1** 1 year, 9 months ago

KRACK attack does not allow the password value to be determined. The attacker only steals the session key.

upvoted 1 times

 **[Removed]** 1 year, 9 months ago

I'm unsure about the accuracy of this statement

upvoted 1 times

 **qwerty100** 1 year, 9 months ago

Selected Answer: B

B. The Wi-Fi password is too complex and long.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 246 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 246

Topic #: 1

[All 312-50v12 Questions]

John, a security analyst, is analyzing a server suspected of being compromised. The attacker has used a non admin account and has already gained a foothold on the system. John discovers that a new Dynamic Link Library is loaded in the application directory of the affected server. This DLL does not have a fully qualified path and seems to be malicious. What privilege escalation technique has the attacker likely used to compromise this server?

- A. DLL Hijacking **Most Voted**
- B. Named Pipe Impersonation
- C. Spectre and Meltdown Vulnerabilities
- D. Exploiting Misconfigured Services

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  DarioReymag at Feb. 6, 2024, 10:38 p.m.

Comments

 **ethacker2** 1 year, 3 months ago

A. DLL Hijacking
CEHv12 Book Module 6 p.711

Most Windows applications do not use the fully qualified path when loading an external DLL library; instead, they first search the directory from which they have been loaded. Taking this as an advantage, if attackers can place a malicious DLL in the application directory, the application will execute the malicious DLL in place of the real DLL. For example, if an application program ".exe" needs library.dll (usually in the Windows system directory) to install the application, and fails to specify the library.dll path, Windows will search for the DLL in the directory from which the application was launched. If an attacker has already placed the DLL in the same directory as program.exe, then that malicious DLL will load instead of the real DLL, which allows the attacker to gain remote access to the target system.

upvoted 3 times

 **qwertyst100** 1 year, 3 months ago

Selected Answer: A
A. DLL Hijacking
(Module 06 page 711)
upvoted 3 times

 **DarioReymag** 1 year, 3 months ago

Is this answer accurate friends
upvoted 1 times

 EXAM 312-50V12 TOPIC 1 QUESTION 129 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 129

Topic #: 1

[All 312-50v12 Questions]

A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?

- A. Test 3: The test was executed to observe the response of the target system when a packet with URC, PSH, SYN, and FIN flags was sent, thereby identifying the OS
- B. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target
- C. Test 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint Most Voted
- D. Test 6: The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [DarioReymag](#) at Feb. 6, 2024, 10:44 p.m.

Comments

 [yicx1](#) 1 year, 5 months ago

Test 6: send to closed port.

Test 2: send empty packet to open port.

Test 3: send packet with set flags SYN|FIN|URG|PSH on open port without any options

So the answer is Test 1: send packet with SYN flag with TCP options on open ports

upvoted 1 times

 [\[Removed\]](#) 1 year, 9 months ago

Could someone help me confirm if this is correct

upvoted 1 times

 [insaniunt](#) 1 year, 9 months ago

Selected Answer: C

Test 1: A TCP packet with the SYN and ECN-Echo flags enabled is sent to an open TCP port.

upvoted 3 times

 [cloudgangster](#) 1 year, 9 months ago

The answer is C, These are the new questions in the pool.

upvoted 3 times

 [cloudgangster](#) 1 year, 9 months ago

CEH V12 PG 333

upvoted 1 times

 [DarioReymag](#) 1 year, 9 months ago

Could someone help me confirm if this is correct

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 255 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 255

Topic #: 1

[All 312-50v12 Questions]

Given below are different steps involved in the vulnerability-management life cycle.

- 1) Remediation
- 2) Identify assets and create a baseline
- 3) Verification
- 4) Monitor
- 5) Vulnerability scan
- 6) Risk assessment

Identify the correct sequence of steps involved in vulnerability management.

A. 2 → 5 → 6 → 1 → 3 → 4 Most Voted

- B. 2 → 4 → 5 → 3 → 6 → 1
C. 2 → 1 → 5 → 6 → 4 → 3
D. 1 → 2 → 3 → 4 → 5 → 6

[Hide Answer](#)

Suggested Answer: A

Community vote distribution



by d10f290 at Feb. 23, 2024, 5:30 p.m.

Comments

Naif2030 8 months, 3 weeks ago

Selected Answer: A

hint" Monitoring is usually the last step
upvoted 1 times

LordXander 1 year, 1 month ago

Selected Answer: A

You need to verify after remediation, hence A
upvoted 1 times

ethacker2 1 year, 3 months ago

Selected Answer: A

A. 2 → 5 → 6 → 1 → 3 → 4
CEHv12 Book Module 5 p.534

The phases involved in vulnerability management are:
▪ Pre-Assessment Phase o Identify Assets and Create a Baseline
▪ Vulnerability Assessment Phase o Vulnerability Scan
▪ Post Assessment Phase o Risk Assessment o Remediation o Verification o Monitoring
upvoted 3 times

ethacker2 1 year, 3 months ago

The phases involved in vulnerability management are:
▪ Pre-Assessment Phase
(Identify Assets and Create a Baseline)
▪ Vulnerability Assessment Phase
(Vulnerability Scan)

- Post Assessment Phase
 - Risk Assessment
 - Remediation
 - Verification
 - Monitoring
- upvoted 3 times

✉️👤 **insaniunt** 1 year, 3 months ago

Selected Answer: A

Module 05 Page 533

upvoted 3 times

✉️👤 **qtygbapjpesdayazko** 1 year, 3 months ago

Could someone help me confirm the accuracy of this data

upvoted 1 times

✉️👤 **d10f290** 1 year, 3 months ago

Selected Answer: B

B maybe ?

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 248 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 248

Topic #: 1

[All 312-50v12 Questions]

Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user.

What is the enumeration technique used by Henry on the organization?

A. DNS zone walking

B. DNS cache snooping Most Voted

C. DNS cache poisoning

D. DNSSEC zone walking

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

 [insaniunt](#) Highly Voted 1 year, 3 months ago

Selected Answer: B

DNS Cache Snooping: This technique involves querying the DNS server's cache for information about the recent DNS resolutions it has performed. By analyzing the cached records, an attacker can gain insights into the websites or services recently visited by the organization's users. This can be a valuable reconnaissance step in understanding the organization's network activity.

upvoted 6 times

 [LordXander](#) Most Recent 1 year, 1 month ago

Selected Answer: B

B - CEH 470 / Module 4

upvoted 2 times

 [qtygbapjpesdayazko](#) 1 year, 3 months ago

Could someone please validate this information

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 254 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 254

Topic #: 1

[All 312-50v12 Questions]

An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.

What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

A. Buffer overflow attack

B. Side-channel attack **Most Voted**

C. Denial-of-service attack

D. HMI-based attack

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

 [ethacker2](#) 1 year, 3 months ago

Selected Answer: B

B. Side-channel attack

CEHv12 Book Module 18 p. 2956

Attackers perform a side-channel attack by monitoring its physical implementation to obtain critical information from a target system. Attackers use two techniques, namely timing analysis and power analysis, to perform side-channel attacks on the target OT systems.

Passwords are often transmitted through a serial channel. Attackers employ a loop strategy to recover these passwords. They use one character at a time to check whether the first character entered is correct; if so, the loop continues for consecutive characters. If not, the loop terminates. Attackers check how much time the device is taking to finish one complete password authentication process, through which they can determine how many characters entered are correct.

upvoted 3 times

 [insaniunt](#) 1 year, 3 months ago

Selected Answer: B

B. Side-channel attack

In this scenario, the attacker is exploiting information leaked through a side channel, which is the time it takes for the authentication process. This method is often referred to as a timing attack.

upvoted 2 times

 [qtygbapjpesdayazko](#) 1 year, 3 months ago

CEH experts can you validate this solution

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 250 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 250

Topic #: 1

[\[All 312-50v12 Questions\]](#)

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. Most Voted
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  [g_man_rap](#) 1 year, 1 month ago

B. Determine the impact of enabling the audit feature.

Analysis: Understanding the impact of enabling auditing is critical. Auditing can have significant effects on system performance, storage requirements, and operational workflows. It is essential to assess how the system will handle the additional load of recording and storing audit logs and how it may affect the system's responsiveness and other functionalities. This option ensures that the bank can plan for any necessary infrastructure upgrades or adjustments in system configurations before the feature is activated.

upvoted 1 times

  [LordXander](#) 1 year, 1 month ago

Selected Answer: B

Just because other options make less sense

upvoted 1 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: B

B. Determine the impact of enabling the audit feature.

upvoted 1 times

  [nosavotor](#) 1 year, 3 months ago

Could someone help me confirm the accuracy of this data

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 258 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 258

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key.

What is the security model implemented by Jane to secure corporate messages?

- A. Zero trust network
- B. Secure Socket Layer (SSL)
- C. Transport Layer Security (TLS)
- D. Web of trust (WOT) Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  **LordXander** 1 year, 1 month ago

Selected Answer: D

CEHv12 3405 - D

upvoted 2 times

  **insaniunt** 1 year, 3 months ago

Selected Answer: D

D. Web of trust (WOT)

In a Web of Trust (WOT) model, users validate the authenticity of each other's public keys, creating a decentralized trust network. This approach is commonly used in Pretty Good Privacy (PGP) and other public-key cryptography systems.

upvoted 1 times

  **nosavotor** 1 year, 3 months ago

Team is this CEH method correct

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 262 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 262

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit.

Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

- A. CAST-128
- B. RC5
- C. TEA
- D. Serpent Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  [kenjeshry](#) 8 months, 2 weeks ago

Selected Answer: D

CEH p3331

Serpent uses a 128-bit symmetric block cipher with 128-, 192-, or 256-bit key sizes

It involves 32 operating rounds on four 32-bit word blocks using 8 variable S-boxes with 4-bit entry and 4-bit exit; each S-box parallelly works 32 times

upvoted 1 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: D

D. Serpent

Serpent is a symmetric key block cipher that meets the specified criteria and is suitable for integration into the software program described by Tony.

upvoted 3 times

  [nosavotor](#) 1 year, 3 months ago

I'm unsure about this ethical hacking strategy

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 271 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 271

Topic #: 1

[All 312-50v12 Questions]

Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.

Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?

A. WS-Work Processes

B. WS-Security **Most Voted**

C. WS-Policy

D. WSDL

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

 [e020fdc](#) 6 months, 1 week ago

Selected Answer: B

WS-Security (Web Services Security):

A standard extension to SOAP ✓

Provides a means for securing SOAP messages ✓

Supports:

Authentication (via tokens, usernames, X.509 certificates) ✓

Message integrity (via digital signatures) ✓

Message confidentiality (via encryption) ✓

Ensures secure communication in web services architecture ✓

 Other Options:

A. WS-Work Processes:

Not a defined standard in Web Services Architecture

 Not related to SOAP security

C. WS-Policy:

Used to describe policy assertions about web services (e.g., security, reliability)

 Describes capabilities/requirements but does not secure the messages itself

D. WSDL (Web Services Description Language):

XML-based language for describing web services interfaces

 Does not provide security or deal with SOAP message integrity

upvoted 1 times

 [shaody](#) 1 year, 3 months ago

Selected Answer: B

WS-Security: It is an extension of SOAP and aims to maintain the integrity and confidentiality of SOAP messages as well as to authenticate users.

upvoted 1 times

✉️👤 **LordXander** 1 year, 7 months ago

Selected Answer: B

CEHv12 - 1890

upvoted 2 times

✉️👤 **insaniunt** 1 year, 9 months ago

Selected Answer: B

Rebecca is using WS-Security to secure the communication. WS-Security is an extension of SOAP that provides a set of mechanisms to ensure the integrity and confidentiality of SOAP messages in web services

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 273 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 273

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.

What is the encryption software employed by Sam for securing the email messages?

- A. PGP
- B. SMTP
- C. GPG **Most Voted**
- D. S/MIME

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  [LordXander](#) 1 year, 1 month ago

Selected Answer: C

CEHv12 - 3402

upvoted 2 times

  [insaniunt](#) 1 year, 3 months ago

Selected Answer: C

Sam is using GPG (GNU Privacy Guard), which is a free implementation of the OpenPGP standard. GPG combines symmetric-key cryptography and asymmetric-key cryptography to provide a hybrid encryption approach, offering both speed and secure key exchange.

upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 274 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 274

Topic #: 1

[All 312-50v12 Questions]

Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

Which type of threat intelligence is used by Roma to secure the internal network?

- A. Operational threat intelligence
- B. Strategic threat intelligence
- C. Tactical threat intelligence
- D. Technical threat intelligence

D. Technical threat intelligence Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

 **shady** 1 year, 3 months ago

Selected Answer: D

Technical threat intelligence is directly fed into the security devices in digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

upvoted 1 times

 **kinaJ** 1 year, 4 months ago

Selected Answer: D

Explanation:

Operational threat intelligence: Provides information about specific threats against the organization. It is typically more focused on specific incidents and real-time situations.

Strategic threat intelligence: Provides a broader, long-term view of threats and trends. It is often used by senior management to inform policy and strategy.

Tactical threat intelligence: Focuses on the tactics, techniques, and procedures (TTPs) used by threat actors. It is generally used for understanding and mitigating specific threats.

Technical threat intelligence: Involves technical details about threats, such as indicators of compromise (IOCs) like IP addresses, domain names, file hashes, and malware signatures. This type of intelligence is used to configure security devices to detect and block malicious activities.

upvoted 3 times

 **LordXander** 1 year, 7 months ago

Selected Answer: D

CEHv12 - 66

upvoted 2 times

 **qwerty100** 1 year, 9 months ago

Selected Answer: D

D. Technical threat intelligence

upvoted 1 times

 **insaniunt** 1 year, 9 months ago

Selected Answer: D

Roma is using Technical threat intelligence to feed information into security devices to identify and block inbound and outbound malicious traffic. Technical threat intelligence typically provides detailed technical information about threats, such as indicators of compromise (IoCs) and specific details about the tactics, techniques, and procedures (TTPs) used by malicious actors.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 277 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 277

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks.

What is the type of threat intelligence collected by Arnold in the above scenario?

- A. Strategic threat intelligence
- B. Operational threat intelligence Most Voted
- C. Technical threat intelligence
- D. Tactical threat intelligence

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  **shaody** 1 year, 3 months ago

Selected Answer: B

It provides contextual information about security events and incidents that help defenders disclose potential risks, provide greater insight into attacker methodologies, identify past malicious activities, and perform investigations on malicious activity in a more efficient way.
upvoted 1 times

  **LordXander** 1 year, 7 months ago

Selected Answer: B

CEHv12 65/66
upvoted 2 times

  **qwerty100** 1 year, 9 months ago

Selected Answer: B

B. Operational threat intelligence
upvoted 2 times

  **insaniunt** 1 year, 9 months ago

Selected Answer: B

Arnold, in the described scenario, is collecting Operational threat intelligence. Operational threat intelligence focuses on the current and near-term threats, providing information about specific security events, incidents, and potential risks. It helps security professionals like Arnold understand attacker methodologies, identify malicious activities, and take appropriate actions.
upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 282 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 282

Topic #: 1

[All 312-50v12 Questions]

When considering how an attacker may exploit a web server, what is web server footprinting?

- A. When an attacker creates a complete profile of the site's external links and file structures
- B. When an attacker uses a brute-force attack to crack a web-server password
- C. When an attacker implements a vulnerability scanner to identify weaknesses
- D. When an attacker gathers system-level data, including account details and server names Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by qtygbapjpesdayazko at Feb. 24, 2024, 12:59 p.m.

Comments

e020fdc 6 months, 1 week ago

Selected Answer: D

ChatGPT also says D. Reasons why others are wrong:

- A. Creating a profile of external links and file structures
✗ This is closer to website spidering or content discovery, not footprinting at the system level.
- B. Using a brute-force attack
✗ This is an active attack method — not passive reconnaissance like footprinting.
- C. Using a vulnerability scanner
✗ This falls under vulnerability assessment or scanning, which usually comes after footprinting.
upvoted 1 times

3936e29 8 months, 1 week ago

Selected Answer: C

Well, I am not sure that D is correct in this specific case.

The question says "When considering how an attacker MAY EXPLOIT a WEB SERVER".

It's not general question about footprinting and getting knowledge about sites, employees, network range, physical location etc
It is question directed at web server footprinting in the context of exploitation.

I would say the answer is C, and this is about active footprinting that means finding services running and weaknesses (vulnerabilities) that could be exploited.

My answer is C.

upvoted 1 times

shaody 1 year, 3 months ago

Selected Answer: D

Gather valuable system-level data such as account details, operating system, software versions, server names, and database schema details
upvoted 1 times

kevin403 1 year, 3 months ago

Selected Answer: D

D. I got full marks and this is one of the questions.

upvoted 2 times

LordXander 1 year, 7 months ago

Selected Answer: D

CEHv12 - 1810

upvoted 2 times

⊕  **ariel004** 1 year, 8 months ago

old Question #: 362 from V11 - it's D

upvoted 1 times

⊕  **sh4dali** 1 year, 8 months ago

Selected Answer: D

D is correct

upvoted 3 times

⊕  **ET0722** 1 year, 8 months ago

The course speaks of a "blueprint" that will be created when the footprinting is complete. This would include the server names, account details, and domains that are available from the company's footprint. I would think that D is the more accurate answer. Ref: Module 2 pg 107-108.

upvoted 1 times

⊕  **qwerty100** 1 year, 9 months ago

Selected Answer: D

D. When an attacker gathers system-level data, including account details and server names

upvoted 1 times

⊕  **nosavotor** 1 year, 9 months ago

Team is this CEH method correct

upvoted 1 times

⊕  **LeongCC** 1 year, 9 months ago

Selected Answer: A

I think the A is more suitable

A. When an attacker creates a complete profile of the site's external links and file structures remains the best fit for the concept of web server footprinting as described in the context of the original question.

upvoted 4 times

 EXAM 312-50V12 TOPIC 1 QUESTION 284 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 284

Topic #: 1

[All 312-50v12 Questions]

James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources.

What is the framework used by James to conduct footprinting and reconnaissance activities?

- A. OSINT framework **Most Voted**
- B. WebSploit Framework
- C. Browser Exploitation Framework
- D. SpeedPhish Framework

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

 [e020fdc](#) 6 months, 1 week ago

Selected Answer: A

Yar it do be A.

ChatGPT invalidates the others as follows

B. WebSploit Framework:

A tool for network and web application penetration testing, not specifically focused on reconnaissance/footprinting.

C. Browser Exploitation Framework (BeEF):

Designed for exploiting browser vulnerabilities, mainly for post-exploitation rather than information gathering.

D. SpeedPhish Framework:

Used for phishing attack simulation, not for reconnaissance or footprinting.

upvoted 1 times

 [kenjeshry](#) 8 months, 2 weeks ago

Selected Answer: A

CEHv12 p207

OSINT Framework is an open-source intelligence gathering framework that helps security professionals for performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering.

upvoted 1 times

 [LordXander](#) 1 year, 1 month ago

Selected Answer: A

open-source framework - literally OSINT framework

upvoted 1 times

 [insaniunt](#) 1 year, 3 months ago

Selected Answer: A

A. OSINT framework

upvoted 3 times

 EXAM 312-50V12 TOPIC 1 QUESTION 288 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 288

Topic #: 1

[All 312-50v12 Questions]

Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server.

Which of the following tools is used by Jack to perform vulnerability scanning?

- A. Infoga
- B. NCollector Studio
- C. Netsparker **Most Voted**
- D. WebCopier Pro

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  [e020fdc](#) 6 months, 1 week ago

Selected Answer: C

A. Infoga

Purpose: Email information gathering (OSINT).

B. NCollector Studio

Purpose: Web crawler and offline website downloader.

C. Netsparker

Purpose: Automated vulnerability scanning tool for web applications. Scans for: SQL injection, XSS, Misconfigurations, Other web-related vulnerabilities

D. WebCopier Pro

Purpose: Offline web browser/downloader.

upvoted 1 times

  [shaody](#) 1 year, 3 months ago

C is correct.

upvoted 1 times

  [yicx1](#) 1 year, 5 months ago

Selected Answer: C

Netsparker is a leading web vulnerability management software tool

upvoted 2 times

  [insaniunt](#) 1 year, 9 months ago

Selected Answer: C

C. Netsparker

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 293 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 293

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks.

What is the technique employed by Kevin to improve the security of encryption keys?

A. Key stretching Most Voted

- B. Public key infrastructure
C. Key derivation function
D. Key reinstallation

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  **shaody** 1 year, 3 months ago

Selected Answer: A

In the key stretching technique, the initial key is given as input to an algorithm that generates an enhanced key. The key must be sufficiently resistant to brute-force attacks.

upvoted 1 times

  **LordXander** 1 year, 7 months ago

Selected Answer: A

CEHv12 - 3462

upvoted 2 times

  **ariel004** 1 year, 8 months ago

C:

Based on the description provided, Kevin employed a technique called a key derivation function (KDF) to enhance the security of encryption keys. A KDF is a cryptographic algorithm that takes an input key and generates a derived key that is resistant to brute-force attacks.

upvoted 1 times

  **insaniunt** 1 year, 9 months ago

Selected Answer: A

A. Key stretching

Key stretching is a technique that increases the computational difficulty of deriving the original key, making it more resistant to brute-force attacks. It is commonly used to enhance the security of passwords and encryption keys.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 295 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 295

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

Which of the following types of fault injection attack is performed by Robert in the above scenario?

- A. Frequency/voltage tampering
- B. Optical, electromagnetic fault injection (EMFI)
- C. Temperature attack
- D. Power/clock/reset glitching Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  **LordXander** 1 year, 1 month ago

Selected Answer: D

CEHv12 - 2818

upvoted 2 times

  **insaniunt** 1 year, 3 months ago

Selected Answer: D

D. Power/clock/reset glitching

upvoted 4 times

EXAM 312-50V12 TOPIC 1 QUESTION 299 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 299

Topic #: 1

[\[All 312-50v12 Questions\]](#)

BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory.

What is this mechanism called in cryptography?

- A. Key archival
- B. Certificate rollover
- C. Key escrow Most Voted
- D. Key renewal

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  **shaody** 1 year, 3 months ago

Selected Answer: C

Key escrow is a key exchange arrangement in which essential cryptographic keys are stored with a third party in escrow.
upvoted 1 times

  **insaniunt** 1 year, 9 months ago

Selected Answer: C

The mechanism implemented to recover cryptographic keys from Active Directory in the context of BitLocker encryption is called:

- C. Key escrow
- upvoted 1 times

EXAM 312-50V12 TOPIC 1 QUESTION 306 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 306

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company.

What is the API vulnerability revealed in the above scenario?

- A. No ABAC validation **Most Voted**
- B. Business logic flaws
- C. Improper use of CORS
- D. Code injections

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [qtygbapjpesdayazko](#) at Feb. 24, 2024, 12:59 p.m.

Comments

  [kenjeshry](#) 8 months, 1 week ago

Selected Answer: A

CEHv12 p2095

upvoted 1 times

  [shaody](#) 1 year, 3 months ago

Selected Answer: A

Lack of proper ABAC validation allows attackers to gain unauthorized access to API objects or actions to perform viewing, updating, or deleting.
upvoted 1 times

  [qwertyst100](#) 1 year, 8 months ago

Selected Answer: A

A. No ABAC validation

upvoted 1 times

  [insaniunt](#) 1 year, 9 months ago

Selected Answer: A

A. No ABAC validation. This means that the API does not implement proper attribute-based access control (ABAC) to verify the permissions of the users who request access to the API object

upvoted 2 times

EXAM 312-50 TOPIC 3 QUESTION 6 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 6

Topic #: 3

[\[All 312-50 Questions\]](#)

A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:

Untrust (Internet) - (Remote network = 217.77.88.0/24)
DMZ (DMZ) - (11.12.13.0/24)
Trust (Intranet) - (192.168.0.0/24)

The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

- A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389
- B. Permit 217.77.88.12 11.12.13.50 RDP 3389**
- C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
- D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

[Hide Answer](#)

Suggested Answer: B

by  **Kiruma** at March 7, 2024, 5:29 a.m.

Comments

 **a4687eb** 1 year, 4 months ago

Answer is B because we talk about static IP of remote host and static IP of server in DMZ and both IPs in answer B are in the range of addresses given in question

upvoted 1 times

 **Kiruma** 1 year, 8 months ago

Answer is B this because of the static IP address in play

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 33 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 33

Topic #: 4

[\[All 312-50 Questions\]](#)

Which of the following is a client-server tool utilized to evade firewall inspection?

- A. tcp-over-dns
- B. kismet
- C. nikto
- D. hping A

[Hide Answer](#)

Suggested Answer: *Explanation*

by  Bright07 at Feb. 9, 2020, 11:23 p.m.

Comments

  milan_todorovic 1 year, 2 months ago

Yes, A is correct ans..

upvoted 2 times

  Bright07 2 years, 3 months ago

Ans A Tcp-over-dns

upvoted 3 times

EXAM 312-50 TOPIC 5 QUESTION 47 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 47

Topic #: 5

[\[All 312-50 Questions\]](#)

Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

- A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security **Most Voted**
- B. Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
- C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
- D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors A

[Hide Answer](#)

Suggested Answer: Explanation

Community vote distribution

A (100%)

by  [Bright07](#) at Feb. 11, 2020, 12:27 a.m.

Comments

  [Novmejst](#) 1 year, 1 month ago

Selected Answer: A

The U.S. Computer Security Incident Response Team (CSIRT) provides incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security. Therefore, the correct option is A.

upvoted 1 times

  [celesgita](#) 2 years, 6 months ago

Selected Answer: A

A is correct

upvoted 1 times

  [Adbucket](#) 3 years, 1 month ago

Agree A

upvoted 1 times

  [Bright07](#) 4 years, 3 months ago

A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
upvoted 4 times

EXAM 312-50 TOPIC 8 QUESTION 91 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 91

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

- A. Use cryptographic storage to store all PII
- B. Use encrypted communications protocols to transmit PII
- C. Use full disk encryption on all hard drives to protect PII
- D. Use a security token to log into all Web applications that use PII

[Hide Answer](#)

Suggested Answer: A

As a matter of good practice any PII should be protected with strong encryption.

References: <https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying-information>

by  [Bright07](#) at Feb. 12, 2020, 2:54 a.m.

Comments

  [Deliman](#) 1 year, 2 months ago

I think B is the correct answer
upvoted 1 times

  [Luukman](#) 1 year, 8 months ago

Bad question. If my website is vulnerable (OWASP: sql injection, csrf, or parameter tampering) none of the answers help..
upvoted 1 times

  [Grezavi](#) 1 year, 11 months ago

A. Justification: Cryptography is Encryption. Storing is any time the data is in any type of memory. B -> A but A is more comprehensive and would cover transmission memory, servers, hard disks etc. It is a more comprehensive answer.
upvoted 2 times

  [cehexam](#) 2 years ago

For Me A and B is the answer but now which is the most correct?.. as they asked for web application and not storage, I will pick B. storage is not done on web application level but on DB/server level
upvoted 2 times

  [IamStuding](#) 2 years, 3 months ago

Also for me is B. We are talking about web services and here encrypted communications are the most important.
upvoted 2 times

  [jasonderules](#) 3 years, 2 months ago

I think it is B also.
upvoted 1 times

  [Bright07](#) 3 years, 3 months ago

Use encrypted communications protocols to transmit PII. Even According to your comment, the right answer is B. I don't know the reason why a lot of website is choosing cryptographic storage. If you choose A as your answer can you give the reason because it has become the bone of contention. Thanks. If there is no reason then B. is the right answer.
upvoted 2 times

EXAM 312-50 TOPIC 2 QUESTION 15 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 15

Topic #: 2

[\[All 312-50 Questions\]](#)

A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

- A. Information reporting
- B. Vulnerability assessment
- C. Active information gathering
- D. Passive information gathering Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [greeklover84](#) at June 9, 2024, 6:42 p.m.

Comments

  [greeklover84](#) 11 months, 3 weeks ago

[Selected Answer: D](#)

agree D.

upvoted 1 times

EXAM 312-50 TOPIC 2 QUESTION 21 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 21

Topic #: 2

[\[All 312-50 Questions\]](#)

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. Most Voted

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

D (100%)

by  [greeklover84](#) at June 9, 2024, 6:55 p.m.

Comments

  [greeklover84](#) 11 months, 3 weeks ago

Selected Answer: D

why not D ?

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 1 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 1

Topic #: 4

[\[All 312-50 Questions\]](#)

When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

- A. Drops the packet and moves on to the next one
- B. Continues to evaluate the packet until all rules are checked
- C. Stops checking rules, sends an alert, and lets the packet continue **Most Voted**
- D. Blocks the connection with the source IP address in the packet

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by  [bic3p](#) at Aug. 23, 2024, 6:55 a.m.

Comments

  **Eyebullet** 8 months ago

Selected Answer: B

By default Snort will continue to check all the rules. Unless explicitly configured to drop.
upvoted 1 times

  **bic3p** 1 year, 3 months ago

Selected Answer: C

The correct answer is C. Stops checking rules, sends an alert, and lets the packet continue.
When an alert rule is matched in a network-based IDS like Snort, the IDS will:
Stop checking rules: Once a rule is matched, Snort will stop evaluating the packet against the remaining rules.
Send an alert: The IDS will generate an alert to notify the system administrator or security team about the potential threat.
Let the packet continue: The packet will be allowed to continue through the network, as the IDS is only monitoring and alerting, not blocking traffic.
upvoted 2 times

EXAM 312-50 TOPIC 3 QUESTION 9 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 9

Topic #: 3

[\[All 312-50 Questions\]](#)

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted. Which cryptography attack is the student attempting?

- A. Man-in-the-middle attack
- B. Brute-force attack
- C. Dictionary attack
- D. Session hijacking

[Hide Answer](#)

Suggested Answer: C

by  Chogi_ at Aug. 24, 2024, 10:43 a.m.

Comments

  Chogi_ 1 year, 3 months ago

Dictionary attack involves using a list of common words or passwords, which is a specific type of brute-force attack
upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 16 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 16

Topic #: 4

[\[All 312-50 Questions\]](#)

Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

- A. NMAP -PN -A -O -sS 192.168.2.0/24
- B. NMAP -P0 -A -O -p1-65535 192.168.0/24 Most Voted
- C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
- D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [pindarots](#) at Feb. 22, 2020, 2:10 p.m.

Comments

  **Pragdeashwar** 1 year, 1 month ago

answer is C "NMAP -P0 -A -sT -p0-65535 192.168.0/16"
upvoted 1 times

  **dorinh** 3 years, 6 months ago

Selected Answer: B

Class C private IP: 192.168.0.0/24
Flags:
-A: Enable OS detection, version detection, script scanning, and traceroute
-O: Enable OS detection
-p: Only scan specified ports (-p1-65535; ALL)
-PO[protocol list]: IP Protocol Ping
upvoted 1 times

  **jasonderules** 5 years, 3 months ago

A wont scan every port though...
upvoted 1 times

  **pindarots** 5 years, 3 months ago

Isn't answer A the right answer?
upvoted 1 times

  **Dave_Bigger** 5 years, 2 months ago

No, because without specifying the ports like answer B does, NMAP will only scan the top 1000 ports. B is the correct answer here.
upvoted 2 times

EXAM 312-50 TOPIC 4 QUESTION 19 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 19

Topic #: 4

[All 312-50 Questions]

A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

- A. Spoofing an IP address
- B. Tunneling scan over SSH
- C. Tunneling over high port numbers
- D. Scanning using fragmented IP packets Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (80%) B (20%)

by  pindarots at Feb. 22, 2020, 2:17 p.m.

Comments

 **pindarots** Highly Voted 5 years, 9 months ago

Scanning using fragmented IP packets?
upvoted 10 times

 **bic3p** Most Recent 1 year, 2 months ago

Selected Answer: B
some ids and ips have the ability to connect the fragmented packets and hence couldnt be the answer. So option b is correct
upvoted 1 times

 **Router** 2 years, 9 months ago

it cant be D cos A is also used to bypass FW.
upvoted 1 times

 **salei** 3 years ago

Selected Answer: D
While the question says the pen tester is trying to scan the internal network from the internet (let's assume static nat or something), then this is the correct answer: <https://nmap.org/book/man-bypass-firewalls-ids.html>

-f (fragment packets); --mtu (using the specified MTU)

The -f option causes the requested scan (including ping scans) to use tiny fragmented IP packets. The idea is to split up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and other annoyances to detect what you are doing

upvoted 2 times

 **swetty** 3 years ago

Selected Answer: D
IP fragmentation scan is a method to attempt evasion of IDS
upvoted 1 times

 **Goki_28** 3 years, 5 months ago

Selected Answer: D
Scanning using fragmented IP packets.
upvoted 1 times

 **Goki_28** 3 years, 5 months ago

Scanning using fragmented IP packets.

upvoted 1 times

✉ **Hacker100** 4 years, 2 months ago

Correct answer is D. Scanning using fragmented IP packets

upvoted 2 times

✉ **brider** 5 years, 7 months ago

B. Tunneling scan over SSH

upvoted 3 times

✉ **virus9** 5 years, 1 month ago

An already established connection in the network is needed first.

<https://isc.sans.edu/forums/diary/Tunneling+scanners+or+really+anything+over+SSH/24286/>

upvoted 1 times

✉ **virus9** 5 years, 1 month ago

But since the question says, "penetration tester" and not a hacker, it means he might already been given the access.

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 8 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 8

Topic #: 4

[\[All 312-50 Questions\]](#)

A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

- A. SSL
- B. Mutual authentication
- C. IPSec
- D. Static IP addresses

[Hide Answer](#)

Suggested Answer: C

by  [sparrowjack](#) at Oct. 22, 2024, 6:53 p.m.

Comments

  [sparrowjack](#) 1 year, 1 month ago

Mutual authentication ensures that both the client and the server authenticate each other before any sensitive data is exchanged. This will reduce the risk of a MitM attack as per my understanding

upvoted 2 times

EXAM 312-50 TOPIC 4 QUESTION 29 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 29

Topic #: 4

[\[All 312-50 Questions\]](#)

Which of the following items of a computer system will an anti-virus program scan for viruses?

- A. Boot Sector
- B. Deleted Files
- C. Windows Process List
- D. Password Protected Files

[Hide Answer](#)

Suggested Answer: A

by  **jasonderules** at Feb. 29, 2020, 9:53 p.m.

Comments

  **cupcake** 1 year, 3 months ago

yes c is correct along with a
upvoted 1 times

  **jasonderules** 2 years, 3 months ago

C is also correct
upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 166 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 166

Topic #: 8

[\[All 312-50 Questions\]](#)

In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.

Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.

Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'?

- A. NT:LM
- B. LM:NT**
- C. LM:NTLM
- D. NTLM:LM

[Hide Answer](#)

Suggested Answer: B

by  Chogi_ at Nov. 24, 2024, 8:10 a.m.

Comments

  **Chogi_** 1 year ago
Why not letter A. NT:LM?
upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 251 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 251

Topic #: 8

[\[All 312-50 Questions\]](#)

The following are types of Bluetooth attack EXCEPT_____?

- A. Bluejacking
- B. Bluesmaking Most Voted
- C. Bluesnarfing
- D. Bluedriving

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

 B (100%)

by  [Chogi_](#) at Nov. 26, 2024, 12:39 p.m.

Comments

  [Chogi_](#) 1 year ago

Selected Answer: B

not recognized as bluetooth attack
upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 10 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 10

Topic #: 1

[All 312-50v13 Questions]

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 **Most Voted**

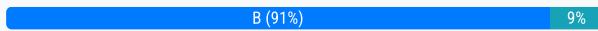
C. Command and control

D. Exploitation

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by JOHNBOO at Jan. 2, 2025, 1:36 p.m.

Comments

lopesjaf 4 months ago

Selected Answer: B

Since you are creating the backdoor to deliver it, you are in the Weaponization stage.

upvoted 1 times

cyb3r321 4 months, 3 weeks ago

Selected Answer: B

Weaponization

upvoted 1 times

getaseadsss 9 months, 1 week ago

Selected Answer: B

Weaponization

upvoted 1 times

Stephanie0208 10 months, 2 weeks ago

Selected Answer: B

I changed my mind...

Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim.

For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary.

upvoted 2 times

Stephanie0208 10 months, 2 weeks ago

Selected Answer: D

Youare creating a client-side backdoor to send it to the employees via email.

However, there is no "Delivery" option.

Then I would suggest D. Exploitation.

Exploitation

After the weapon is transmitted to the intended victim, exploitation triggers the adversary's malicious code to exploit a vulnerability in the operating system, application, or server on a target system. At this stage, the organization may face threats such as authentication and authorization attacks, arbitrary code execution, physical security threats, and security misconfiguration. Activities of the adversary include the following:

- o Exploiting software or hardware vulnerabilities to gain remote access to the target system

upvoted 1 times

 **MHafizC** 10 months, 2 weeks ago

Selected Answer: B

It's weaponization. The stage preparing tools after gathering enough information.

upvoted 1 times

 **cb56e21** 10 months, 2 weeks ago

Selected Answer: B

It is weaponization

upvoted 1 times

 **935f9c3** 10 months, 3 weeks ago

Selected Answer: B

B. Weaponization

upvoted 2 times

 **JOHNBOO** 11 months ago

Selected Answer: B

B Weaponization is the correct option

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 137 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 137

Topic #: 1

[\[All 312-50v13 Questions\]](#)

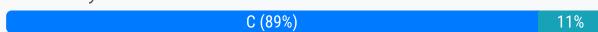
A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exhort the TGS tickets from memory for offline cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?

- A. Perform a system reboot to clear the memory
- B. Delete the compromised user's account
- C. Change the NTLM password hash used to encrypt the ST Most Voted
- D. Invalidate the TGS the attacker acquired

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by  [Jez92](#) at Jan. 9, 2025, 7:18 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: C

C. Change the NTLM password hash used to encrypt the ST — effectively change the service account password to invalidate existing tickets.
upvoted 2 times

  [msrkntk](#) 7 months ago

Selected Answer: D

A Kerberoasting attack is a technique that exploits the Kerberos authentication protocol to obtain the password hash of a service account that has a Service Principal Name (SPN). An attacker can request a service ticket (TGS) for the SPN using a valid user's ticket (TGT) and then attempt to crack the password hash offline. To prevent the attacker from using the TGS to access the service, the system administrator should invalidate the TGS as soon as possible. This can be done by changing the password of the service account, which will generate a new password hash and render the old TGS useless. Alternatively, the system administrator can use tools like Mimikatz to purge the TGS from the memory of the domain controller or the client system.

upvoted 1 times

  [NikoTomas](#) 8 months, 2 weeks ago

Selected Answer: C

Correct is C:
o As the attacker already extracted TGS ticket from memory, the attack continues as follows:

1. Perform Offline Brute-Force on the Ticket
• Since the TGS ticket is encrypted with the service account's NTLM hash, the attacker cracks it offline using Hashcat or John the Ripper.

2. Obtain the Service Account's Cleartext Password
• Once cracked, the attacker can authenticate as the service account, potentially escalating to domain admin.

o So the password of service account (which are usually targets of this attack) is the main goal of the attacker.
o We need to change NTLM password (i. e. account password... which also changes the NTLM hash as it is derived from the password) to avoid attacker accessing the service account with password from the cracked NTLM hash, which he/she already has.

upvoted 4 times

  [NikoTomas](#) 8 months, 2 weeks ago

Incorrect:

A) and D) – It's too late for clearing the memory (A) and invalidating TGS ticket (D) as the attacker already has the TGS ticket containing service account's NTLM hash.

B) – Delete compromised USER account – INCORRECT as the compromised USER account is not target of this attack (it has usually low privileges, so attacker is looking for service accounts with higher priv.). USER account has been already compromised (i. e. attacker already has credentials) and utilized it for obtaining TGS of service account with higher privileges.

upvoted 1 times

 **Gibsonmd** 8 months, 2 weeks ago

Selected Answer: C

A Kerberoasting attack involves an attacker obtaining a Ticket Granting Service (TGS) ticket from memory and attempting to crack it offline to extract the service account's password hash. Since the attacker was stopped before completing the attack, the immediate remediation step should focus on preventing further exploitation.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 233 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 233

Topic #: 1

[All 312-50v13 Questions]

Martin, a Certified Ethical Hacker (CEH), is conducting a penetration test on a large enterprise network. He suspects that sensitive information might be leaking out of the network. Martin decides to use network sniffing as part of his testing methodology. Which of the following sniffing techniques should Martin employ to get a comprehensive understanding of the data flowing across the network?

A. Raw Sniffing **Most Voted**

B. MAC Flooding

C. ARP Poisoning

D. DNS Poisoning

[Hide Answer](#)

Suggested Answer: A

Community vote distribution



by [Jez92](#) at Jan. 10, 2025, 1:14 p.m.

Comments

✉ **lopesjaf** 3 months, 4 weeks ago

Selected Answer: B

B. MAC Flooding: This is an active attack to overwhelm a switch's CAM table, forcing it into fail-open mode and turning it into a hub, so traffic is broadcast. It can help sniff traffic on a switched network.

upvoted 2 times

✉ **e30b32d** 6 months, 1 week ago

Selected Answer: A

keyword "network sniffing", Raw Sniffing, all other will cause problems.

upvoted 1 times

✉ **Cherubael** 6 months, 2 weeks ago

Selected Answer: A

During an actual Penetration Test you would NEVER do an ARP Poisoning attack especially if the question did not specify this was in a test environment. That is how you go out-of-scope real quick and get kicked off the premises or worse, sued for damages.

upvoted 2 times

✉ **NikoTomas** 8 months, 1 week ago

Selected Answer: A

A - Raw sniffing.

upvoted 1 times

✉ **killwitch** 8 months, 2 weeks ago

Selected Answer: C

ARP (Address Resolution Protocol) poisoning, also known as ARP spoofing, is a highly effective sniffing technique used by attackers and penetration testers to intercept network traffic on switched networks.

Since modern networks use switches (which segment traffic to prevent traditional sniffing), Martin needs a way to redirect traffic through his machine. ARP poisoning allows him to do this by tricking devices into sending their traffic to him instead of the intended recipient.

upvoted 1 times

✉ **Dogeo** 9 months ago

Selected Answer: C

is not a commonly recognized term in the context of network sniffing techniques. It may refer to passive packet capture, but it doesn't specifically describe a method that would enable an ethical hacker to manipulate or redirect traffic, as required for a comprehensive understanding of network data flow.

upvoted 2 times

 **bibibi** 9 months ago

Selected Answer: A

B, C and D are not sniffing technique

upvoted 3 times

 **NikoTomas** 8 months, 1 week ago

Agree.

Moreover, they are causing mess in the network and non-standard communication behaviors, which complicates investigation required to find out how data are leaking.

Raw Sniffing is correct for me.

upvoted 1 times

 **MHafizC** 10 months, 2 weeks ago

Selected Answer: A

It's sniffing across the network and involving suspicion on leaking out of the network. RAW Sniffing is correct.

upvoted 3 times

 **Jez92** 10 months, 3 weeks ago

Selected Answer: C

should be ARP Poisoning

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 114 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 114

Topic #: 1

[All 312-50v13 Questions]

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 FIN/ACK 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 **Most Voted**
- D. ACK flag probe scan

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  Bob00036 at Jan. 12, 2025, 2:12 p.m.

Comments

 **lopesjaf** 4 months ago

Selected Answer: C

TCP Maimon scan sends FIN/ACK probes and relies on the behavior of the target responding with an RST packet to indicate a closed port.
upvoted 1 times

 **e30b32d** 6 months, 1 week ago

Selected Answer: C

In a TCP Maimon scan, the attacker sends a FIN/ACK combination (or sometimes just a FIN or FIN/PSH/URG flag combo) to a target port. The response behavior helps determine the port's status:

If the port is closed, the target responds with an RST packet.

If the port is open or filtered, no response is sent.

upvoted 1 times

 **killwitch** 8 months, 3 weeks ago

Selected Answer: C

C. TCP Maimon scan.

Sam sends FIN/ACK probes and gets RST packet in response.

FIN/ACK probes followed by RST response follows exactly the Maimon scan definition.

upvoted 2 times

 **marcel9999** 8 months, 4 weeks ago

Selected Answer: C

This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FIN/ACK. 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.

upvoted 2 times

 **Dogeo** 9 months, 3 weeks ago

Selected Answer: C

In a TCP Maimon scan, the attacker sends a FIN/ACK probe to the target.

upvoted 2 times

 **pindinga1** 10 months ago

Selected Answer: C

this response is C , TCP Maimon scan

upvoted 2 times

 **Bob00036** 10 months, 2 weeks ago

Selected Answer: C

<https://nmap.org/book/scan-methods-maimon-scan.html>

upvoted 3 times

EXAM 312-50 TOPIC 8 QUESTION 324 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 324

Topic #: 8

[\[All 312-50 Questions\]](#)

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

- A. har.txt
- B. SAM file**
- C. wwwroot
- D. Repair file

[Hide Answer](#)

Suggested Answer: B

by  **jasonderules** at March 4, 2020, 6:53 p.m.

Comments

 **alismaini** 1 year, 4 months ago

Is the question even complete?

upvoted 1 times

 **jasonderules** 4 years, 8 months ago

no extract?

upvoted 2 times

EXAM 312-50 TOPIC 8 QUESTION 366 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 366

Topic #: 8

[\[All 312-50 Questions\]](#)

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

- A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
- B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer [1] Steganography techniques
- D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

[Hide Answer](#)

Suggested Answer: C

by  [jasonderules](#) at March 4, 2020, 7:23 p.m.

Comments

 [salei](#) 1 year, 1 month ago

C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
upvoted 1 times

 [phmb14](#) 3 years, 8 months ago

C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
upvoted 3 times

 [jasonderules](#) 3 years, 8 months ago

bad formatting?
upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 23 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 23

Topic #: 1

[All 312-50v13 Questions]

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 Most Voted
- D. EarthExplorer

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  Rangnarok at Jan. 15, 2025, 11:43 a.m.

Comments

 **lopesjaf** 4 months ago

Selected Answer: C

JXplorer: An open-source LDAP browser and editor that allows querying and browsing LDAP directories. ✓
upvoted 1 times

 **mesh_with_u** 5 months, 3 weeks ago

Selected Answer: C

JXplorer - JXplorer is a Java-based LDAP browser and editor used to manage and interact with LDAP directories. It allows users to browse, search, and modify LDAP data, including importing and exporting LDIF files. JXplorer supports LDAP version 3.0 and also provides limited support for LDAP version 2 and DSML.

upvoted 3 times

 **e30b32d** 6 months, 1 week ago

Selected Answer: C

JXplorer: It is a popular open-source LDAP browser and directory client. It allows users to connect to LDAP servers and query for sensitive information such as usernames, addresses, organizational units, and server details. This makes it a useful tool for gathering information during reconnaissance.

upvoted 2 times

 **gohchinwei** 6 months, 2 weeks ago

Selected Answer: C

JXplorer is a cross platform LDAP browser and editor. It is a standards compliant general purpose LDAP client that can be used to search, read and edit any standard LDAP directory, or any directory service with an LDAP or DSML interface.

It is highly flexible and can be extended and customised in a number of ways. JXplorer is written in java, and the source code and Ant build system are available via svn or as a packaged build for users who want to experiment or further develop the program.

JX is available in two versions; the free open source version under an OSI Apache 2 style licence, or in the JXWorkBench Enterprise bundle with built in reporting, administrative and security tools.

JX has been through a number of different versions since its creation in 1999; the most recent stable release is version 3.3.1, the August 2013 release.

upvoted 1 times

👤 **NikoTomas** 8 months, 3 weeks ago

Selected Answer: C

Correct: C (JXplorer)

- A. ike-scan = discover and fingerprint IKE hosts (IPsec VPN Servers)
- B. Zabasearch = for searching people contacts
- C. JXplorer = a cross platform LDAP browser and editor.
- D. EarthExplorer = looks like the satelite imagery tool

upvoted 4 times

👤 **Rangnarok** 10 months, 2 weeks ago

Selected Answer: C

The only tool that works with LDAP among the given choices

upvoted 2 times

 EXAM 312-50V13 TOPIC 1 QUESTION 42 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 42

Topic #: 1

[All 312-50v13 Questions]

In the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

- A. 4.0-6.0
- B. 3.9-6.9
- C. 3.0-6.9
- D. 4.0-6.9 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by Rangnarok at Jan. 15, 2025, 3:06 p.m.

Comments

lopesjaf 4 months ago

Selected Answer: D

In CVSS v3.1, the severity rating ranges are:

None: 0.0

Low: 0.1 – 3.9

Medium: 4.0 – 6.9

High: 7.0 – 8.9

Critical: 9.0 – 10.0

upvoted 2 times

killwitch 8 months, 2 weeks ago

Selected Answer: D

In the Common Vulnerability Scoring System (CVSS) v3.1, the severity ratings are classified as follows:

None: 0.0

Low: 0.1 - 3.9

Medium: 4.0 - 6.9

High: 7.0 - 8.9

Critical: 9.0 - 10.0

upvoted 3 times

NikoTomas 8 months, 3 weeks ago

Selected Answer: D

Correct is D (4.0 - 6.9)

Severity mapping table for particular CVSS versions:
<https://nvd.nist.gov/vuln-metrics/cvss>

upvoted 3 times

Dogeo 9 months ago

Selected Answer: A

The Medium severity rating in CVSS v3.1 applies to vulnerabilities with a score in the range of 4.0-6.0.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 130 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 130

Topic #: 1

[All 312-50v13 Questions]

In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with 'y' columns. Each table contains 'z' records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include 'UNION SELECT' statements and 'DBMS_XSLPROCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted ' $E=xyz*u$ '. Assuming ' $x=4$ ', ' $y=2$ ', and varying ' z ' and ' u ', which situation is likely to result in the highest extracted data volume?

- A. $z=600, u=2$: The attacker devises 2 SQL payloads, each aimed at tables holding 600 records, affecting all columns across all tables.
- B. $z=550, u=2$: Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables.
- C. $z=500, u=3$: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables.
- D. $z=400, u=4$: The attacker constructs 4 SQL payloads, each focusing on tables with 400 records, influencing all columns of all tables.

Most Voted

Hide Answer

Suggested Answer: D

Community vote distribution

D (100%)

by  MHafizC at Jan. 15, 2025, 6:56 p.m.

Comments

  lopesjaf 4 months ago

Selected Answer: D

The highest extracted data volume corresponds to the highest E
upvoted 1 times

  HazalAlenazi 9 months, 3 weeks ago

Selected Answer: D

$A=4 \times 2 \times 600 \times 2 = 9600$
 $B=4 \times 2 \times 550 \times 2 = 8800$
 $C=4 \times 2 \times 500 \times 3 = 12000$
 $D=4 \times 2 \times 400 \times 4 = 12800$
so the answer is D
upvoted 3 times

  MHafizC 10 months, 2 weeks ago

Selected Answer: D

If all are under same value for x and y , that's just left with z and u .
So the highest result from the multiplication of z and u should be the answer.
In this case, D is the highest.
upvoted 3 times

 EXAM 312-50V13 TOPIC 1 QUESTION 131 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 131

Topic #: 1

[All 312-50v13 Questions]

A large enterprise has been experiencing sporadic system crashes and instability, resulting in limited access to its web services. The security team suspects it could be a result of a Denial of Service (DoS) attack. A significant increase in traffic was noticed in the network logs, with patterns suggesting packet sizes exceeding the prescribed size limit. Which among the following DoS attack techniques best describes this scenario?

- A. Smurf attack
- B. UDP flood attack
- C. Pulse wave attack
- D. Ping of Death attack Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  **MHafizC** at Jan. 15, 2025, 6:58 p.m.

Comments

 **lopesjaf** 4 months ago

Selected Answer: D

Ping of Death attack is a classic DoS attack where oversized or malformed packets (larger than the maximum allowed IP packet size of 65,535 bytes) are sent to the target, causing crashes or instability.

upvoted 1 times

 **91a0021** 9 months ago

Selected Answer: D

A Ping of Death (PoD) attack occurs when an attacker sends malformed or oversized ICMP packets (greater than 65,535 bytes) to a target system. Many systems cannot handle oversized packets properly, causing buffer overflows, crashes, or system instability. The packets exceed the normal size limit, which matches the behavior observed in the network logs.

This attack was common in older systems but remains a concern for legacy infrastructure or unpatched devices.

upvoted 2 times

 **Dogeo** 9 months, 3 weeks ago

Selected Answer: D

Ping of Death, where the attack involves sending pings (ICMP echo requests) that exceed the maximum allowable size

upvoted 1 times

 **pindinga1** 10 months ago

Selected Answer: D

correct answer is D "Ping of Death attack"

upvoted 1 times

 **MHafizC** 10 months, 2 weeks ago

Selected Answer: D

The statement of "packet sizes exceeding the prescribed size limit" is referring to Ping of Death attack.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 141 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 141

Topic #: 1

[All 312-50v13 Questions]

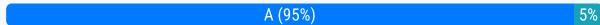
An organization suspects a persistent threat from a cybercriminal. They hire an ethical hacker, John, to evaluate their system security. John identifies several vulnerabilities and advises the organization on preventive measures. However, the organization has limited resources and opts to fix only the most severe vulnerability. Subsequently, a data breach occurs exploiting a different vulnerability. Which of the following statements best describes this scenario?

- A. The organization is at fault because it did not fix all identified vulnerabilities. **Most Voted**
- B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.
- C. John is at fault because he did not emphasize the necessity of patching all vulnerabilities.
- D. The organization is not at fault because they used their resources as per their understanding.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

 A (95%) 5%

by  [MHafizC](#) at Jan. 15, 2025, 7:24 p.m.

Comments

 [MHafizC](#) **Highly Voted** 10 months, 2 weeks ago

Selected Answer: A

I would opt for A. John did what was tasked, and the company understood the risk, but they decided not to do an amendment accordingly.
upvoted 6 times

 [lopesjaf](#) **Most Recent** 4 months ago

Selected Answer: A

John, as an ethical hacker, fulfilled his duty by identifying several vulnerabilities and advising on preventive measures.

The organization made a risk-based decision to fix only the most severe issue, but knowingly left other vulnerabilities unpatched.

When a breach occurs due to one of the unfixed vulnerabilities, the responsibility lies with the organization for not addressing all known risks, even if resources were limited.

Ethical hackers recommend actions, but organizations are ultimately responsible for risk acceptance or mitigation decisions.

upvoted 1 times

 [killwitch](#) 8 months, 3 weeks ago

Selected Answer: A

Organization opted to fix only the most severe vulnerability.
Other vulnerabilities have been left open, so it's organization's fault.
upvoted 3 times

 [marcel9999](#) 8 months, 4 weeks ago

Selected Answer: A

John was hired and created his report, the company is then responsible to fix..
upvoted 4 times

 [HazalAlenazi](#) 9 months, 3 weeks ago

Selected Answer: B

The Organization's Responsibility:
1- They had limited resources, but prioritizing only one vulnerability was a poor risk management decision.
2- Cybersecurity is about holistic protection, not just fixing one critical issue.
3- Ignoring other known vulnerabilities left the system exposed, leading to the data breach.

John's Responsibility:

- 1- As a professional ethical hacker, John should have clearly communicated the risks of leaving other vulnerabilities unpatched.
- 2- He should have provided a risk-based prioritization with possible mitigation strategies for all vulnerabilities.
- 3- If the organization couldn't patch everything, he could have suggested compensating controls (e.g., monitoring, segmentation, or temporary mitigations).

Cybersecurity is a shared responsibility, and this case reflects poor risk prioritization rather than a single point of failure.

upvoted 1 times

 **NikoTomas** 8 months, 2 weeks ago

I disagree.

This is not like in the cloud environment with "shared responsibility" model between provider and customer.

This is pure organizational decision to leave vulnerabilities without fixes.

Responsible is always management of the organization - they are driving the business and they must know what is crucial for reaching their goals and what level of risk can be accepted.

The security specialists (especially risk managers) just elaborate analysis and provide it to the management. The management must decide what to do. The security specialist don't have to know about all business affairs...

upvoted 1 times

 **pindinga1** 10 months ago

Selected Answer: A

I think John has nothing to do with the company's problems, he has just started to identify the problems, I think he is alternative A

upvoted 4 times

EXAM 312-50V13 TOPIC 1 QUESTION 150 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 150

Topic #: 1

[\[All 312-50v13 Questions\]](#)

A large organization has recently performed a vulnerability assessment using Nessus Professional, and the security team is now preparing the final report. They have identified a high-risk vulnerability, named XYZ, which could potentially allow unauthorized access to the network. In preparing the report, which of the following elements would NOT be typically included in the detailed documentation for this specific vulnerability?

- A. Proof of concept (PoC) of the vulnerability, if possible, to demonstrate its potential impact on the system.
- B. The total number of high, medium, and low-risk vulnerabilities detected throughout the network. **Most Voted**
- C. The list of all affected systems within the organization that are susceptible to the identified vulnerability.
- D. The CVE ID of the vulnerability and its mapping to the vulnerability's name, XYZ.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  **MHafizC** at Jan. 15, 2025, 7:50 p.m.

Comments

 **lopesjaf** 4 months ago

Selected Answer: B

When preparing a detailed vulnerability report for a specific vulnerability (like XYZ), the documentation typically includes:

Proof of Concept (PoC) to show how the vulnerability can be exploited (Option A)

List of all affected systems susceptible to that vulnerability (Option C)

CVE ID and mapping to the vulnerability name for clear identification (Option D)

upvoted 1 times

 **91a0021** 9 months ago

Selected Answer: B

Listing the total number of vulnerabilities across the entire network is part of the overall assessment summary, not the detailed documentation for one specific vulnerability.

While the total count of vulnerabilities is relevant for trend analysis, it does not provide useful technical details about vulnerability XYZ specifically

upvoted 3 times

 **MHafizC** 10 months, 2 weeks ago

Selected Answer: B

The risk level is not mentioned in the book under the security vulnerability report.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 180 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 180

Topic #: 1

[All 312-50v13 Questions]

During a reconnaissance mission, an ethical hacker uses Maltego, a popular footprinting tool, to collect information about a target organization. The information includes the target's Internet infrastructure details (domains, DNS names, Netblocks, IP address information). The hacker decides to use social engineering techniques to gain further information. Which of the following would be the least likely method of social engineering to yield beneficial information based on the data collected?

- A. Dumpster diving in the target company's trash bins for valuable printouts
- B. Impersonating an ISP technical support agent to trick the target into providing further network details
- C. Shoulder surfing to observe sensitive credentials input on the target's computers **Most Voted**
- D. Eavesdropping on internal corporate conversations to understand key topics

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by MHafizC at Jan. 16, 2025, 8:27 a.m.

Comments

lopesjaf 4 months ago

Selected Answer: A

In the context of the question, the ethical hacker has already gathered Internet infrastructure details through Maltego — including domains, DNS names, IPs, etc. They're now shifting to social engineering to collect more information.

upvoted 1 times

paske 5 months, 1 week ago

Selected Answer: A

Correct A

upvoted 1 times

NikoTomas 8 months, 1 week ago

Selected Answer: C

Choosing C) because with information gathered till now (domains, DNS names, Netblocks, IP address information) the next logical step would be utilizing the and/or extending the gathered information, which is described in these 3 options:

--> A) search for new information in trash – extend information base
--> B) impersonate an ISP technician – extend information base about networks, domains, etc...
--> D) use gathered knowledge about networks and evesdrop there... (maybe you don't have physical access but there can be WiFi signal...)

C) lefts – shoulder surfing is LEAST likely method of social engineering to yield information based on the data collected.

upvoted 1 times

GibsonD 8 months, 2 weeks ago

Selected Answer: C

The ethical hacker has collected infrastructure-related data (e.g., IP addresses, DNS details, domains, Netblocks) and now intends to use social engineering to extract more information. The most effective social engineering techniques in this case would involve leveraging the collected data to impersonate a trusted entity or extract information from employees.

upvoted 2 times

NikoTomas 8 months, 1 week ago

Read question properly:

"would be the LEAST likely method of social engineering to yield beneficial information "

upvoted 1 times

 **Dogeo** 9 months, 2 weeks ago

Selected Answer: D

Eavesdropping on corporate conversations may provide general business intelligence but is unlikely to reveal specific technical details like network configurations, IP ranges, or login credentials that would be useful for hacking.

upvoted 2 times

 **MHafizC** 10 months, 2 weeks ago

Selected Answer: C

You have to be inside the company and especially close to the target to do shoulder surfing. The answer is C.

upvoted 3 times

EXAM 312-50V13 TOPIC 1 QUESTION 184 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 184

Topic #: 1

[All 312-50v13 Questions]

Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (CHDB) with an emphasis on VPN footprinting. Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

- A. location: This operator finds information for a specific location **Most Voted**
- B. inurl: This operator restricts the results to only the pages containing the specified word in the URL
- C. link: This operator searches websites or pages that contain links to the specified website or page
- D. intitle: This operator restricts results to only the pages containing the specified term in the title

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (67%)

C (33%)

by  MHaFizC at Jan. 16, 2025, 8:41 a.m.

Comments

 **lopesjaf** 3 months, 4 weeks ago

Selected Answer: A

The question asks for the least useful Google search operator for VPN-related footprinting — in other words, which one provides the least value to an attacker trying to uncover sensitive VPN configuration or access data through Google hacking.

upvoted 1 times

 **KnightHeart** 6 months ago

Selected Answer: C

C. link: This operator searches for pages linking to a specified website

The link: operator identifies external pages that link to a target site, which typically provides contextual or promotional information (e.g., partner pages, news articles) rather than technical VPN details.

upvoted 2 times

 **KnightHeart** 6 months ago

A not the answer.

Relevance to VPNs:

VPN servers often have specific geographic locations, and organizations may host VPN endpoints in strategic regions.

Searching for location:"New York" VPN or location:"corporate name" VPN can reveal VPN infrastructure details (e.g., server locations, regional access points).

Example Use Case:

An attacker could use inurl:openvpn location:"London" to find VPN servers in London running OpenVPN.

upvoted 1 times

 **GibsonD** 8 months, 2 weeks ago

Selected Answer: A

The attacker is using Google hacking techniques and the Google Hacking Database (GHDB) to footprint VPN-related information. Google advanced search operators help attackers extract exposed credentials, configuration files, or sensitive data.

upvoted 2 times

👤 **Dogeo** 9 months, 2 weeks ago

Selected Answer: A

If a VPN is being used then the location would not be accurate even if it did give it to you.
upvoted 2 times

👤 **pindinga1** 9 months, 3 weeks ago

Selected Answer: C

The correct answer is:

C. link: This operator searches websites or pages that contain links to the specified website or page

Explanation:

In the context of a footprinting attack to obtain information about VPNs via advanced Google searches, the link: operator would not be as useful compared to the other operators mentioned. The link: operator is used to search for pages that contain links to a specific URL, which is not related to directly obtaining sensitive or specific information about VPNs. The usefulness of this operator in the context of a search for sensitive information about VPNs is limited.

upvoted 2 times

👤 **MHafizC** 10 months, 2 weeks ago

Selected Answer: A

Key is using VPN.
upvoted 3 times

EXAM 312-50V13 TOPIC 1 QUESTION 206 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 206

Topic #: 1

[All 312-50v13 Questions]

An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure. During the scan, he discovers an active host with multiple open ports running various services. The hacker uses TCP communication flags to establish a connection with the host and starts communicating with it. He sends a SYN packet to a port on the host and receives a SYN/ACK packet back. He then sends an ACK packet for the received SYN/ACK packet, which triggers an open connection. Which of the following actions should the ethical hacker perform next?

- A. Send a PSH packet to inform the receiving application about the buffered data.
- B. Conduct a vulnerability scan on the open port to identify any potential weaknesses. **Most Voted**
- C. Scan another port on the same host using the SYN, ACK, and RST flags.
- D. Send a FIN or RST packet to close the connection.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  **MHafizC** at Jan. 16, 2025, 1:12 p.m.

Comments

 **lopesjaf** 3 months, 4 weeks ago

Selected Answer: B

After establishing a TCP connection, the ethical hacker should interact with the service to identify vulnerabilities rather than immediately closing the connection or moving on to other ports.

upvoted 1 times

 **marcel9999** 8 months, 4 weeks ago

Selected Answer: B

see previous answers

upvoted 4 times

 **Dogeo** 9 months, 2 weeks ago

Selected Answer: B

Since the hacker has successfully established a connection with the target host, the next best step is to conduct a vulnerability scan on the open port to identify weaknesses in the system.

upvoted 4 times

 **MHafizC** 10 months, 2 weeks ago

Selected Answer: B

At this point, vulnerability scan is the one.

upvoted 3 times

EXAM 312-50V13 TOPIC 1 QUESTION 2 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 2

Topic #: 1

[All 312-50v13 Questions]

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 **Most Voted**
- C. CSRF
- D. XSS

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by Booict at Jan. 16, 2025, 2:46 p.m.

Comments

suraj028 2 months ago

Selected Answer: B

Buffer overflow
upvoted 1 times

lopesjaf 4 months ago

Selected Answer: B

Buffer Overflow attack — where data is written beyond the boundaries of a buffer, potentially overwriting memory and leading to system compromise.
upvoted 1 times

Jasper_Ng 7 months ago

Selected Answer: B

In C, an array like char buff[10] has valid indices from 0 to 9 — that's 10 elements. buff[10] is out of bounds — it's the 11th element, which does not exist.
upvoted 2 times

n19htf4ll 7 months, 2 weeks ago

Selected Answer: B

'buff' is a 10 characters long string (from 0 to 9) and the user is trying to write the 11th position, which is over its last position. So the right answer is B. overflow
upvoted 3 times

nicejob 9 months, 3 weeks ago

Selected Answer: B

buffer overflow, it not possible is sqli
upvoted 1 times

Osanyindoro 10 months, 2 weeks ago

Selected Answer: B

The answer is B (buffer overflow)

Reasons:

The buffer buff is defined to hold 10 elements (indices 0 through 9).

Writing to buff[10] attempts to access memory beyond the allocated buffer size.

This can lead to overwriting adjacent memory, potentially corrupting data, crashing the application, or enabling the execution of malicious code.

upvoted 4 times

 **Booict** 10 months, 2 weeks ago

Selected Answer: B

the answer is B and not A. Ignore my previous answer

upvoted 1 times

 **Booict** 10 months, 2 weeks ago

Selected Answer: A

SQL injection attack involves inserting malicious SQL code into a web application's input fields to manipulate the database

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 230 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 230

Topic #: 1

[\[All 312-50v13 Questions\]](#)

Consider a scenario where a Certified Ethical Hacker is attempting to infiltrate a company's network without being detected. The hacker intends to use a stealth scan on a BSD-derived TCP/IP stack, but he suspects that the network security devices may be able to detect SYN packets. Based on this information, which of the following methods should he use to bypass the detection mechanisms and why?

- A. Maimon Scan, because it is very similar to NULL, FIN, and Xmas scans, but the probe used here is FIN/ACK
- B. Xmas Scan, because it can pass through filters undetected, depending on the security mechanisms installed
- C. TCP Connect/Full-Open Scan, because it completes a three-way handshake with the target machine
- D. ACK Flag Probe Scan, because it exploits the vulnerabilities within the BSD-derived TCP/IP stack

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by  [MHafizC](#) at Jan. 16, 2025, 3:54 p.m.

Comments

 [lopesjaf](#) 3 months, 4 weeks ago

Selected Answer: A

The question is about bypassing detection of SYN packets on BSD-derived TCP/IP stacks using stealth scanning.

Maimon Scan is designed specifically for this, using a FIN/ACK probe which is less likely to be detected and effective against BSD TCP/IP stacks.
upvoted 2 times

 [e30b32d](#) 6 months, 1 week ago

Selected Answer: D

The correct is D. Keyword "BSD-derived TCP/IP stack", BSD have a limitation in TCP/IP stack.
upvoted 1 times

 [NikoTomas](#) 8 months, 1 week ago

Selected Answer: B

Correct is B - Xmas

All these three scans - A (Maimon), B (Xmas) and D (ACK scan) - are suitable for stealth scanning avoiding FW and IDS detection as connection is not properly established and logged (many firewalls and IPSes logs only established connections, not failed attempts).

Key to choosing the correct answer is BSD-based TCP/IP stack in the question:

In CEH v11 and v12 EC-Council specifically notes:

"Xmas tree scans can be useful on systems like BSD/UNIX because these platforms follow RFC 793, which defines how to handle packets with unusual flag combinations like FIN, URG, and PSH."

Xmas Scan Behavior:

- Sends TCP packets with FIN, URG, and PSH flags set.
- RFC 793 says:
 - If the port is closed, the host should reply with RST
 - If the port is open or filtered, there should be no response

BSD stacks behave exactly this way, making it possible to infer:

- Closed port → Responds with RST
- Open/Filtered port → No response

upvoted 1 times

marcel9999 8 months, 4 weeks ago

Selected Answer: D

answer B get detected right away, so D is correct
upvoted 1 times

Dogeo 9 months, 1 week ago

Selected Answer: D

The Maimon scan is often used to bypass firewalls by sending FIN/ACK packets, exploiting the way the BSD-derived TCP/IP stack handles these packets
upvoted 2 times

MHafizC 10 months, 2 weeks ago

Selected Answer: D

ACK Flag Probe Scan
upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 3 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 3

Topic #: 1

[All 312-50v13 Questions]

John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization.

Which of the following attack techniques is used by John?

- A. Insider threat
- B. Diversion theft
- C. Spear-phishing sites
- D. Advanced persistent threat Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Osanyindoro](#) at Jan. 18, 2025, 10:17 a.m.

Comments

✉  [lopesjaf](#) 4 months ago

Selected Answer: D

These are key characteristics of an Advanced Persistent Threat (APT) — a stealthy, continuous hacking process typically performed by skilled attackers to gain and maintain access to a network over an extended period.

upvoted 1 times

✉  [Jasper_Ng](#) 7 months ago

Selected Answer: D

Sophisticated tools and methods used. Maintains access over time without detection. Real and targeted — usually against big organizations.

upvoted 1 times

✉  [n19htf4ll](#) 7 months, 2 weeks ago

Selected Answer: D

he is acting as an advanced persistent threat or APT

upvoted 1 times

✉  [Osanyindoro](#) 10 months, 2 weeks ago

Selected Answer: D

Advanced Persistent Threat (APT) refers to an attack where a threat actor gains unauthorised access to a network and remains undetected for an extended period.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 21 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 21

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [SNimlaka](#) at Jan. 25, 2025, 7:08 a.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: D

D. Cloud carrier: Provides connectivity and transport between consumers and providers. 
upvoted 1 times

  [sky9te](#) 9 months, 2 weeks ago

Selected Answer: D

A cloud carrier is an entity that provides the connectivity and transport services needed for accessing cloud services.
upvoted 1 times

  [SNimlaka](#) 10 months, 1 week ago

Selected Answer: D

Cloud Carrier:
A cloud carrier acts as an intermediary that provides connectivity and transport services between CSPs and cloud consumers. The cloud carrier provides access to consumers via a network, telecommunication, or other access devices.

Page 3047

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 84 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 84

Topic #: 1

[All 312-50v13 Questions]

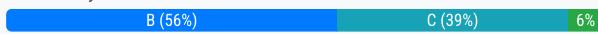
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network. Which of the following host discovery techniques must he use to perform the given task?

- A. UDP scan
- B. ARP ping scan **Most Voted**
- C. ACK flag probe scan
- D. TCP Maimon scan

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by rmycyc at Jan. 29, 2025, 6:32 p.m.

Comments

chakrs 2 months, 1 week ago

Selected Answer: C

ACK scans are designed to map out hosts behind restrictive firewalls by sending TCP packets with the ACK flag set. Firewalls may allow these packets through since they look like part of an established connection, revealing hidden active systems.
upvoted 2 times

Ma06RC 3 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

See page 301 CEHv13

upvoted 1 times

lopesjaf 4 months ago

Selected Answer: B

ARP ping scan is very effective in discovering hosts on a local network, even behind restrictive firewalls because ARP requests are handled at the data link layer and are not typically blocked by firewalls that filter at higher layers.
upvoted 1 times

KnightHeart 6 months ago

Selected Answer: C

Key Context for ACK Flag Probe Scans

Firewall Evasion: ACK probes are useful for bypassing simple firewalls that allow outbound traffic but restrict inbound connections. By sending ACK packets (which resemble response packets), they can elicit responses from hosts behind the firewall.

Host Detection: While not definitive (some firewalls may drop all ACK packets), this method is more likely to succeed than other scans when dealing with restrictive rules.

Stateful Firewalls: If the firewall tracks connection states, an ACK packet for an unsolicited connection may be rejected, but the response (or lack thereof) can still provide clues about host activity.

upvoted 1 times

e30b32d 6 months, 1 week ago

Selected Answer: B

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 1 times

👤 **NikoTomas** 8 months, 2 weeks ago

Selected Answer: A

Correct: A (UDP scan)

Question: Discovering devices hidden by RESTRICTIVE FW - for me it means you are NOT inside the network but behind the FW. So you can't use ARP resolution, which is L2 protocol working only inside the LAN.

As FW is restrictive (supposedly stateful), it will for sure block incomplete TCP sessions - i. e. ACK flag scan will be blocked by FW (no session exists on FW).

TCP Maimon scan will be blocked by FW as well - like ACK scan, Maimon is also based on incomplete TCP session with FIN/ACK flags set (no session exists on FW).

UDP scan:

- Many FWs struggle to track UDP sessions (UDP is stateless, no handshake like TCP).
- Some FWs mistakenly assume that UDP is harmless and allow it without strict filtering.
- UDP scanning can identify misconfigured firewall rules, revealing hidden services.
- Many FWs focus on filtering TCP traffic because most applications use TCP.
- UDP is often less restricted as it is required for essential services like DNS (53), SNMP (161) and DHCP (67/68).
- UDP scanning can identify open services that a FW does not properly restrict.

upvoted 1 times

👤 **killwitch** 8 months, 3 weeks ago

Selected Answer: B

B. ARP ping scan.

ARP (Address Resolution Protocol) ping scan works at the link layer (Layer 2) and does not rely on IP-based scanning techniques like TCP or UDP. Since firewalls typically block ICMP pings and other IP-based scans, an ARP scan bypasses these restrictions by directly querying MAC addresses in the local network.

This method is highly effective in discovering all active hosts on a LAN because all devices must respond to ARP requests.

upvoted 1 times

👤 **getaseadsss** 9 months ago

Selected Answer: C

ACK scan

upvoted 2 times

👤 **Dogeo** 9 months, 4 weeks ago

Selected Answer: C

An ACK flag probe scan is used to discover active hosts behind a restrictive firewall by sending TCP packets with the ACK flag set.

upvoted 2 times

👤 **pindinga1** 10 months ago

Selected Answer: B

This correct answer is ARP ping scan

upvoted 3 times

👤 **rmycyc** 10 months ago

Selected Answer: B

How it works: Sends ARP (Address Resolution Protocol) requests to discover devices on the same local network segment.

Use case: Highly effective for host discovery within the same subnet because ARP is a layer 2 protocol and is rarely blocked by firewalls.

Suitability: This is the best choice for discovering active devices hidden by a restrictive firewall, especially if the target network is within the same subnet.

upvoted 3 times

EXAM 312-50V13 TOPIC 1 QUESTION 120 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 120

Topic #: 1

[\[All 312-50v13 Questions\]](#)

Which of the following protocols can be used to secure an LDAP service against anonymous queries?

A. NTLM Most Voted

B. RADIUS

C. WPA

D. SSO

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (75%)

B (25%)

by  pindinga1 at Jan. 30, 2025, 8:45 p.m.

Comments

  lopesjaf 4 months ago

Selected Answer: B

RADIUS (Remote Authentication Dial-In User Service) is a protocol used for centralized authentication, authorization, and accounting, and it can be used to authenticate users accessing the LDAP service, thereby preventing anonymous queries.

upvoted 1 times

  91a0021 9 months ago

Selected Answer: A

NTLM (NT LAN Manager) is an authentication protocol that can be used to secure LDAP services by enforcing authentication requirements and preventing anonymous queries.

LDAP over NTLM ensures that only authenticated users can access directory services.

It prevents unauthenticated or anonymous users from querying sensitive directory information.

NTLM is commonly used in Windows Active Directory environments to secure LDAP authentication.

upvoted 1 times

  Dogeo 9 months, 3 weeks ago

Selected Answer: A

NTLM (NT LAN Manager) is a authentication protocol that can be used in conjunction with LDAP (Lightweight Directory Access Protocol) to secure the service by preventing anonymous queries.

upvoted 1 times

  pindinga1 10 months ago

Selected Answer: A

A.NTLM.

NTLM (NT LAN Manager) is an authentication protocol used in Windows networks. Although not specifically designed to secure a Lightweight Directory Access Protocol (LDAP) service, NTLM can be used to authenticate and authorize users attempting to access an LDAP server. By enabling NTLM or Kerberos authentication on the LDAP server, anonymous queries can be prevented, as users must authenticate before accessing directory information.

upvoted 1 times

 EXAM 312-50 TOPIC 8 QUESTION 295 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 295

Topic #: 8

[All 312-50 Questions]

Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

s-1-5-21-1125394485-807628933-54978560-100Johns
s-1-5-21-1125394485-807628933-54978560-652Rebecca
s-1-5-21-1125394485-807628933-54978560-412Sheela
s-1-5-21-1125394485-807628933-54978560-999Shawn
s-1-5-21-1125394485-807628933-54978560-777Somia
s-1-5-21-1125394485-807628933-54978560-500chang
s-1-5-21-1125394485-807628933-54978560-555Micah

From the above list identify the user account with System Administrator privileges.

- A. John
- B. Rebecca
- C. Sheela
- D. Shawn
- E. Somia
- F. Chang **Most Voted**
- G. Micah F

[Hide Answer](#)

Suggested Answer: Explanation

Community vote distribution

F (67%) A (33%)

by  [styx](#) at March 5, 2020, 3:41 p.m.

Comments

 [styx](#) **Highly Voted** 5 years, 2 months ago

The SID for the Administrator account in Windows always ends in 500
upvoted 5 times

 [igodomigododevcenter](#) **Most Recent** 1 year ago

Selected Answer: F
my first submission was made in error. google said windows server 2000 sid for root is 500
upvoted 1 times

 [igodomigododevcenter](#) 1 year ago

Selected Answer: A
according to google, windows 2000 sid for administrator is 500
upvoted 1 times

 [Water07](#) 2 years, 3 months ago

Selected Answer: F
i follow
upvoted 1 times

 [Joker20](#) 4 years ago

Correct answer :
Chang
upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 195 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 195

Topic #: 1

[All 312-50v13 Questions]

A Certified Ethical Hacker (CEH) is analyzing a target network. To do this, he decides to utilize an IDLE/IPID header scan using Nmap. The network analysis reveals that the IPID number increases by 2 after following the steps of an IDLE scan. Based on this information, what can the CEH conclude about the target network?

- A. The ports on the target network are open **Most Voted**
- B. The target network has no firewall present
- C. The ports on the target network are closed
- D. The target network has a stateful firewall present

[Hide Answer](#)

Suggested Answer: A

Community vote distribution



by nicejob at Feb. 5, 2025, 7 a.m.

Comments

✉ lopesjaf 3 months, 4 weeks ago

Selected Answer: C

IPID increment by 2 → Target sent RST → Port closed

IPID increment by 1 → Target responded with SYN/ACK → Port open
upvoted 1 times

✉ killwitch 8 months, 3 weeks ago

Selected Answer: A

An IDLE/IPID header scan is a stealthy port scanning technique that exploits predictable IP identification (IPID) values from a zombie host to infer open ports on a target system without directly interacting with the target.

How an IDLE Scan Works:

The attacker finds a zombie host (a machine with predictable IPID values).

The attacker sends a SYN packet to the target spoofed as coming from the zombie.

The target responds:

If the port is open, the target replies to the zombie with a SYN/ACK. Since the zombie was unaware of the connection, it sends an RST response, increasing its IPID value by 2.

If the port is closed, the target replies with an RST, which does not cause the zombie's IPID value to increment by 2.

Since the IPID increased by 2, this means the target responded with a SYN/ACK, causing the zombie to send an RST—indicating that the port is open.

upvoted 1 times

✉ ehsarx 8 months, 3 weeks ago

Selected Answer: A

an IPID increase of two indicates that a zombie host sent a packet between two probes. This usually means that the port is open.

upvoted 1 times

✉ Dogeo 9 months, 2 weeks ago

Selected Answer: D

The IDLE scan in Nmap reveals that the IPID number increases by 2, which indicates that the target network is likely protected by a stateful firewall. This type of firewall tracks connection states and influences how the IPID field is modified, providing clues about the network's configuration.

upvoted 1 times

✉ nicejob 9 months, 3 weeks ago

Selected Answer: A

IPID+2 mean target port is opened
upvoted 3 times

 EXAM 312-50V13 TOPIC 1 QUESTION 160 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 160

Topic #: 1

[All 312-50v13 Questions]

You are a cybersecurity professional managing cryptographic systems for a global corporation. The company uses a mix of Elliptic Curve Cryptography (ECC) for key exchange and symmetric encryption algorithms for data encryption. The time complexity of ECC key pair generation is $O(n^3)$, where 'n' is the size of the key. An advanced threat actor group has a quantum computer that can potentially break ECC with a time complexity of $O((\log n)^2)$. Given that the ECC key size is 'n=512' and varying symmetric encryption algorithms and key sizes, which scenario would provide the best balance of security and performance?

- A. Data encryption with AES-128: Provides moderate security and fast encryption, offering a balance between the two.
- B. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes. Most Voted
- C. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to 3DES's inherent inefficiencies.
- D. Data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (80%) A (20%)

by  [Doge0](#) at Feb. 13, 2025, 12:28 p.m.

Comments

 [lopesjaf](#) 4 months ago

Selected Answer: B

AES-256 is the most secure and performant symmetric encryption option under a quantum-capable threat scenario, especially when ECC is known to be vulnerable.

upvoted 1 times

 [killwitch](#) 8 months, 2 weeks ago

Selected Answer: B

Since quantum computers can break ECC much more efficiently due to its $O((\log n)^2)$ time complexity, the focus should be on strong symmetric encryption that is resistant to quantum attacks.

AES-256 is widely recommended for post-quantum security because:

- It offers high security against both classical and quantum attacks.
- Grover's algorithm reduces the effective key space of AES-256 to AES-128 security levels, but that is still secure.
- AES-256 is much faster than 3DES and Blowfish while maintaining strong security.

upvoted 1 times

 [Gibson0d](#) 8 months, 2 weeks ago

Selected Answer: B

AES (Advanced Encryption Standard), is not directly broken by quantum computing in the same way as ECC. Instead, Grover's algorithm can reduce brute-force attacks on AES from $O(2^k)$ to $O(2^{k/2})$, meaning AES-256 has an effective strength of 128-bit security against quantum attacks.

upvoted 2 times

 [Doge0](#) 9 months, 2 weeks ago

Selected Answer: A

AES-128 is the best for balance between security and performance.

upvoted 1 times

 EXAM 312-50V13 TOPIC 1 QUESTION 201 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 201

Topic #: 1

[All 312-50v13 Questions]

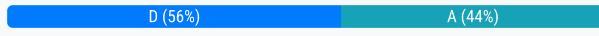
A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

- A. Inference-based assessment solution
- B. Tree-based assessment approach
- C. Product-based solution installed on a private network
- D. Service-based solution offered by an auditing firm **Most Voted**

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by Dogeo at Feb. 16, 2025, 11:16 p.m.

Comments

lopesjaf 3 months, 4 weeks ago

Selected Answer: A

Inference-based assessment solutions simulate attackers' reasoning by correlating multiple pieces of information and vulnerabilities to identify real security risks and attack paths.

They offer a more attacker-like perspective and provide well-organized, inference-driven testing.

They typically have automatic scanning with continuously updated vulnerability databases.

Such solutions are capable of handling multiple networks and environments.

upvoted 2 times

Cherubael 6 months, 2 weeks ago

Selected Answer: A

This is just wrong, a service based solution by an auditing firm will not work on a periodic basis. An inference based assessment mimics an attacker's perspective, offering an external view of the organization's security posture.

upvoted 2 times

marcel9999 8 months, 4 weeks ago

Selected Answer: D

Service-based solutions are offered by third parties, such as auditing or security consulting firms. Some solutions are hosted inside the network, while others are hosted outside the network. A drawback of this solution is that attackers can perform network vulnerability scans from the Internet/external network.

upvoted 2 times

Dogeo 9 months, 2 weeks ago

Selected Answer: D

a service-based vulnerability assessment from an auditing firm is the best choice for a comprehensive, continuously updated, and external-focused security assessment.

upvoted 3 times

EXAM 312-50V13 TOPIC 1 QUESTION 208 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 208

Topic #: 1

[All 312-50v13 Questions]

As a certified ethical hacker, you are performing a system hacking process for a company that is suspicious about its security system. You found that the company's passwords are all known words, but not in the dictionary. You know that one employee always changes the password by just adding some numbers to the old password. Which attack is most likely to succeed in this scenario?

- A. Brute-Force Attack
- B. Password Spraying Attack
- C. Hybrid Attack **Most Voted**
- D. Rule-based Attack

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by Dogeo at Feb. 16, 2025, 11:27 p.m.

Comments

✉ Ma06RC 2 months, 3 weeks ago

Selected Answer: C

See page 642 of CEHv13

upvoted 1 times

✉ lopesjaf 3 months, 4 weeks ago

Selected Answer: C

Since the passwords are words (not in the dictionary) + added numbers, a Hybrid Attack that starts with known words and adds numbers would be effective.

Rule-based Attack is also viable because it applies rules like "append numbers," but hybrid attacks are generally described as combining dictionary words with common mutations, which fits better here.

upvoted 1 times

✉ KnightHeart 6 months, 1 week ago

Selected Answer: D

" passwords are all known words, but not in the dictionary.' mean it is not hybrid attack.

D seem more perfer.

upvoted 2 times

✉ hiddenmessages 7 months, 2 weeks ago

Selected Answer: D

This is taught in OSCP and CPTS training. This is rule-based attacking. You apply a rule like if the old password for the targeted user is "NewPassword123!" The rule would be NewPassword[RULE]. Trick question, since this is a hacking exam, it's rule based

upvoted 1 times

✉ ehsarx 8 months, 3 weeks ago

Selected Answer: D

Rule based attack is sophisticated by the use of patterns to guess the password.

Hybrid works by combining dictionary attack and some pattern. Yet the words are not dictionary based.

I think D is correct

upvoted 1 times

✉ marcel9999 8 months, 4 weeks ago

Selected Answer: C

This type of attack depends on the dictionary attack. Often, people change their passwords merely by adding some numbers to their old passwords.

upvoted 3 times

 **Doge0** 9 months, 2 weeks ago

Selected Answer: C

Since the passwords are based on common words with slight modifications (like numbers added at the end), the Hybrid Attack is the best choice to efficiently crack them.

upvoted 3 times

EXAM 312-50V12 TOPIC 1 QUESTION 312 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 312

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Ethical hacker Jane Doe is attempting to crack the password of the head of the IT department of ABC company. She is utilizing a rainbow table and notices upon entering a password that extra characters are added to the password after submitting.

What countermeasure is the company using to protect against rainbow tables?

- A. Password key hashing
- B. Password salting**
- C. Account lockout
- D. Password hashing

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

 B (100%)

by  [Lennin](#) at Feb. 21, 2025, 9:07 a.m.

Comments

  [Lennin](#) 9 months, 1 week ago

Selected Answer: B

The correct answer is B. Password salting.

Salting involves adding random data (the "salt") to a password before it is hashed. This makes each password hash unique, even if two users have the same password. By adding extra characters or salt to the password before it is hashed, it becomes much more difficult for attackers to use rainbow tables, which rely on precomputed hash values.

- A. Password key hashing refers to hashing passwords, but it doesn't provide protection against rainbow tables unless combined with salting.
- C. Account lockout is a security measure to block access after a number of failed login attempts, not specifically related to rainbow tables.
- D. Password hashing alone, without salting, can still be vulnerable to rainbow tables.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 222 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 222

Topic #: 1

[All 312-50v13 Questions]

Being a Certified Ethical Hacker (CEH), a company has brought you on board to evaluate the safety measures in place for their network system. The company uses a network time protocol server in the demilitarized zone. During your enumeration, you decide to run a ntptrace command. Given the syntax: ntptrace [-n] [-m maxhosts] [servername/IP_address], which command usage would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network?

- A. ntptrace -n -m 5192.168.1.1
- B. ntptrace -m 5192.168.1.1
- C. ntptrace -n localhost
- D. ntptrace 192.168.1.1 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by Dogeo at Feb. 24, 2025, 2:38 p.m.

Comments

lopesjaf 3 months, 4 weeks ago

Selected Answer: D

The ntptrace command is used to trace the chain of NTP (Network Time Protocol) servers back to the primary time source. It tells you where an NTP server is getting its time from, and follows upstream peers recursively.

upvoted 1 times

KnightHeart 5 months, 4 weeks ago

Selected Answer: A

"Given the syntax: ntptrace [-n] [-m maxhosts] [servername/IP_address]" Only A meet the requirement.

Uses -n to avoid unnecessary DNS lookups, ensuring direct targeting.

Sets -m 5 to balance between thoroughness and efficiency in tracing the NTP hierarchy.

Targets the specified NTP server IP in the DMZ, aligning with the objective of enumerating where the server gets its time and the connected NTP servers.

upvoted 1 times

marcel9999 8 months, 4 weeks ago

Selected Answer: D

is only correct answer

upvoted 3 times

Dogeo 9 months, 1 week ago

Selected Answer: D

A and B are incorrect syntax and C only refers to local machine so D is the correct answer.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 135 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 135

Topic #: 1

[All 312-50v13 Questions]

As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data. However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

- A. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure.
- B. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay.
- C. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries. **Most Voted**
- D. The hacker alters his approach and injects a 'DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  91a0021 at Feb. 28, 2025, 6:53 a.m.

Comments

 lopesjaf 4 months ago

Selected Answer: C

C. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries.

Encoding techniques (URL encoding, Unicode encoding, double encoding) are often used to evade filtering.
upvoted 2 times

 NikoTomas 8 months, 2 weeks ago

Selected Answer: C

For sure C.
As stated in the question, the input sanitization is in place, so the attacker must overcome it somehow - C) Using encoding to avoid blocking of unallowed special characters and/or keywords.
upvoted 2 times

 Gibbsmd 8 months, 2 weeks ago

Selected Answer: C

Your application already filters special characters in user inputs, which is an effective measure against traditional SQL Injection attacks.
upvoted 1 times

 91a0021 9 months ago

Selected Answer: C

The key details in the question indicate:

The attacker is using UNION-based SQL Injection.

This means the goal is to extract data directly rather than relying on indirect inference techniques like time-based delays.

The application filters special characters.

The hacker's immediate problem is bypassing the input sanitization, not dealing with a lack of visible output

upvoted 4 times

EXAM 312-50 TOPIC 8 QUESTION 312 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 312

Topic #: 8

[\[All 312-50 Questions\]](#)

Which DNS resource record can indicate how long any "DNS poisoning" could last?

- A. MX
- B. SOA**
- C. NS
- D. TIMEOUT

[Hide Answer](#)

Suggested Answer: B

by  **phmb14** at March 10, 2020, 2:25 a.m.

Comments

 **phmb14** 1 year, 2 months ago

The SOA contains information of secondary servers, update intervals and expiration times.

upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 348 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 348

Topic #: 8

[\[All 312-50 Questions\]](#)

Password cracking programs reverse the hashing process to recover passwords. (True/False.)

A. True

B. False

[Hide Answer](#)

Suggested Answer: B

by  **phmb14** at March 11, 2020, 1:51 a.m.

Comments

  **Grezavi** 1 year, 4 months ago

False, password hashes cannot be reversed
upvoted 1 times

  **phmb14** 2 years, 8 months ago

cannot reverse hashes.
upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 7 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 7

Topic #: 1

[All 312-50v13 Questions]

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. Pluto

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by [NikoTomas](#) at March 9, 2025, 8:36 p.m.

Comments

✉ [supunabeysinghe](#) 1 month, 3 weeks ago

Selected Answer: C

Ans: C) zANTI

zANTI is a mobile (Android) network penetration-testing toolkit that can perform DNS/host discovery, DNS lookups/spoofing, network mapping and WHOIS queries — exactly the kind of automated DNS footprinting described.

A) Towelroot — an Android rooting exploit/tool (created by geohot). It's used to root Android devices, not for DNS/zone enumeration or network footprinting.

B) Knative — an open-source Kubernetes-based platform for building serverless apps (event-driven compute). Not a network reconnaissance tool.

D) Pluto — not a widely-known DNS/footprinting product/tool in the penetration-testing community (and not a match for automated DNS zone enumeration).

upvoted 1 times

✉ [lopesjaf](#) 4 months ago

Selected Answer: D

These are typical features of Pluto, a DNS information gathering tool used for DNS enumeration, zone transfer testing, and Whois lookups — commonly used in reconnaissance stages.

upvoted 2 times

✉ [NikoTomas](#) 8 months, 3 weeks ago

Selected Answer: D

Correct: D

A. Towelroot = tool for rooting Android

B. Knative = enables serverless workloads to run on Kubernetes clusters. It makes building and orchestrating containers with Kubernetes faster and easier. Knative (pronounced Kay-NAY-tive) is an extension of the Kubernetes container orchestration platform.

C. zANTI = With zANTI 3.0 you can simulate real-world, commonly-used mobile malicious cyber attack techniques

D. Pluto = Pluto is a Python-based tool for DNS recon, DNS zone transfer testing, DNS wild card checks, DNS brute forcing, e-mail enumeration and more.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 9 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 9

Topic #: 1

[\[All 312-50v13 Questions\]](#)

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

- A. [inurl:]
- B. [info:]
- C. [site:]
- D. [related:] Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [NikoTomas](#) at March 9, 2025, 8:42 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: D

D. related: — Finds websites related to the specified URL (similar sites).
upvoted 1 times

  [d503c75](#) 6 months, 2 weeks ago

Selected Answer: D

The "related:" operator is no longer supported, but this google search operator was previously used to find websites that Google considered similar or related to a specified website.
upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 11 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 11

Topic #: 1

[All 312-50v13 Questions]

While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

A. -sA **Most Voted**

B. -sX

C. -sT

D. -sF

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [NikoTomas](#) at March 9, 2025, 9:05 p.m.

Comments

✉  [lopesjaf](#) 4 months ago

Selected Answer: A

-sA (ACK scan):

Sends ACK packets to see if the firewall tracks connection states.

A stateful firewall will drop unsolicited ACK packets (no connection state), so ports appear filtered.

A stateless firewall (or no firewall) may respond differently.

This is commonly used to detect firewall behavior.

upvoted 2 times

✉  [e30b32d](#) 6 months, 1 week ago

Selected Answer: A

-sA (ACK scan) is specifically designed to determine firewall rules and to detect whether a firewall is stateful or stateless.

upvoted 1 times

✉  [NikoTomas](#) 8 months, 3 weeks ago

Selected Answer: A

Correct: A = TCP ACK Scan (-sA)

Special scan - never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

<https://nmap.org/book/scan-methods-ack-scan.html>

TCP Connect Scan (-sT)

By default used when default SYN scan (-sS) is not an option due to missing raw packet privileges or scanning IPv6 networks. Instead of writing raw packets, Nmap asks the underlying OS to establish a connection by "connect" system call.

<https://nmap.org/book/scan-methods-connect-scan.html>

TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX):

Null scan (-sN) - Does not set any bits (TCP flag header is 0)

FIN scan (-sF) - Sets just the TCP FIN bit.

Xmas scan (-sX) - Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

- scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open.

<https://nmap.org/book/scan-methods-null-fin-xmas-scan.html>

upvoted 2 times

✉  **NikoTomas** 8 months, 3 weeks ago

Additional info:

TCP SYN (Stealth) Scan (-sS)

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 27 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 27

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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 Most Voted

B. JSON-RPC

C. SOAP API

D. REST API

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [NikoTomas](#) at March 9, 2025, 10:22 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: A

A. RESTful API: Correct term for APIs following REST principles. 

upvoted 1 times

  [e30b32d](#) 6 months, 1 week ago

Selected Answer: A

RESTful API (Representational State Transfer API) is a widely used architectural style for building web services that utilize HTTP methods like GET, POST, PUT, and DELETE.

upvoted 2 times

  [NikoTomas](#) 8 months, 3 weeks ago

Selected Answer: A

Correct: A (RESTful API):

REST is a style of software architecture for distributed software
Conforming to the REST constraints is referred to as being 'RESTful'.

RESTful is typically used to refer to web services implementing such an architecture.
RESTful is just used as an adjective describing something that respects the REST constraints.

<https://stackoverflow.com/questions/1568834/whats-the-difference-between-rest-restful>

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 50 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 50

Topic #: 1

[All 312-50v13 Questions]

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [NikoTomas](#) at March 10, 2025, 10:25 p.m.

Comments

 [lopesjaf](#) 4 months ago

Selected Answer: D

me.

The malware often displays aggressive ads, collects data, or performs malicious activities without the user's knowledge.

This malware was famously named "Agent Smith" (after the character in The Matrix) due to its ability to silently take over legitimate apps while keeping their appearance unchanged.

upvoted 1 times

 [NikoTomas](#) 8 months, 3 weeks ago

Selected Answer: D

Correct: D - Agent Smith attack

Agent Smith is mobile malware that generates financial gain by replacing legitimate applications on devices with malicious versions that include fraudulent ads. As of July 2019 Agent Smith had infected around 25 million devices, primarily targeting India though effects had been observed in other Asian countries as well as Saudi Arabia, the United Kingdom, and the United States

<https://attack.mitre.org/software/S0440/>

upvoted 3 times

 EXAM 312-50V13 TOPIC 1 QUESTION 58 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 58

Topic #: 1

[All 312-50v13 Questions]

Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources.

What is the attack technique used by Jude for finding loopholes in the above scenario?

A. Spoofed session flood attack **Most Voted**

- B. UDP flood attack
- C. Peer-to-peer attack
- D. Ping-of-death attack

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [NikoTomas](#) at March 10, 2025, 11:24 p.m.

Comments

 [lopesjaf](#) 4 months ago

Selected Answer: A

Jude is creating forged TCP sessions by sending SYN, ACK, RST, or FIN packets — this is typical of TCP spoofing and session flooding.

The goal is to exhaust network resources and bypass protections like firewalls.

This technique often results in DDoS attacks aimed at overwhelming the target's TCP/IP stack or network capacity.

upvoted 1 times

 [e30b32d](#) 6 months, 1 week ago

Selected Answer: A

Spoofed Session Flood Attack

Attackers create fake or spoofed TCP sessions by carrying multiple SYN, ACK, and RST or FIN packets. Bypass firewalls and perform DDoS attacks against the target network, exhausting its network resources. (P.1319/1303)

upvoted 1 times

 [NikoTomas](#) 8 months, 3 weeks ago

Selected Answer: A

Correct: A

A spoofed session flood is a form of DDoS (Distributed Denial of Service) attack where an attacker overwhelms a system by creating fake sessions that mimic legitimate user interactions. By manipulating session data to look like valid communication, the attacker floods the system with these fake requests, consuming resources and potentially causing the application to become unresponsive or leading to unauthorized access.

This type of attack exploits weaknesses in session management and network traffic monitoring, making it difficult to detect and mitigate.

Attackers can submit a fake SYN packet (used to initiate a TCP connection), followed by multiple ACK packets (which acknowledge the receipt of data), and at least one RST (reset) or FIN (connection termination) packet. By crafting these packets, they mimic a genuine TCP session, tricking security systems into believing the communication is legitimate.

<https://www.indusface.com/learning/spoofed-session-flood-attack/>

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 73 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 73

Topic #: 1

[All 312-50v13 Questions]

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [NikoTomas](#) at March 12, 2025, 9:50 p.m.

Comments

 [lopesjaf](#) 4 months ago

Selected Answer: D

Infoga is an email reconnaissance tool specifically designed to:

Gather email-related information from public sources

upvoted 1 times

 [KnightHeart](#) 5 months, 3 weeks ago

Selected Answer: D

D. Infoga

Infoga is specifically designed for email reconnaissance, integrating data from public sources and haveibeenpwned to gather the exact information Wilson uses in the scenario.

upvoted 1 times

 [e30b32d](#) 6 months, 1 week ago

Selected Answer: D

Infoga is an information gathering tool specifically designed for collecting email-related data. It can:

upvoted 1 times

 [NikoTomas](#) 8 months, 3 weeks ago

Selected Answer: D

Answer: D

Infoga - Email Information Gathering

Infoga is a tool for gathering e-mail accounts information from different public sources (search engines, pgp key servers). Is a really simple tool, but very effective for the early stages of a penetration test or just to know the visibility of your company in the Internet.

upvoted 2 times

EXAM 312-50V12 TOPIC 1 QUESTION 313 DISCUSSION

Actual exam question from ECCouncil's 312-50v12

Question #: 313

Topic #: 1

[\[All 312-50v12 Questions\]](#)

Which type of virus can change its own code and then cipher itself multiple times as it replicates?

- A. Tunneling virus
- B. Cavity virus
- C. Encryption virus Most Voted
- D. Stealth virus

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [agelbahri](#) at March 13, 2025, 11:01 p.m.

Comments

 [e020fdc](#) 6 months, 1 week ago

Selected Answer: C

A. Tunneling virus

Attempts to intercept or bypass antivirus detection by operating below security software (e.g., by hooking into low-level OS functions).

B. Cavity virus

Hides itself by overwriting unused space within legitimate files.

C. Encryption virus

Type of self-replicating malware that encrypts its own code to avoid detection. Each time it replicates, it may use a different encryption key, making every copy look different — a technique that helps it evade signature-based antivirus detection.

D. Stealth virus

Hides its presence by intercepting system requests and returning false information. While stealthy, it doesn't necessarily encrypt or mutate its code like an encryption virus does.

upvoted 1 times

 EXAM 312-50V13 TOPIC 1 QUESTION 129 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 129

Topic #: 1

[All 312-50v13 Questions]

A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?

A. Test 3: The test was executed to observe the response of the target system when a packet with URC, PSH, SYN, and FIN flags was sent, thereby identifying the OS

B. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target

C. Test 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint **Most Voted**

D. Test 6: The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [NikoTomas](#) at March 14, 2025, 10:23 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: C

This question refers to advanced TCP/IP stack fingerprinting, particularly as used by tools like Nmap in its OS detection process.
upvoted 1 times

  [NikoTomas](#) 8 months, 2 weeks ago

Selected Answer: C

Correct: C

TCP ECN Scan (-sN):

- ◆ The Explicit Congestion Notification (ECN) scan is a special type of TCP scan that checks for firewall and OS fingerprinting behavior.
- ◆ It sends a SYN packet with the ECN-Echo (ECE) and CWR flags set to probe how a target responds.
- ◆ If the target replies with SYN + ECN-Echo (ECE) flags set, it indicates that the host supports ECN.

Example:

```
nmap -sN -p 80 <target-ip>
```

- ✓ Sends SYN + ECN-Echo (ECE) + CWR flags
- ✓ Checks for ECN support in TCP handshake

Useful for:

- ✓ Firewall Detection: Some firewalls block ECN-enabled connections.
- ✓ OS Fingerprinting: Identifies operating systems that support ECN (e.g., modern Linux, Windows, BSD).
- ✓ Stealthy Reconnaissance: Some IDS/IPS systems don't log ECN scans as aggressive behavior.

upvoted 2 times

EXAM 312-50 TOPIC 3 QUESTION 49 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 49

Topic #: 3

[\[All 312-50 Questions\]](#)

Which type of scan measures a person's external features through a digital video camera?

- A. Iris scan
- B. Retinal scan
- C. Facial recognition scan Most Voted
- D. Signature kinetics scan C

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (100%)

by  [devilman](#) at March 18, 2020, 8:23 a.m.

Comments

  [igodomigododevcenter](#) 1 year ago

Selected Answer: C

C makes more sense
upvoted 1 times

  [raousman](#) 1 year, 4 months ago

Selected Answer: C

Answer is C
upvoted 1 times

  [jaimeigs](#) 2 years, 10 months ago

Selected Answer: C

The correct answer is C
upvoted 1 times

  [isaackitonyi](#) 3 years, 4 months ago

The correct answer is C
upvoted 4 times

  [Halibay](#) 4 years, 7 months ago

Video - Facial recognition
upvoted 2 times

  [Mangalam](#) 4 years, 11 months ago

Answer is C
upvoted 2 times

  [devilman](#) 5 years, 2 months ago

the correct answer is C
upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 140 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 140

Topic #: 1

[\[All 312-50v13 Questions\]](#)

XYZ company recently discovered a potential vulnerability on their network, originating from misconfigurations. It was found that some of their host servers had enabled debugging functions and unknown users were granted administrative permissions. As a Certified Ethical Hacker, what would be the most potent risk associated with this misconfiguration?

- A. An attacker may be able to inject a malicious DLL into the current running process
- B. Weak encryption might be allowing man-in-the-middle attacks, leading to data tampering
- C. Unauthorized users may perform privilege escalation using unnecessarily created accounts Most Voted
- D. An attacker may carry out a Denial-of-Service assault draining the resources of the server in the process

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by  [GibsonD](#) at March 15, 2025, 9:40 p.m.

Comments

 [lopesjaf](#) 4 months ago

Selected Answer: C

Misconfigurations that allow unknown users administrative access most critically enable privilege escalation and unauthorized control over systems, making option C the primary risk.

upvoted 1 times

 [killwitch](#) 8 months, 2 weeks ago

Selected Answer: C

The primary risk associated with misconfigurations—such as enabling debugging functions and granting administrative permissions to unknown users—is that unauthorized users could escalate their privileges.

upvoted 1 times

 [NikoTomas](#) 8 months, 2 weeks ago

Selected Answer: A

For me, correct is A:

Question states: "host servers had enabled debugging functions and unknown users were granted administrative permissions" – this already happened and they are asking what can be next.

--> Debugging & Admin privileges together implies that you can perform DLL injection into any process. Debugging function is a standard way how to do it but you need also administrative rights.

Incorrect:

B) – weak encryption has nothing to do with this...

C) – privilege escalation using unnecessarily created accounts – question states that the users were granted admin permissions already so they don't have to escalate anything.

D) – DoS attack by exhausting resources... you can do it even without admin privileges and debugging if you have any access.

upvoted 1 times

 **Gibson0d** 8 months, 2 weeks ago

Selected Answer: C

Misconfigurations, such as debugging functions enabled and unknown users having administrative privileges, present a high risk of privilege escalation. Attackers with unauthorized admin-level access can exploit these misconfigurations to elevate their privileges and gain full control over affected systems.

upvoted 2 times

 EXAM 312-50V13 TOPIC 1 QUESTION 142 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 142

Topic #: 1

[All 312-50v13 Questions]

An ethical hacker is attempting to crack NTLM hashed passwords from a Windows SAM file using a rainbow table attack. He has dumped the on-disk contents of the SAM file successfully and noticed that all LM hashes are blank. Given this scenario, which of the following would be the most likely reason for the blank LM hashes?

- A. The SAM file has been encrypted using the SYSKEY function.
- B. The passwords exceeded 14 characters in length and therefore, the LM hashes were set to a "dummy" value.
- C. The Windows system is Vista or a later version, where LM hashes are disabled by default. Most Voted
- D. The Windows system is using the Kerberos authentication protocol as the default method.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [Gibsonmd](#) at March 16, 2025, midnight

Comments

 [lopesjaf](#) 4 months ago

Selected Answer: C

Starting with Windows Vista and later versions, Microsoft disabled the creation and storage of LM (LAN Manager) hashes by default due to their inherent insecurity.

upvoted 1 times

 [e30b32d](#) 6 months, 1 week ago

Selected Answer: C

C - correct answer

upvoted 1 times

 [NikoTomas](#) 8 months, 2 weeks ago

Selected Answer: C

Correct: C

- o Since Windows Vista/Server 2008, insecure LM hashes are not stored – this means that there is BLANK password – i. e. NULL character.
- o LM password is always padded up to 14 characters by appending NULL characters.
- o This means that in this case, NULL password is padded with another 13 NULL characters up to 14 NULL characters.
- o LM hash is computed so that the 14 characters are split into two 7-character chunks and each is hashed individually before sticking them back together to form final LM hash.
- o LM-hashed 7-character NULL string = AAD3B435B51404EE – concatenate two of these and you get AAD3B435B51404EEAAD3B435B51404EE (two same hashes AAD3B435B51404EE connected together) = LM hash of EMPTY (BLANK) PASSWORD – this is always the same as LM hashing doesn't use salt.
- o Also if password exceeds 14 characters, LM hash is not stored (you will see again BLANK password hash in the SAM database – as shown above), so option B could be also correct, but BLANK password is NOT considered "dummy value" as B suggests, so correct is C.

upvoted 1 times

 [Gibsonmd](#) 8 months, 2 weeks ago

Selected Answer: C

LAN Manager (LM) hashes are considered weak and highly vulnerable to attacks (such as rainbow table attacks). Starting with Windows Vista and later versions, LM hash storage was disabled by default due to security concerns.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 143 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 143

Topic #: 1

[\[All 312-50v13 Questions\]](#)

A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

- A. The system failed to establish a connection due to an incorrect port number.
- B. The enumeration process was blocked by the target system's intrusion detection system.
- C. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation. Most Voted**
- D. The Python version installed on the CEH's machine is incompatible with the ldap3 library.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [Gibsonmd](#) at March 16, 2025, 12:02 a.m.

Comments

✉  [lopesjaf](#) 4 months ago

Selected Answer: C

In Python LDAP libraries (like ldap3), specifying use_ssl=True when creating the server object is mandatory to enable a secure connection.
upvoted 1 times

✉  [NikoTomas](#) 8 months, 2 weeks ago

Selected Answer: C

Answer: C

Q: "After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain..."

C) - You can use SSL basic authentication with the use_ssl parameter of the Server object, you can also specify a port (636 is the default for secure ldap):
s = Server('servername', port = 636, use_ssl = True) # define a secure LDAP server

Ref.: <https://ldap3.readthedocs.io/en/latest/ssltls.html>

upvoted 1 times

✉  [NikoTomas](#) 8 months, 2 weeks ago

Incorrect answers:

- A) – incorrect port number – connection would not be established at all.

- B) – blocked by intrusion DETECTION system – not possible as it is not IPS (prevention) just IDS

- D) – Python incompatibility with Ldap3 library is not probable as:

"Ldap3 is a pure Python LDAP 3 client library strictly conforming to RFC4510 and is released under the LGPL v3 open source license. RFC4510 is the current LDAP specification (June 2006)

...
Ldap3 can be used with any Python version starting from 2.6, including all Python 3 versions. It also works with PyPy and PyPy3."

Ref.: <https://ldap3.readthedocs.io/en/latest/>

upvoted 1 times

✉  [Gibsonmd](#) 8 months, 2 weeks ago

Selected Answer: C

Since the system only accepts secure LDAP connections, the CEH must explicitly enable SSL when initializing the connection in Python. If use_ssl=True is not set, the connection will fail or not return the expected data.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 149 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 149

Topic #: 1

[\[All 312-50v13 Questions\]](#)

An audacious attacker is targeting a web server you oversee. He intends to perform a Slow HTTP POST attack, by manipulating 'a' HTTP connection. Each connection sends a byte of data every 'b' second, effectively holding up the connections for an extended period. Your server is designed to manage 'm' connections per second, but any connections exceeding this number tend to overwhelm the system. Given 'a=100' and variable 'm', along with the attacker's intention of maximizing the attack duration 'D=a*b', consider the following scenarios. Which is most likely to result in the longest duration of server unavailability?

- A. m=90, b=15: The server can manage 90 connections per second, but the attacker's 100 connections exceed this, and with each connection held up for 15 seconds, the attack duration could be significant. **Most Voted**
- B. m=105, b=12: The server can manage 105 connections per second, more than the attacker's 100 connections, likely maintaining operation despite a moderate hold-up time.
- C. m=110, b=20: Despite the attacker sending 100 connections, the server can handle 110 connections per second, therefore likely staying operative, regardless of the hold-up time per connection.
- D. m=95, b=10: Here, the server can handle 95 connections per second, but it falls short against the attacker's 100 connections, albeit the hold-up time per connection is lower.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [Gibsonmd](#) at March 16, 2025, 2:02 a.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: A

- ◆ A. m=90, b=15

Attacker opens 100 connections, server can handle only 90, so overloaded.

Each connection stays open for 15 seconds ⇒ Total duration:

$$D = 100 * 15 = 1500 \text{ seconds}$$

Longest hold time and server is overwhelmed

 Most damaging scenario

upvoted 2 times

  [Gibsonmd](#) 8 months, 2 weeks ago

Selected Answer: A

The attacker's 100 connections exceed the server limit, keeping connections tied up for 15 seconds. Server remains functional because it can handle more than 100 connections.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 152 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 152

Topic #: 1

[\[All 312-50v13 Questions\]](#)

A network security analyst, while conducting penetration testing, is aiming to identify a service account password using the Kerberos authentication protocol. They have a valid user authentication ticket (TGT) and decided to carry out a Kerberoasting attack. In the scenario described, which of the following steps should the analyst take next?

- A. Carry out a passive wire sniffing operation using Internet packet sniffers
- B. Perform a PRobability INfinite Chained Elements (PRINCE) attack
- C. Extract plaintext passwords, hashes, PIN codes, and Kerberos tickets using a tool like Mimikatz
- D. Request a service ticket for the service principal name of the target service account

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Gibsonmd](#) at March 16, 2025, 2:16 a.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: D

Kerberoasting involves requesting a service ticket (TGS) for a service principal name (SPN) associated with a service account.

Once the service ticket is obtained, the attacker extracts the encrypted part of the ticket, which can be brute-forced offline to reveal the service account's plaintext password.

upvoted 1 times

  [Gibsonmd](#) 8 months, 2 weeks ago

Selected Answer: D

A Kerberoasting attack is a post-exploitation attack where an attacker with a valid Ticket Granting Ticket (TGT) requests a service ticket (TGS) for a service account in an Active Directory environment. The goal is to obtain a TGS ticket encrypted with the service account's NTLM hash, which can then be cracked offline to recover the plaintext password.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 153 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 153

Topic #: 1

[All 312-50v13 Questions]

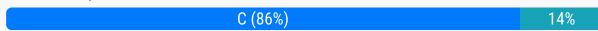
As a cybersecurity analyst at IoT Defend, you are working with a large utility company that uses Industrial Control Systems (ICS) in its operational technology (OT) environment. The company has recently integrated IoT devices into this environment to enable remote monitoring and control. They want to ensure these devices do not become a weak link in their security posture. To identify potential vulnerabilities in the IoT devices, which of the following actions should you recommend as the first step?

- A. Use stronger encryption algorithms for data transmission between IoT devices.
- B. Implement network segmentation to isolate IoT devices from the rest of the network.
- C. Conduct a vulnerability assessment specifically for the IoT devices. **Most Voted**
- D. Install the latest antivirus software on each IoT device.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by **Gibsond** at March 16, 2025, 2:24 a.m.

Comments

lopesjaf 4 months ago

Selected Answer: C

Conducting a vulnerability assessment is the foundational step to understand the current security posture of the IoT devices by identifying weaknesses, misconfigurations, outdated firmware, or vulnerabilities.

upvoted 1 times

Luispe 5 months ago

Selected Answer: C

Conduct a vulnerability assessment specifically for the IoT devices.

upvoted 1 times

NikoTomas 8 months, 1 week ago

Selected Answer: C

Correct is C)

Read question:

"To identify potential vulnerabilities in the IoT devices, which of the following actions..."

Segmentation in IoT networks is correct design but that's not what they are asking about.

To identify vulnerabilities, perform vulnerability scan and assessment = C)

upvoted 3 times

killwitch 8 months, 2 weeks ago

Selected Answer: C

C. Conduct a vulnerability assessment specifically for the IoT devices.

Before implementing any security measures, the first step should always be to identify existing vulnerabilities. A vulnerability assessment will:

- Identify weaknesses in the IoT devices (e.g., outdated firmware, weak authentication, open ports).
- Help prioritize security fixes based on risk levels.
- Provide a clear security baseline before making further security improvements.

upvoted 1 times

Gibsond 8 months, 2 weeks ago

Selected Answer: B

Isolates vulnerable IoT devices from critical systems, preventing lateral movement in case of compromise and limits attack surfaces
upvoted 1 times

 EXAM 312-50V13 TOPIC 1 QUESTION 154 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 154

Topic #: 1

[All 312-50v13 Questions]

A penetration tester is performing an enumeration on a client's network. The tester has acquired permission to perform enumeration activities. They have identified a remote inter-process communication (IPC) share and are trying to collect more information about it. The tester decides to use a common enumeration technique to collect the desired data. Which of the following techniques would be most appropriate for this scenario?

- A. Probe the IPC share by attempting to brute force admin credentials **Most Voted**
- B. Brute force Active Directory
- C. Extract usernames using email IDs
- D. Conduct a DNS zone transfer

[Hide Answer](#)

Suggested Answer: A

Community vote distribution



by [Gibsonmd](#) at March 16, 2025, 2:28 a.m.

Comments

✉ **lopesjaf** 4 months ago

Selected Answer: A

To enumerate a remote IPC share, probing it with authentication attempts (e.g., brute forcing admin credentials) is a common and effective method.

upvoted 1 times

✉ **e30b32d** 6 months, 1 week ago

Selected Answer: A

A - correct answer - Probe the IPC share by attempting to brute force admin credentials

upvoted 1 times

✉ **hiddenmessages** 7 months, 2 weeks ago

Selected Answer: C

Why would you brute force when the goal is just enumeration? Answer is C

upvoted 1 times

✉ **killwitch** 8 months, 2 weeks ago

Selected Answer: A

A. Probe the IPC share by attempting to brute-force admin credentials

Inter-Process Communication (IPC) shares are used for data exchange between processes and can be a common target for enumeration in Windows environments.

If misconfigured, IPC shares can leak sensitive information, such as usernames, service accounts, or even password hashes.

Brute-forcing admin credentials against the IPC share is a logical step to see if weak or default credentials can be exploited for further access.

upvoted 2 times

✉ **Gibsonmd** 8 months, 2 weeks ago

Selected Answer: C

When performing network enumeration or reconnaissance, attackers often try to extract usernames from publicly available data, such as email addresses.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 157 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 157

Topic #: 1

[\[All 312-50v13 Questions\]](#)

You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions. Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest. However, they are unsure of how to securely manage and distribute the symmetric keys to users. Which of the following strategies would you recommend to them?

- A. Use hash functions to distribute the keys.
- B. Use HTTPS protocol for secure key transfer.
- C. Use digital signatures to encrypt the symmetric keys.
- D. Implement the Diffie-Hellman protocol for secure key exchange. Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Gibsonmd](#) at March 16, 2025, 5:34 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: D

Use Diffie-Hellman to securely exchange symmetric keys between users and the cloud platform before encrypting data at rest.
upvoted 1 times

  [Gibsonmd](#) 8 months, 2 weeks ago

Selected Answer: D

Symmetric encryption is fast and efficient for encrypting data at rest, but it requires secure key distribution because both encryption and decryption use the same key. The Diffie-Hellman (DH) protocol is a widely used method for secure key exchange over an insecure channel without needing prior shared secrets.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 163 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 163

Topic #: 1

[\[All 312-50v13 Questions\]](#)

You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a suitable replacement to enhance the security of the company's wireless network?

- A. Open System authentication
- B. WPA2-PSK with AES encryption Most Voted
- C. SSID broadcast disabling
- D. MAC address filtering

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Gibsonmd](#) at March 16, 2025, 6:09 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: B

If available, WPA3 would be even better than WPA2. But if WPA3 is not an option, WPA2 with AES remains the recommended secure alternative to WEP.

upvoted 1 times

  [Gibsonmd](#) 8 months, 2 weeks ago

Selected Answer: B

The best replacement for WEP is WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) with AES encryption because, AES (Advanced Encryption Standard) is highly secure and resistant to brute-force attacks, and WPA2-PSK provides strong encryption for home and small business networks that do not use enterprise authentication.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 168 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 168

Topic #: 1

[\[All 312-50v13 Questions\]](#)

You are a cybersecurity trainee tasked with securing a small home network. The homeowner is concerned about potential "Wi-Fi eavesdropping," where unauthorized individuals could intercept the wireless communications. What would be the most effective first step to mitigate this risk, considering the simplicity and the residential nature of the network?

- A. Disable the network's SSID broadcast
- B. Enable encryption on the wireless network Most Voted
- C. Enable MAC address filtering
- D. Reduce the signal strength of the wireless router

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Gibsonmd](#) at March 16, 2025, 6:25 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: B

Wi-Fi eavesdropping refers to unauthorized individuals intercepting data transmitted over a wireless network. The most effective first step to prevent this is to encrypt the wireless traffic, ensuring that even if someone intercepts the data, it is unreadable without the encryption key.
upvoted 1 times

  [killwitch](#) 8 months, 2 weeks ago

Selected Answer: B

B. Enable encryption on the wireless network.

Encryption (WPA2 or WPA3) ensures that the data transmitted over the network is encrypted, making it much more difficult for unauthorized individuals to intercept and read the communication. This is the most effective method to secure wireless traffic from eavesdropping, especially in a home network scenario.

upvoted 1 times

  [Gibsonmd](#) 8 months, 2 weeks ago

Selected Answer: B

You are a cybersecurity trainee tasked with securing a small home network. The homeowner is concerned about potential "Wi-Fi eavesdropping," where unauthorized individuals could intercept the wireless communications. What would be the most effective first step to mitigate this risk, considering the simplicity and the residential nature of the network?

- A. Disable the network's SSID broadcast
- B. Enable encryption on the wireless network
- C. Enable MAC address filtering
- D. Reduce the signal strength of the wireless router

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 171 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 171

Topic #: 1

[\[All 312-50v13 Questions\]](#)

A company recently experienced a debilitating social engineering attack that led to substantial identity theft. An inquiry found that the employee inadvertently provided critical information during an innocuous phone conversation. Considering the specific guidelines issued by the company to thwart social engineering attacks, which countermeasure would have been the most successful in averting the incident?

- A. Conduct comprehensive training sessions for employees on various social engineering methodologies and the risks associated with revealing confidential data. **Most Voted**
- B. Implement a well-documented change management process for modifications related to hardware or software.
- C. Adopt a robust software policy that restricts the installation of unauthorized applications.
- D. Reinforce physical security measures to limit access to sensitive zones within the company premises, thereby warding off unauthorized intruders.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  **Gibsonmd** at March 16, 2025, 8:26 p.m.

Comments

 **lopesjaf** 4 months ago

Selected Answer: A

The incident involved an employee inadvertently revealing critical information during a phone conversation, a classic social engineering tactic.

The best defense against social engineering is employee awareness and training so they can recognize and appropriately respond to manipulation attempts.

Training helps employees understand the risks and the importance of not disclosing confidential data over phone or other communication channels.

upvoted 1 times

 **Gibsonmd** 8 months, 2 weeks ago

Selected Answer: A

Social engineering attacks exploit human psychology rather than technical vulnerabilities. Since the breach occurred because an employee unknowingly provided critical information over a phone call, the most effective preventive measure is comprehensive employee training on social engineering tactics and awareness.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 174 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 174

Topic #: 1

[\[All 312-50v13 Questions\]](#)

During a recent vulnerability assessment of a major corporation's IT systems, the security team identified several potential risks. They want to use a vulnerability scoring system to quantify and prioritize these vulnerabilities. They decide to use the Common Vulnerability Scoring System (CVSS). Given the characteristics of the identified vulnerabilities, which of the following statements is the most accurate regarding the metric types used by CVSS to measure these vulnerabilities?

- A. Temporal metric represents the inherent qualities of a vulnerability.
- B. Base metric represents the inherent qualities of a vulnerability. **Most Voted**
- C. Temporal metric involves measuring vulnerabilities based on a specific environment or implementation.
- D. Environmental metric involves the features that change during the lifetime of the vulnerability.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Gibsonmd](#) at March 16, 2025, 8:34 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: B

Base metrics represent the intrinsic, fundamental characteristics of a vulnerability that are constant over time and across environments. This includes aspects like attack vector, complexity, privileges required, impact on confidentiality, integrity, and availability.

Temporal metrics reflect characteristics that change over time, such as exploitability, remediation level, and report confidence.

Environmental metrics represent the features that are specific to a particular environment or implementation and measure how the vulnerability's impact changes in

upvoted 1 times

  [Gibsonmd](#) 8 months, 2 weeks ago

Selected Answer: B

The Base metric measures the inherent, unchanging qualities of a vulnerability (such as whether it is remotely exploitable or affects confidentiality).

upvoted 1 times

 EXAM 312-50V13 TOPIC 1 QUESTION 176 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 176

Topic #: 1

[All 312-50v13 Questions]

In an advanced digital security scenario, a multinational enterprise is being targeted with a complex series of assaults aimed to disrupt operations, manipulate data integrity, and cause serious financial damage. As the Lead Cybersecurity Analyst with CEH and CISSP certifications, your responsibility is to correctly identify the specific type of attack based on the following indicators:

The attacks are exploiting a vulnerability in the target system's hardware, inducing misprediction of future instructions in a program's control flow. The attackers are strategically inducing the victim process to speculatively execute instruction sequences that would not have been executed in the absence of the misprediction, leading to subtle side effects. These side effects, which are observable from the shared state, are then utilized to infer the values of in-flight data.

What type of attack best describes this scenario?

A. Rowhammer Attack

B. Watering Hole Attack

C. Side-Channel Attack Most Voted

D. Privilege Escalation Attack

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [GibsonD](#) at March 16, 2025, 8:49 p.m.

Comments

 [lopesjaf](#) 4 months ago

Selected Answer: C

The attack involves exploiting speculative execution and misprediction in hardware, causing the victim process to execute instructions that leak sensitive data via side effects in the system's shared state.

This matches the characteristics of side-channel attacks like Spectre and Meltdown, which leverage hardware vulnerabilities to infer sensitive data by observing indirect effects (timing, cache states, etc.).

upvoted 1 times

 [e30b32d](#) 6 months, 1 week ago

Selected Answer: C

Exploit a hardware-level vulnerability.

Force the CPU to mis-predict control flow (typically through branch prediction).

Leverage speculative execution to access in-flight (uncommitted) data.

Use observable side effects (like CPU cache state changes) to infer sensitive data.

This technique is characteristic of side-channel attacks, particularly Spectre and Meltdown, which are prime examples of exploiting speculative execution and microarchitectural side channels.

upvoted 1 times

 [GibsonD](#) 8 months, 2 weeks ago

Selected Answer: C

key give away to a side channel attack is that it effects the "hardware"

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 177 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 177

Topic #: 1

[\[All 312-50v13 Questions\]](#)

In the process of implementing a network vulnerability assessment strategy for a tech company, the security analyst is confronted with the following scenarios:

- 1) A legacy application is discovered on the network, which no longer receives updates from the vendor.
- 2) Several systems in the network are found running outdated versions of web browsers prone to distributed attacks.
- 3) The network firewall has been configured using default settings and passwords.
- 4) Certain TCP/IP protocols used in the organization are inherently insecure.

The security analyst decides to use vulnerability scanning software. Which of the following limitations of vulnerability assessment should the analyst be most cautious about in this context?

- A. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations Most Voted
- B. Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed
- C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time
- D. Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (50%)

C (25%)

B (25%)

by  [GibsonD](#) at March 16, 2025, 8:50 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: B

Vulnerability scanners rely on databases of known vulnerabilities and detection logic, which may have flaws or gaps, causing them to miss serious vulnerabilities.

upvoted 1 times

  [KnightHeart](#) 6 months ago

Selected Answer: C

C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time

Dependence on Updated Vulnerability Databases:

Vulnerability scanners rely on predefined signatures and knowledge bases to identify known issues. For legacy applications (Scenario 1) and outdated browsers (Scenario 2), the scanner can only detect vulnerabilities if:

The vendor's updates (which may include patch information) are no longer available, and

The scanner's database includes entries for the specific outdated versions in use.

upvoted 1 times

  [KnightHeart](#) 6 months ago

If the scanner's database is not updated, it may miss:

Newly discovered vulnerabilities in unsupported software,
Exploits for browser versions that are no longer maintained, or
Configuration flaws in protocols that have since been deemed insecure.

Inability to Predict Emerging Threats:

Inherently insecure protocols (Scenario 4) may have known risks, but the scanner must have dedicated checks to flag them. If the scanner lacks modules for these protocols (e.g., Telnet, FTP), it will overlook their risks.

Default firewall settings (Scenario 3) may include known insecure configurations, but the scanner must have rules to detect such defaults. If these rules are absent or outdated, the risks remain undetected.

Time-Bound Detection Capability:

A scan provides a snapshot of vulnerabilities at a specific moment. If a zero-day exploit emerges for an outdated browser after the scan, the scanner cannot identify it, highlighting the limitation of relying on historical data.

upvoted 1 times

 **KnightHeart** 6 months ago

Not A.

While impact assessment is important for prioritization, the scenarios focus on detecting vulnerabilities rather than evaluating their business impact.

The analyst's first step is to identify risks, and impact analysis can follow via separate business context evaluation.

upvoted 1 times

 **Cherubael** 7 months ago

Selected Answer: A

What answer A. should have been worded as: "Vulnerability scanners cannot define a vulnerability's impact on business operations."

This is a really dumb question that should not even be on the exam due to the poor verbiage in the multiple choice.

upvoted 1 times

 **Gibsomd** 8 months, 2 weeks ago

Selected Answer: A

Vulnerability scanners are automated tools designed to identify security weaknesses in a network, but they do not provide contextual insights into how these vulnerabilities impact specific business operations.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 185 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 185

Topic #: 1

[\[All 312-50v13 Questions\]](#)

In a recent cyber-attack against a large corporation, an unknown adversary compromised the network and began escalating privileges and lateral movement. The security team identified that the adversary used a sophisticated set of techniques, specifically targeting zero-day vulnerabilities. As a Certified Ethical Hacker (CEH) hired to understand this attack and propose preventive measures, which of the following actions will be most crucial for your initial analysis?

- A. Identifying the specific tools used by the adversary for privilege escalation.
- B. Analyzing the initial exploitation methods, the adversary used. **Most Voted**
- C. Checking the persistence mechanisms used by the adversary in compromised systems.
- D. Investigating the data exfiltration methods used by the adversary.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Gibsonmd](#) at March 17, 2025, 12:37 a.m.

Comments

  [lopesjaf](#) 3 months, 4 weeks ago

Selected Answer: B

When responding to a cyber-attack that involves zero-day vulnerabilities, the most crucial first step is to understand how the attacker got in. This involves analyzing the initial exploitation methods — i.e., the entry point of the attack.

upvoted 1 times

  [Gibsonmd](#) 8 months, 2 weeks ago

Selected Answer: B

When investigating a cyberattack involving zero-day vulnerabilities, the first priority is to understand how the attacker initially exploited the system.

upvoted 2 times

 EXAM 312-50V13 TOPIC 1 QUESTION 203 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 203

Topic #: 1

[All 312-50v13 Questions]

An ethical hacker is hired to conduct a comprehensive network scan of a large organization that strongly suspects potential intrusions into their internal systems. The hacker decides to employ a combination of scanning tools to obtain a detailed understanding of the network. Which sequence of actions would provide the most comprehensive information about the network's status?

A. Use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities. **Most Voted**

B. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities.

C. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3.

D. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [killwitch](#) at March 18, 2025, 3:35 p.m.

Comments

 [lopesjaf](#) 3 months, 4 weeks ago

Selected Answer: A

Step 1: Hping3 ICMP ping scan

This efficiently discovers live hosts on the network by sending ICMP echo requests. It's a good first step for network reconnaissance.

Step 2: Nmap SYN scan on active hosts

Once live hosts are identified, an Nmap SYN scan quickly and stealthily determines open TCP ports and services, revealing potential vulnerabilities.

Step 3: Metasploit exploitation

With known open ports and services, Metasploit can be used to exploit identified vulnerabilities for further penetration testing.

upvoted 2 times

 [killwitch](#) 8 months, 2 weeks ago

Selected Answer: A

This sequence of actions provides the most structured and comprehensive approach to network scanning and penetration testing:

Hping3 for ICMP Ping Scan:

Identifies live hosts on the network by sending ICMP Echo Requests. Can bypass some firewalls and filters compared to standard ping. Helps to narrow down the target list for further scanning.

Nmap for SYN Scan:

Performs a stealthy port scan on the active hosts identified in the first step. Helps detect open ports and running services without completing a full TCP handshake. Can be combined with service and version detection for deeper analysis.

Metasploit for Exploitation:

Uses vulnerabilities identified in the scanning phase. Helps determine real-world risks by testing for possible exploitation. Provides insights into security weaknesses that need patching.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 181 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 181

Topic #: 1

[\[All 312-50v13 Questions\]](#)

An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the following tools would be the best choice for this purpose and why?

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files

Most Voted

B. Koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware

C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (67%)

D (33%)

by  NikoTomas at March 22, 2025, 10:31 p.m.

Comments

  lopesjaf 3 months, 4 weeks ago

Selected Answer: A

The question is about reinforcing intrusion detection with YARA rules and finding a tool that complements Snort, specifically with a rule-based approach. The goal is to generate high-quality YARA rules to detect malware or anomalies more effectively.
upvoted 1 times

  KnightHeart 6 months ago

Selected Answer: D

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files

A. yarGen - Generates YARA rules from malware strings, removing those in goodware

B. Koodous - Combines social networking with antivirus signatures and YARA rules

C. YaraRET - Helps reverse engineer Trojans to generate YARA rules

upvoted 1 times

  NikoTomas 8 months, 1 week ago

Selected Answer: A

Answer: A

A. yarGen

 yarGen is a tool that automatically generates YARA rules from binary files by extracting suspicious strings found in malware and filtering out common strings found in clean software (goodware). It's often used in malware analysis and threat hunting.

B. Koodous

 Koodous is a collaborative malware analysis platform that combines social interaction, antivirus engine results, and YARA rules to enable the community to analyze and label Android apps. It allows users to create and apply YARA rules to large repositories of apps.

C. YaraRET

 YaraRET (YARA Rule Extraction Tool) assists in reverse engineering by extracting strings, constants, and patterns from disassembled malware, helping analysts create custom YARA rules based on reverse-engineered code.

D. AutoYara

 AutoYara is a framework that automates the creation of YARA rules by comparing known malware samples with clean files to identify distinctive byte patterns, useful for automated signature generation at scale.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 212 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 212

Topic #: 1

[\[All 312-50v13 Questions\]](#)

A large corporate network is being subjected to repeated sniffing attacks. To increase security, the company's IT department decides to implement a combination of several security measures. They permanently add the MAC address of the gateway to the ARP cache, switch to using IPv6 instead of IPv4, implement the use of encrypted sessions such as SSH instead of Telnet, and use Secure File Transfer Protocol instead of FTP. However, they are still faced with the threat of sniffing. Considering the countermeasures, what should be their next step to enhance network security?

- A. Use HTTP instead of HTTPS for protecting usernames and passwords
- B. Implement network scanning and monitoring tools Most Voted
- C. Enable network identification broadcasts
- D. Retrieve MAC addresses from the OS

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [NikoTomas](#) at March 23, 2025, 2:39 p.m.

Comments

  [lopesjaf](#) 3 months, 4 weeks ago

Selected Answer: B

- B. Implement network scanning and monitoring tools

This is a strong defensive approach: detecting ongoing sniffing attacks or suspicious traffic.

Tools like IDS/IPS, network monitors, or anomaly detection can help identify sniffers or man-in-the-middle activity.

It complements existing encryption and static ARP defenses by actively detecting attacks.

upvoted 1 times

  [NikoTomas](#) 8 months, 1 week ago

Selected Answer: B

Answer: B

o They deployed encrypted protocols (HTTPS, FTPS, etc..) so the communication must be encrypted end-to-end.
This means that sniffing, even if it is still ongoing, don't have an effect (the attacker can't read encrypted data).

If sniffing is still happening, we can suppose that it can be carried out for example on network device (SPAN port, if attacker has such access) or on the endpoint itself (capturing traffic before it gets encrypted – but it is more about malware than network sniffing).

However, sniffing can occur on encrypted traffic as well (it has no effect but it is still sniffing on the network).

To resolve this tricky situation, implementing network scanning and monitoring tools looks like most appropriate solution - B).

upvoted 1 times

  [NikoTomas](#) 8 months, 1 week ago

Incorrect answers:

C) - Network Identification Broadcast is a network-layer broadcast message used by certain legacy systems or protocols to announce the presence of a host or network segment to other devices on the same local network. It's typically used for discovery, name resolution, or service announcement.

You do not want to enable it to make your services being advertised to the attacker.

D) Retrieve MAC addresses from the OS – well, it may help in investigation if there is some communication with suspicious host(s) in the LAN, but I think it doesn't satisfy question: "step to enhance network security".

But implementing scanning and monitoring tools (B) enhances it.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 218 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 218

Topic #: 1

[All 312-50v13 Questions]

An ethical hacker is testing the security of a website's database system against SQL Injection attacks. They discover that the IDS has a strong signature detection mechanism to detect typical SQL injection patterns. Which evasion technique can be most effectively used to bypass the IDS signature detection while performing a SQL Injection attack?

- A. Employ IP fragmentation to obscure the attack payload Most Voted
- B. Implement case variation by altering the case of SQL statements
- C. Leverage string concatenation to break identifiable keywords
- D. Use Hex encoding to represent the SQL query string

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by NikoTomas at March 25, 2025, 9:03 p.m.

Comments

kingq 4 months ago

Selected Answer: C

Correct Answer: C. Leverage string concatenation to break identifiable keywords

Explanation:

In this scenario, the IDS (Intrusion Detection System) is using signature-based detection to identify SQL injection attacks. These signatures typically look for known patterns such as:
UNION SELECT
' OR '1'='1
DROP TABLE, etc.
upvoted 1 times

KnightHeart 6 months, 1 week ago

Selected Answer: D

D: Highly effective for bypassing static keyword-based signatures, as the IDS sees encoded data instead of plaintext SQL keywords.
upvoted 2 times

NikoTomas 8 months, 1 week ago

Selected Answer: A

Answer: A

According to EC-Council training materials (especially CEH — Certified Ethical Hacker), the most effective evasion technique against signature-based Intrusion Detection Systems (IDS) is:

Employing IP Fragmentation

"IP fragmentation is one of the most effective techniques to evade signature-based IDS, as it breaks the attack payload into multiple packets that may not be reassembled correctly by the IDS."

upvoted 1 times

NikoTomas 8 months, 1 week ago

Other Options Explained:

B. Implement case variation by altering the case of SQL statements

- Most modern IDSs normalize input.

- 🚫 Limited effectiveness.

C. Leverage string concatenation to break identifiable keywords

- Turns UNION SELECT into UNI + ON SEL + ECT

- Some IDS systems detect common string obfuscation patterns, so this is partially effective, but not stealthy.

 Moderately useful for application-level filters, but weaker at the network layer.

- D. Use Hex encoding to represent the SQL query string
 - Converts payload to something like 0x73656c65637420 (select)
 - Many modern IDS/IPS systems decode hex automatically
-  Good for bypassing input filters, less effective at evading advanced IDS.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 224 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 224

Topic #: 1

[All 312-50v13 Questions]

An ethical hacker is preparing to scan a network to identify live systems. To increase the efficiency and accuracy of his scans, he is considering several different host discovery techniques. He expects several unused IP addresses at any given time, specifically within the private address range of the LAN, but he also anticipates the presence of restrictive firewalls that may conceal active devices. Which scanning method would be most effective in this situation?

- A. ICMP ECHO Ping Sweep
- B. ICMP Timestamp Ping
- C. TCP SYN Ping
- D. ARP Ping Scan **Most Voted**

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by [NikoTomas](#) at March 26, 2025, 7:21 p.m.

Comments

lopesjaf 3 months, 4 weeks ago

Selected Answer: D

For discovering live hosts in a private LAN with firewalls, ARP Ping Scan is the best choice because it directly queries MAC addresses on the local network and cannot be blocked by IP-level firewalls.

upvoted 1 times

[Removed] 7 months, 2 weeks ago

Selected Answer: D

D is the correct answer.
ARP Ping Scan operates at Layer 2 (Data Link Layer) and is highly effective in local networks (LANs). It identifies live hosts by sending ARP requests and waiting for ARP replies, which are not blocked by firewalls that filter higher-layer protocols like ICMP or TCP.

Since the network is within a private address range and restrictive firewalls are anticipated, ARP Ping Scan is ideal because it bypasses these restrictions and accurately detects active devices.

upvoted 2 times

KnightHeart 5 months, 4 weeks ago

Only suitable for narrow local subnet scans, not for networks with complex configurations.

upvoted 1 times

hiddenmessages 7 months, 2 weeks ago

Selected Answer: D

I meant it's all a LAN*

upvoted 2 times

hiddenmessages 7 months, 2 weeks ago

Selected Answer: D

question doesn't say the firewall switches to a WAN. It's all a WAN there is no need to use TCP SYN which will get detected by a firewall.

upvoted 2 times

NikoTomas 8 months, 1 week ago

Selected Answer: C

Correct: C - TCP SYN "ping"

Incorrect answers:

- A) Ping sweep would be fine inside LAN but its worse when getting through firewalls (mentioned in question)
- B) Same as A) but even worse - it's less probable that ICMP Timestamp requests will be allowed through FW than ICMP Echo in A).
- D) ARP can't traverse behind FW, it's pure LAN protocol between L2/L3 layers, can't be routed out of LAN
upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 250 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 250

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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. Most Voted
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [NikoTomas](#) at March 27, 2025, 5:31 p.m.

Comments

  [NikoTomas](#) 8 months ago

Selected Answer: B

Answer: B - determine impact

In the CEH curriculum, EC-Council emphasizes that before enabling system auditing, organizations should:

- Understand the technical and performance impact
- Consider how enabling auditing affects system performance, storage, and logging capacity
- Analyze which events to audit to avoid excessive or irrelevant log collection

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 279 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 279

Topic #: 1

[\[All 312-50v13 Questions\]](#)

What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?

- A. FISMA
- B. PCI-DSS
- C. SOX
- D. ISO/IEC 27001:2013

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [NikoTomas](#) at March 27, 2025, 8:33 p.m.

Comments

  [lopesjaf](#) 3 months, 4 weeks ago

Selected Answer: C

The Sarbanes-Oxley Act (SOX) was enacted to protect investors, stakeholders, and the public by improving the accuracy and reliability of corporate disclosures, preventing accounting fraud and errors.

SOX mandates strict reforms to enhance corporate governance and accountability.

It is primarily focused on financial reporting and auditing controls within organizations.

upvoted 1 times

  [NikoTomas](#) 8 months ago

Selected Answer: C

Answer: C (SOX)

The Sarbanes-Oxley Act (SOX), enacted in 2002 in the United States, is a federal law aimed at:

- Protecting stakeholders, investors, and the public
- Preventing accounting fraud, financial misreporting, and corporate misconduct
- Enforcing transparency and internal controls in financial reporting

SOX is primarily about financial accountability, but it has information security implications, such as:

- Requiring secure storage of financial records
- Ensuring data integrity
- Monitoring and logging access to financial systems
- Supporting auditability and traceability

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 40 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 40

Topic #: 1

[All 312-50v13 Questions]

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 **Most Voted**

B. FTP

C. HTTPS

D. IP

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (83%) B (17%)

by  Fiete at April 2, 2025, 7:01 p.m.

Comments

 **lopesjaf** 4 months ago

Selected Answer: A

Bella is dealing with file transfers that originally occurred in plaintext, leading to session hijacking risks. She responds by implementing encryption and digital certificates, which indicates the use of FTPS.

upvoted 1 times

 **GSH** 5 months, 3 weeks ago

Selected Answer: A

Answer is A once configured

upvoted 1 times

 **e30b32d** 6 months, 1 week ago

Selected Answer: A

correct answer option a) FTPS- FTPS includes full support for the TLS and SSL cryptographic protocols, including the use of serverside public key authentication certificates and client-side authorization certificates

upvoted 2 times

 **sokucutayfa** 6 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

 **sokucutayfa** 6 months, 1 week ago

Selected Answer: B

Shared in plaintext that's why it needs to be FTP.

upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 87 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 87

Topic #: 8

[\[All 312-50 Questions\]](#)

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 Most Voted
- B. Privilege escalation
- C. Directory traversal
- D. Brute force login A

[Hide Answer](#)

Suggested Answer: Explanation

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

References: http://codex.wordpress.org/Hardening_WordPress

Community vote distribution

A (100%)

by  [youngins](#) at April 4, 2020, 10:07 p.m.

Comments

  [tyw82](#) 1 year, 1 month ago

Selected Answer: A

Not B because it says the the activities were done by the 'anonymous user account' which logged in to the server.
upvoted 1 times

  [igodomigododecenter](#) 1 year, 7 months ago

Selected Answer: A

File system permission is required to be able to run a script inside the folder
upvoted 1 times

  [Pragdeashwar](#) 1 year, 7 months ago

File System Permission, it is the weakness that allowed adversary to copy malicious file also allowed to execute it.
upvoted 1 times

  [Luukman](#) 4 years, 2 months ago

Ftp users don't have permissions to start processes. Privelige escalation is needed to achieve this
upvoted 1 times

  [Sasiron](#) 4 years, 11 months ago

File system permissions is correct
upvoted 1 times

  [amal1302](#) 5 years, 1 month ago

To upload files user needs file permissions
upvoted 2 times

  [youngins](#) 5 years, 7 months ago

A. file permission
upvoted 2 times

 **youngins** 5 years, 7 months ago

Privilege Escalation

upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 162 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 162

Topic #: 8

[All 312-50 Questions]

Emil uses nmap to scan two hosts using this command.

```
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
```

He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
161/tcp   closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

What is his conclusion?

- A. Host 192.168.99.7 is an iPad.
- B. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7. **Most Voted**
- C. Host 192.168.99.1 is the host that he launched the scan from.
- D. Host 192.168.99.7 is down. B

[Hide Answer](#)

Suggested Answer: Explanation

Community vote distribution

B (100%)

by  Smaug at May 8, 2020, 5:03 a.m.

Comments

✉  igodomigododevcenter 1 year ago

Selected Answer: B

B is the answer

upvoted 1 times

✉  dtwostar 1 year, 2 months ago

Selected Answer: B

He performed a -sS (SYN scan) and -O (OS scan) on hosts 192.168.99.1 and 192.168.99.7

upvoted 1 times

✉  aids00123 1 year, 9 months ago

Weird question. That's not really his conclusion, it's his action.

upvoted 2 times

✉  Smaug 5 years ago

He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.

-sS and -O options.

upvoted 4 times

EXAM 312-50 TOPIC 2 QUESTION 16 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 16

Topic #: 2

[\[All 312-50 Questions\]](#)

The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103  
Destination:192.168.1.106 Protocol:TCP  
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103  
Destination:192.168.1.106 Protocol:TCP  
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103  
Destination:192.168.1.106 Protocol:TCP  
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103  
Destination:192.168.1.106 Protocol:TCP  
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103  
Destination:192.168.1.106 Protocol:TCP  
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103  
Destination:192.168.1.106 Protocol:TCP  
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103  
Destination:192.168.1.106 Protocol:TCP
```

What type of activity has been logged?

- A. Port scan targeting 192.168.1.103
- B. Teardrop attack targeting 192.168.1.106
- C. Denial of service attack targeting 192.168.1.103
- D. Port scan targeting 192.168.1.106

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:04 p.m.

Comments

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

EXAM 312-50 TOPIC 2 QUESTION 19 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 19

Topic #: 2

[\[All 312-50 Questions\]](#)

What information should an IT system analysis provide to the risk assessor?

- A. Management buy-in
- B. Threat statement **Most Voted**
- C. Security architecture
- D. Impact analysis

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 B (50%)  C (50%)

by [deleted] at April 4, 2025, 12:05 p.m.

Comments

 **Amimu** 5 months, 1 week ago

Selected Answer: C

One of the results of performing a systems analysis is how the systems are designed and interact. The outcome of this is a systems architecture. The risks assessor analyses the architecture to establish threat sources and impacts. Management buy-in is a process of soliciting for financial and other support from management to assist with implementing presented solutions that mitigate identified threats.

upvoted 1 times

 **ethanlxx** 5 months, 1 week ago

Selected Answer: B

Threat statement outline potential threat an It system may face

upvoted 1 times

EXAM 312-50 TOPIC 2 QUESTION 27 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 27

Topic #: 2

[\[All 312-50 Questions\]](#)

Least privilege is a security concept that requires that a user is

- A. limited to those functions required to do the job.
- B. given root or administrative privileges.
- C. trusted to keep all data and access to that data under their sole control.
- D. given privileges equal to everyone else in the department.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:05 p.m.

Comments

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

EXAM 312-50 TOPIC 2 QUESTION 28 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 28

Topic #: 2

[\[All 312-50 Questions\]](#)

If the final set of security controls does not eliminate all risk in a system, what could be done next?

- A. Continue to apply controls until there is zero risk.
- B. Ignore any remaining risk.
- C. If the residual risk is low enough, it can be accepted.
- D. Remove current controls since they are not completely effective.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:05 p.m.

Comments

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

EXAM 312-50 TOPIC 3 QUESTION 2 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 2

Topic #: 3

[\[All 312-50 Questions\]](#)

Which type of access control is used on a router or firewall to limit network activity?

- A. Mandatory
- B. Discretionary
- C. Rule-based
- D. Role-based

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:05 p.m.

Comments

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

EXAM 312-50 TOPIC 3 QUESTION 15 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 15

Topic #: 3

[\[All 312-50 Questions\]](#)

While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

- A. Validate web content input for query strings.
- B. Validate web content input with scanning tools.
- C. Validate web content input for type, length, and range.
- D. Validate web content input for extraneous queries.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:05 p.m.

Comments

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

EXAM 312-50 TOPIC 3 QUESTION 20 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 20

Topic #: 3

[\[All 312-50 Questions\]](#)

When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

- A. A bottom-up approach
- B. A top-down approach**
- C. A senior creation approach
- D. An IT assurance approach

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:06 p.m.

Comments

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

EXAM 312-50 TOPIC 3 QUESTION 41 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 41

Topic #: 3

[\[All 312-50 Questions\]](#)

A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.

During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.

Which of the following is an issue with the situation?

- A. Segregation of duties
- B. Undue influence
- C. Lack of experience
- D. Inadequate disaster recovery plan

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:06 p.m.

Comments

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

EXAM 312-50 TOPIC 3 QUESTION 53 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 53

Topic #: 3

[\[All 312-50 Questions\]](#)

A newly discovered flaw in a software application would be considered which kind of security vulnerability?

- A. Input validation flaw
- B. HTTP header injection vulnerability
- C. 0-day vulnerability
- D. Time-to-check to time-to-use flaw

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:06 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 3 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 3

Topic #: 4

[\[All 312-50 Questions\]](#)

An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

- A. The wireless card was not turned on.
- B. The wrong network card drivers were in use by Wireshark.
- C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
- D. Certain operating systems and adapters do not collect the management or control packets.

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:06 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 14 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 14

Topic #: 4

[\[All 312-50 Questions\]](#)

One advantage of an application-level firewall is the ability to

- A. filter packets at the network level.
- B. filter specific commands, such as http:post.
- C. retain state information for each packet.
- D. monitor tcp handshaking.

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:06 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 15 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 15

Topic #: 4

[\[All 312-50 Questions\]](#)

Which of the statements concerning proxy firewalls is correct?

- A. Proxy firewalls increase the speed and functionality of a network.
- B. Firewall proxy servers decentralize all activity for an application.
- C. Proxy firewalls block network packets from passing to and from a protected network.
- D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:07 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 17 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 17

Topic #: 4

[\[All 312-50 Questions\]](#)

While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

- A. 10.10.10.10
- B. 127.0.0.1
- C. 192.168.1.1
- D. 192.168.168.168

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:07 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 25 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 25

Topic #: 4

[\[All 312-50 Questions\]](#)

On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

- A. nessus +
- B. nessus *s
- C. nessus &
- D. nessus -d

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:07 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 26 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 26

Topic #: 4

[\[All 312-50 Questions\]](#)

Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

- A. NMAP
- B. Metasploit
- C. Nessus
- D. BeEF

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:07 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 27 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 27

Topic #: 4

[\[All 312-50 Questions\]](#)

What is the best defense against privilege escalation vulnerability?

- A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
- B. Run administrator and applications on least privileges and use a content registry for tracking.
- C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
- D. Review user roles and administrator privileges for maximum utilization of automation services.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:07 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 40 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 40

Topic #: 4

[\[All 312-50 Questions\]](#)

Which of the following is a hashing algorithm?

- A. MD5
- B. PGP
- C. DES
- D. ROT13

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:08 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 41 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 41

Topic #: 4

[\[All 312-50 Questions\]](#)

Which of the following problems can be solved by using Wireshark?

- A. Tracking version changes of source code
- B. Checking creation dates on all webpages on a server
- C. Resetting the administrator password on multiple systems
- D. Troubleshooting communication resets between two systems

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:08 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 44 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 44

Topic #: 4

[\[All 312-50 Questions\]](#)

Which of the following is an example of two factor authentication?

- A. PIN Number and Birth Date
- B. Username and Password
- C. Digital Certificate and Hardware Token
- D. Fingerprint and Smartcard ID

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:08 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 50 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 50

Topic #: 4

[\[All 312-50 Questions\]](#)

A security administrator notices that the log file of the company's webserver contains suspicious entries:

```
\[20/Mar/2011:10:49:07] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978
```

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include(' ../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

- A. command injection.
- B. SQL injection.**
- C. directory traversal.
- D. LDAP injection.

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:08 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 51 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 51

Topic #: 4

[\[All 312-50 Questions\]](#)

Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

- A. Firewall
- B. Honeypot**
- C. Core server
- D. Layer 4 switch

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:08 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 53 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 53

Topic #: 4

[\[All 312-50 Questions\]](#)

What results will the following command yield: 'NMAP -sS -O -p 123-153 192.168.100.3'?

- A. A stealth scan, opening port 123 and 153
- B. A stealth scan, checking open ports 123 to 153
- C. A stealth scan, checking all open ports excluding ports 123 to 153
- D. A stealth scan, determine operating system, and scanning ports 123 to 153

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:08 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 55 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 55

Topic #: 4

[\[All 312-50 Questions\]](#)

Which of the following open source tools would be the best choice to scan a network for potential targets?

- A. NMAP
- B. NIKTO
- C. CAIN
- D. John the Ripper

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:08 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 57 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 57

Topic #: 4

[\[All 312-50 Questions\]](#)

A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

- A. Fraggle
- B. MAC Flood
- C. Smurf
- D. Tear Drop

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:08 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 61 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 61

Topic #: 4

[\[All 312-50 Questions\]](#)

An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?

- A. By using SQL injection
- B. By changing hidden form values
- C. By using cross site scripting
- D. By utilizing a buffer overflow attack

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:09 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 64 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 64

Topic #: 4

[\[All 312-50 Questions\]](#)

A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:

NMAP n sS P0 p 80 ***.***.**.**

What type of scan is this?

- A. Quick scan
- B. Intense scan
- C. Stealth scan
- D. Comprehensive scan

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:09 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 65 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 65

Topic #: 4

[\[All 312-50 Questions\]](#)

What is the broadcast address for the subnet 190.86.168.0/22?

- A. 190.86.168.255
- B. 190.86.255.255
- C. 190.86.171.255
- D. 190.86.169.255

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:09 p.m.

Comments

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

EXAM 312-50 TOPIC 4 QUESTION 71 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 71

Topic #: 4

[\[All 312-50 Questions\]](#)

What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

- A. Scripting languages are hard to learn.
- B. Scripting languages are not object-oriented.
- C. Scripting languages cannot be used to create graphical user interfaces.
- D. Scripting languages are slower because they require an interpreter to run the code.

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:09 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 3 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 3

Topic #: 5

[\[All 312-50 Questions\]](#)

The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

- A. Multiple keys for non-repudiation of bulk data
- B. Different keys on both ends of the transport medium
- C. Bulk encryption for data transmission over fiber
- D. The same key on each end of the transmission medium

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:09 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 9 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 9

Topic #: 5

[\[All 312-50 Questions\]](#)

Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?

- A. Certificate issuance
- B. Certificate validation**
- C. Certificate cryptography
- D. Certificate revocation

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:09 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 10 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 10

Topic #: 5

[\[All 312-50 Questions\]](#)

Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

- A. Key registry
- B. Recovery agent
- C. Directory
- D. Key escrow

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:09 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 11 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 11

Topic #: 5

[\[All 312-50 Questions\]](#)

To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

- A. Harvesting
- B. Windowing
- C. Hardening
- D. Stealthing

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:09 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 13 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 13

Topic #: 5

[\[All 312-50 Questions\]](#)

The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?

- A. Investigate based on the maintenance schedule of the affected systems.
- B. Investigate based on the service level agreements of the systems.
- C. Investigate based on the potential effect of the incident.
- D. Investigate based on the order that the alerts arrived in.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:10 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 15 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 15

Topic #: 5

[\[All 312-50 Questions\]](#)

Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

- A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
- B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
- C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
- D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:10 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 20 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 20

Topic #: 5

[\[All 312-50 Questions\]](#)

Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

- A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
- B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
- C. Configure the firewall to allow traffic on TCP port 53.
- D. Configure the firewall to allow traffic on TCP port 8080.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:10 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 21 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 21

Topic #: 5

[\[All 312-50 Questions\]](#)

While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:

<script>alert(" Testing Testing Testing ")</script>

Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

- A. Buffer overflow
- B. Cross-site request forgery
- C. Distributed denial of service
- D. Cross-site scripting

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:10 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 23 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 23

Topic #: 5

[\[All 312-50 Questions\]](#)

The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

- A. An extensible security framework named COBIT
- B. A list of flaws and how to fix them
- C. Web application patches
- D. A security certification for hardened web applications

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:10 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 27 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 27

Topic #: 5

[\[All 312-50 Questions\]](#)

Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

- A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
- B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
- C. Hashing is faster compared to more traditional encryption algorithms.
- D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:10 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 28 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 28

Topic #: 5

[\[All 312-50 Questions\]](#)

Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?

- A. Poly key exchange
- B. Cross certification
- C. Poly key reference
- D. Cross-site exchange

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:10 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 29 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 29

Topic #: 5

[\[All 312-50 Questions\]](#)

Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

- A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
- B. The root CA stores the user's hash value for safekeeping.
- C. The CA is the trusted root that issues certificates.
- D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:10 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 30 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 30

Topic #: 5

[\[All 312-50 Questions\]](#)

A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

- A. Implementing server-side PKI certificates for all connections
- B. Mandating only client-side PKI certificates for all connections
- C. Requiring client and server PKI certificates for all connections
- D. Requiring strong authentication for all DNS queries

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:11 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 34 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 34

Topic #: 5

[\[All 312-50 Questions\]](#)

SOAP services use which technology to format information?

- A. SATA
- B. PCI
- C. XML
- D. ISDN

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:11 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 36 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 36

Topic #: 5

[\[All 312-50 Questions\]](#)

If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

- A. SDLC process
- B. Honey pot
- C. SQL injection
- D. Trap door

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:11 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 38 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 38

Topic #: 5

[\[All 312-50 Questions\]](#)

Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

- A. Ping of death
- B. SYN flooding
- C. TCP hijacking
- D. Smurf attack

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:11 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 39 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 39

Topic #: 5

[\[All 312-50 Questions\]](#)

Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

- A. Timing options to slow the speed that the port scan is conducted
- B. Fingerprinting to identify which operating systems are running on the network
- C. ICMP ping sweep to determine which hosts on the network are not available
- D. Traceroute to control the path of the packets sent during the scan

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:11 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 41 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 41

Topic #: 5

[\[All 312-50 Questions\]](#)

Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

- A. WebBugs
- B. WebGoat**
- C. VULN_HTML
- D. WebScarab

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:11 p.m.

Comments

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

EXAM 312-50 TOPIC 5 QUESTION 44 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 44

Topic #: 5

[\[All 312-50 Questions\]](#)

Which cipher encrypts the plain text digit (bit or byte) one by one?

- A. Classical cipher
- B. Block cipher
- C. Modern cipher
- D. Stream cipher

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:11 p.m.

Comments

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

EXAM 312-50 TOPIC 6 QUESTION 2 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 2

Topic #: 6

[\[All 312-50 Questions\]](#)

Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

- A. Regulatory compliance
- B. Peer review
- C. Change management
- D. Penetration testing

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:11 p.m.

Comments

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

EXAM 312-50 TOPIC 6 QUESTION 4 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 4

Topic #: 6

[\[All 312-50 Questions\]](#)

When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

- A. At least once a year and after any significant upgrade or modification
- B. At least once every three years or after any significant upgrade or modification
- C. At least twice a year or after any significant upgrade or modification
- D. At least once every two years and after any significant upgrade or modification

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:12 p.m.

Comments

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

EXAM 312-50 TOPIC 6 QUESTION 6 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 6

Topic #: 6

[\[All 312-50 Questions\]](#)

How can a policy help improve an employee's security awareness?

- A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security
- B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
- C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
- D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:12 p.m.

Comments

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

EXAM 312-50 TOPIC 7 QUESTION 6 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 6

Topic #: 7

[\[All 312-50 Questions\]](#)

A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

- A. Say no; the friend is not the owner of the account.
- B. Say yes; the friend needs help to gather evidence.
- C. Say yes; do the job for free.
- D. Say no; make sure that the friend knows the risk she's asking the CEH to take.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:12 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 1 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 1

Topic #: 8

[\[All 312-50 Questions\]](#)

It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.

Which of the following terms best matches the definition?

- A. Threat
- B. Attack
- C. Vulnerability
- D. Risk

[Hide Answer](#)

Suggested Answer: A

A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

References: [https://en.wikipedia.org/wiki/Threat_\(computer\)](https://en.wikipedia.org/wiki/Threat_(computer))

by [deleted] at April 4, 2025, 12:12 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 6 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 6

Topic #: 8

[\[All 312-50 Questions\]](#)

A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.

Which sort of trojan infects this server?

- A. Botnet Trojan
- B. Turtle Trojans
- C. Banking Trojans
- D. Ransomware Trojans

[Hide Answer](#)

Suggested Answer: A

In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. A coordinated DDoS attack by multiple botnet machines also resembles a zombie horde attack.

Incorrect Answers:

B: Turtle Trojans are about getting backdoor access to an intruder.

C: A Banker Trojan-horse (commonly called Banker Trojan) is a malicious program used in an attempt to obtain confidential information about customers and clients using online banking and payment systems.

D: Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan.

References: <https://en.wikipedia.org/wiki/Botnet>

by [deleted] at April 4, 2025, 12:13 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 8 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 8

Topic #: 8

[\[All 312-50 Questions\]](#)

It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again.

Which of the following terms best matches the definition?

- A. Ransomware
- B. Adware
- C. Spyware
- D. Riskware

[Hide Answer](#)

Suggested Answer: A

Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan.

References: <https://en.wikipedia.org/wiki/Ransomware>

by [deleted] at April 4, 2025, 12:13 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 14 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 14

Topic #: 8

[\[All 312-50 Questions\]](#)

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. Restrict Physical Access to Server Rooms hosting Critical Servers
- D. Use Static IP Address

[Hide Answer](#)

Suggested Answer: A

A way to protect your network traffic from being sniffed is to use encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption doesn't prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet's payload so that all the sniffer sees is encrypted gibberish.

References: <http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm>

by [deleted] at April 4, 2025, 12:13 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 21 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 21

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is a component of a risk assessment?

- A. Administrative safeguards
- B. Physical security
- C. DMZ
- D. Logical interface

[Hide Answer](#)

Suggested Answer: A

Risk assessment include:

- ⇒ The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.
- ⇒ The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

References: https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

by [deleted] at April 4, 2025, 12:14 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 24 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 24

Topic #: 8

[\[All 312-50 Questions\]](#)

Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability.

What is this style of attack called?

A. zero-day

B. zero-hour

C. zero-sum

D. no-day

[Hide Answer](#)

Suggested Answer: A

Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon. Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software.

References: <https://en.wikipedia.org/wiki/Stuxnet>

by [deleted] at April 4, 2025, 12:14 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 25 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 25

Topic #: 8

[\[All 312-50 Questions\]](#)

An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attackers database.

<iframe src="http://www.vulnweb.com/updateif.php" style="display:none"></iframe>

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

- A. Cross-Site Request Forgery
- B. Cross-Site Scripting
- C. SQL Injection
- D. Browser Hacking

[Hide Answer](#)

Suggested Answer: A

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Different HTTP request methods, such as GET and POST, have different level of susceptibility to CSRF attacks and require different levels of protection due to their different handling by web browsers.

References: https://en.wikipedia.org/wiki/Cross-site_request_forgery

by [deleted] at April 4, 2025, 12:14 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 46 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 46

Topic #: 8

[\[All 312-50 Questions\]](#)

`env x=`(){ :};echo exploit` bash -c 'cat /etc/passwd'`

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

- A. Display passwd content to prompt
- B. Removes the passwd file
- C. Changes all passwords in passwd
- D. Add new user to the passwd file

[Hide Answer](#)

Suggested Answer: A

To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:

`() {():}; /bin/cat /etc/passwd`

That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.

References: <https://blog.cloudflare.com/inside-shellshock/>

by [deleted] at April 4, 2025, 12:16 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 59 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 59

Topic #: 8

[\[All 312-50 Questions\]](#)

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.

What proxy tool will help you find web vulnerabilities?

- A. Burpsuite
- B. Maskgen
- C. Dimitry
- D. Proxychains

[Hide Answer](#)

Suggested Answer: A

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

References: <https://portswigger.net/burp/>

by [deleted] at April 4, 2025, 12:17 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 60 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 60

Topic #: 8

[\[All 312-50 Questions\]](#)

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.dstport==514 && ip.dst==192.168.0.150`
- B. `tcp.srcport==514 && ip.src==192.168.0.99`
- C. `tcp.dstport==514 && ip.dst==192.168.0.0/16`
- D. `tcp.srcport==514 && ip.src==192.168.150`

[Hide Answer](#)

Suggested Answer: A

We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.

References: <https://wiki.wireshark.org/DisplayFilters>

by [deleted] at April 4, 2025, 12:17 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 63 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 63

Topic #: 8

[\[All 312-50 Questions\]](#)

What is the process of logging, recording, and resolving events that take place in an organization?

A. Incident Management Process

B. Security Policy

C. Internal Procedure

D. Metrics

[Hide Answer](#)

Suggested Answer: A

The activities within the incident management process include:

- ⇒ Incident detection and recording
- ⇒ Classification and initial support
- ⇒ Investigation and analysis
- ⇒ Resolution and record
- ⇒ Incident closure
- ⇒ Incident ownership, monitoring, tracking and communication
- ⇒ Establish incident framework management
- ⇒ Evaluation of incident framework management

References: [https://en.wikipedia.org/wiki/Incident_management_\(ITSM\)#Incident_management_procedure](https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure)

by [deleted] at April 4, 2025, 12:17 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 73 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 73

Topic #: 8

[\[All 312-50 Questions\]](#)

The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

- A. Wireless Intrusion Prevention System
- B. Wireless Access Point
- C. Wireless Access Control List
- D. Wireless Analyzer

[Hide Answer](#)

Suggested Answer: A

A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

References: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

by [deleted] at April 4, 2025, 12:18 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 75 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 75

Topic #: 8

[\[All 312-50 Questions\]](#)

You are using NMAP to resolve domain names into IP addresses for a ping sweep later.

Which of the following commands looks for IP addresses?

- A. >host -t a hackeddomain.com
- B. >host -t soa hackeddomain.com
- C. >host -t ns hackeddomain.com
- D. >host -t AXFR hackeddomain.com

[Hide Answer](#)

Suggested Answer: A

The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.

References: https://en.wikipedia.org/wiki/List_of_DNS_record_types

by [deleted] at April 4, 2025, 12:18 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 76 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 76

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

- A. tcpdump
- B. nessus
- C. etherea
- D. Jack the ripper

[Hide Answer](#)

Suggested Answer: A

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>

by [deleted] at April 4, 2025, 12:18 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 78 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 78

Topic #: 8

[\[All 312-50 Questions\]](#)

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

A. unicode characters

B. spyware

C. port knocking

D. subnetting

[Hide Answer](#)

Suggested Answer: A

Unicode attacks can be effective against applications that understand it. Unicode is the international standard whose goal is to represent every character needed by every written human language as a single integer number. What is known as Unicode evasion should more correctly be referenced as UTF-8 evasion. Unicode characters are normally represented with two bytes, but this is impractical in real life.

One aspect of UTF-8 encoding causes problems: non-Unicode characters can be represented encoded. What is worse is multiple representations of each character can exist. Non-Unicode character encodings are known as overlong characters, and may be signs of attempted attack.

References: <http://books.gigatux.nl/mirror/apacheseecurity/0596007248/apachesc-chp-10-sect-8.html>

by [deleted] at April 4, 2025, 12:18 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 79 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 79

Topic #: 8

[\[All 312-50 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: A

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates[1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

References: https://en.wikipedia.org/wiki/Public_key_infrastructure

by [deleted] at April 4, 2025, 12:18 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 83 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 83

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is the greatest threat posed by backups?

- A. A backup is the source of Malware or illicit information.
- B. A backup is unavailable during disaster recovery.
- C. A backup is incomplete because no verification was performed.
- D. An un-encrypted backup can be misplaced or stolen.

[Hide Answer](#)

Suggested Answer: *D*

If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.

References: <http://resources.infosecinstitute.com/backup-media-encryption/>

by [deleted] at April 4, 2025, 12:19 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 88 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 88

Topic #: 8

[\[All 312-50 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: A

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Example and characteristics -

If an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.

Incorrect Answers:

C: Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.

References: https://en.wikipedia.org/wiki/Cross-site_request_forgery

by [deleted] at April 4, 2025, 12:19 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 92 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 92

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

- A. Validate and escape all information sent to a server
- B. Use security policies and procedures to define and implement proper security settings
- C. Verify access right before allowing access to protected information and UI controls
- D. Use digital certificates to authenticate a server prior to sending data

[Hide Answer](#)

Suggested Answer: A

Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.

References: https://en.wikipedia.org/wiki/Cross-site_scripting#Contextual_output_encoding.2Fescaping_of_string_input

by [deleted] at April 4, 2025, 12:19 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 95 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 95

Topic #: 8

[\[All 312-50 Questions\]](#)

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. Intrusion Prevention System (IPS)
- C. Network sniffer
- D. Vulnerability scanner

[Hide Answer](#)

Suggested Answer: A

A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.

References: https://en.wikipedia.org/wiki/Packet_analyzer

by [deleted] at April 4, 2025, 12:19 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 97 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 97

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is a protocol specifically designed for transporting event messages?

A. SYSLOG

B. SMS

C. SNMP

D. ICMP

[Hide Answer](#)

Suggested Answer: A

syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

References: https://en.wikipedia.org/wiki/Syslog#Network_protocol

by [deleted] at April 4, 2025, 12:19 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 98 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 98

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following security operations is used for determining the attack surface of an organization?

- A. Running a network scan to detect network services in the corporate DMZ
- B. Training employees on the security policy regarding social engineering
- C. Reviewing the need for a security clearance for each employee
- D. Using configuration management to determine when and where to apply security patches

[Hide Answer](#)

Suggested Answer: A

For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.

References: <http://meisecurity.com/home/consulting/consulting-network-scanning/>

by [deleted] at April 4, 2025, 12:20 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 100 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 100

Topic #: 8

[\[All 312-50 Questions\]](#)

The "black box testing" methodology enforces which kind of restriction?

- A. Only the external operation of a system is accessible to the tester.
- B. Only the internal operation of a system is known to the tester.
- C. The internal operation of a system is only partly accessible to the tester.
- D. The internal operation of a system is completely known to the tester.

[Hide Answer](#)

Suggested Answer: A

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.

References: https://en.wikipedia.org/wiki/Black-box_testing

by [deleted] at April 4, 2025, 12:20 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 101 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 101

Topic #: 8

[\[All 312-50 Questions\]](#)

The "gray box testing" methodology enforces what kind of restriction?

- A. The internal operation of a system is only partly accessible to the tester.
- B. The internal operation of a system is completely known to the tester.
- C. Only the external operation of a system is accessible to the tester.
- D. Only the internal operation of a system is known to the tester.

[Hide Answer](#)

Suggested Answer: A

A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.

References: https://en.wikipedia.org/wiki/Gray_box_testing

by [deleted] at April 4, 2025, 12:20 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 102 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 102

Topic #: 8

[\[All 312-50 Questions\]](#)

The "white box testing" methodology enforces what kind of restriction?

- A. The internal operation of a system is completely known to the tester.
- B. Only the external operation of a system is 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 only partly accessible to the tester.

[Hide Answer](#)

Suggested Answer: A

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.

References: https://en.wikipedia.org/wiki/White-box_testing

by [deleted] at April 4, 2025, 12:20 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 103 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 103

Topic #: 8

[\[All 312-50 Questions\]](#)

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. Fuzzing
- B. Randomizing
- C. Mutating
- D. Bounding

[Hide Answer](#)

Suggested Answer: A

Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

References: https://en.wikipedia.org/wiki/Fuzz_testing

by [deleted] at April 4, 2025, 12:20 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 104 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 104

Topic #: 8

[\[All 312-50 Questions\]](#)

To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

- A. Vulnerability scanner
- B. Protocol analyzer
- C. Port scanner
- D. Intrusion Detection System

[Hide Answer](#)

Suggested Answer: A

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses. They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.

References: https://en.wikipedia.org/wiki/Vulnerability_scanner

by [deleted] at April 4, 2025, 12:20 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 108 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 108

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System

B. Firewall

C. Proxy

D. Router

[Hide Answer](#)

Suggested Answer: A

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.

References: https://en.wikipedia.org/wiki/Intrusion_detection_system

by [deleted] at April 4, 2025, 12:20 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 109 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 109

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is a low-tech way of gaining unauthorized access to systems?

- A. Social Engineering
- B. Sniffing
- C. Eavesdropping
- D. Scanning

[Hide Answer](#)

Suggested Answer: A

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))

by [deleted] at April 4, 2025, 12:20 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 110 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 110

Topic #: 8

[\[All 312-50 Questions\]](#)

PGP, SSL, and IKE are all examples of which type of cryptography?

- A. Public Key
- B. Secret Key
- C. Hash Algorithm
- D. Digest

[Hide Answer](#)

Suggested Answer: A

Public-key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as

Secure Sockets Layer (SSL), Transport Layer Security (TLS), S/MIME, PGP, Internet Key Exchange (IKE or IKEv2), and GPG.

References: https://en.wikipedia.org/wiki/Public-key_cryptography

by [deleted] at April 4, 2025, 12:21 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 111 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 111

Topic #: 8

[\[All 312-50 Questions\]](#)

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

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

[Hide Answer](#)

Suggested Answer: A

Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.

References: https://en.wikipedia.org/wiki/Password_cracking

by [deleted] at April 4, 2025, 12:21 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 116 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 116

Topic #: 8

[\[All 312-50 Questions\]](#)

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. Whisker

B. tcpsplice

C. Burp

D. Hydra

[Hide Answer](#)

Suggested Answer: A

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

by [deleted] at April 4, 2025, 12:21 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 129 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 129

Topic #: 8

[\[All 312-50 Questions\]](#)

If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

- A. Civil
- B. International
- C. Criminal
- D. Common

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:22 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 130 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 130

Topic #: 8

[\[All 312-50 Questions\]](#)

What is the role of test automation in security testing?

- A. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.
- B. It is an option but it tends to be very expensive.
- C. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
- D. Test automation is not usable in security due to the complexity of the tests.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:22 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 136 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 136

Topic #: 8

[\[All 312-50 Questions\]](#)

Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

- A. Internal Whitebox
- B. External, Whitebox
- C. Internal, Blackbox
- D. External, Blackbox

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:22 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 142 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 142

Topic #: 8

[\[All 312-50 Questions\]](#)

A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

- A. Ignore it.
- B. Try to sell the information to a well-paying party on the dark web.
- C. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
- D. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:23 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 161 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 161

Topic #: 8

[\[All 312-50 Questions\]](#)

What is the correct process for the TCP three-way handshake connection establishment and connection termination?

- A. Connection Establishment: FIN, ACK-FIN, ACK Connection Termination: SYN, SYN-ACK, ACK
- B. Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: ACK, ACK-SYN, SYN
- C. Connection Establishment: ACK, ACK-SYN, SYN Connection Termination: FIN, ACK-FIN, ACK
- D. Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: FIN, ACK-FIN, ACK

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:24 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 165 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 165

Topic #: 8

[\[All 312-50 Questions\]](#)

Which protocol is used for setting up secured channels between two devices, typically in VPNs?

- A. IPSEC
- B. PEM
- C. SET
- D. PPP

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:24 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 167 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 167

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following Nmap commands will produce the following output?

Output:

```
Starting Nmap 6.47 (http://nmap.org ) at 2015-05-26 12:50 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).
Not shown: 65530 open|filtered ports, 65529 filtered ports
PORT      STATE SERVICE
111/tcp    open  rpcbind
999/tcp    open  garcon
1017/tcp   open  unknown
1021/tcp   open  expl
1023/tcp   open  netvenuechat
2049/tcp   open  nfs
17501/tcp  open  unknown
111/udp   open  rpcbind
123/udp   open  ntp
137/udp   open  netbios-ns
2049/udp  open  nfs
5353/udp  open  zeroconf
17501/udp open|filtered unknown
51857/udp open|filtered unknown
54358/udp open|filtered unknown
56228/udp open|filtered unknown
57598/udp open|filtered unknown
59488/udp open|filtered unknown
60027/udp open|filtered unknown
```

- A. nmap -sN -Ps -T4 192.168.1.1
- B. nmap -sT -sX -Pn -p 1-65535 192.168.1.1
- C. nmap -sS -Pn 192.168.1.1
- D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:24 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 168 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 168

Topic #: 8

[\[All 312-50 Questions\]](#)

Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

- A. msfpayload
- B. msfcli
- C. msfencode
- D. msfd

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:24 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 180 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 180

Topic #: 8

[\[All 312-50 Questions\]](#)

What is not a PCI compliance recommendation?

- A. Limit access to card holder data to as few individuals as possible.
- 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. Use a firewall between the public network and the payment card data.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:25 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 181 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 181

Topic #: 8

[\[All 312-50 Questions\]](#)

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

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

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:25 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 185 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 185

Topic #: 8

[\[All 312-50 Questions\]](#)

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

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

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:26 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 189 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 189

Topic #: 8

[\[All 312-50 Questions\]](#)

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 probably a legitimate message as it comes from a respectable organization.
- B. Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.
- C. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
- D. This is a scam because Bob does not know Scott.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:26 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 191 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 191

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following will perform an Xmas scan using NMAP?

- A. nmap -sA 192.168.1.254
- B. nmap -sP 192.168.1.254
- C. nmap -sX 192.168.1.254
- D. nmap -sV 192.168.1.254

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:26 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 192 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 192

Topic #: 8

[\[All 312-50 Questions\]](#)

As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in

Wireshark will help you to find this kind of traffic?

- A. request smtp 25
- B. tcp.port eq 25
- C. smtp port
- D. tcp.contains port 25

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:26 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 201 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 201

Topic #: 8

[\[All 312-50 Questions\]](#)

Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?

- A. Windows
- B. Unix
- C. Linux
- D. OS X

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:27 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 203 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 203

Topic #: 8

[\[All 312-50 Questions\]](#)

It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

- A. Containment
- B. Eradication
- C. Recovery
- D. Discovery

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:27 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 206 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 206

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following 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.

- A. Heartbleed Bug
- B. POODLE
- C. SSL/TLS Renegotiation Vulnerability
- D. Shellshock

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:27 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 226 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 226

Topic #: 8

[\[All 312-50 Questions\]](#)

What kind of risk will remain even if all theoretically possible safety measures would be applied?

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

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:29 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 230 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 230

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?

- A. Metasploit
- B. Wireshark
- C. Maltego
- D. Cain & Abel

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:29 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 231 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 231

Topic #: 8

[\[All 312-50 Questions\]](#)

If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?

- A. Running a network scan to detect network services in the corporate DMZ
- B. Reviewing the need for a security clearance for each employee
- C. Using configuration management to determine when and where to apply security patches
- D. Training employees on the security policy regarding social engineering

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:29 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 235 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 235

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is NOT an ideal choice for biometric controls?

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

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:29 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 236 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 236

Topic #: 8

[\[All 312-50 Questions\]](#)

While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

- A. Immediately stop work and contact the proper legal authorities
- B. Ignore the data and continue the assessment until completed as agreed
- C. Confront the client in a respectful manner and ask her about the data
- D. Copy the data to removable media and keep it in case you need it

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:29 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 238 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 238

Topic #: 8

[\[All 312-50 Questions\]](#)

Suppose you've gained access to your client's hybrid network. On which port should you listen to in order to know which Microsoft Windows workstations have file sharing enabled?

- A. 1433
- B. 161
- C. 445
- D. 3389

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:29 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 240 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 240

Topic #: 8

[\[All 312-50 Questions\]](#)

What is the term coined for logging, recording and resolving events in a company?

- A. Internal Procedure
- B. Security Policy
- C. Incident Management Process
- D. Metrics

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:30 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 242 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 242

Topic #: 8

[\[All 312-50 Questions\]](#)

A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails. What type of Trojan did the hacker use?

- A. Turtle Trojans
- B. Ransomware Trojans
- C. Botnet Trojan
- D. Banking Trojans

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:30 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 247 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 247

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

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

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:30 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 252 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 252

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is the BEST approach to prevent Cross-site Scripting (XSS) flaws?

- A. Use digital certificates to authenticate a server prior to sending data.
- B. Verify access right before allowing access to protected information and UI controls.
- C. Verify access right before allowing access to protected information and UI controls.
- D. Validate and escape all information sent to a server.

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:31 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 257 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 257

Topic #: 8

[\[All 312-50 Questions\]](#)

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

- A. SOA
- B. Single-Sign On
- C. PKI
- D. Biometrics

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:31 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 259 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 259

Topic #: 8

[\[All 312-50 Questions\]](#)

What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

- A. c:\compmgmt.msc
- B. c:\gpedit
- C. c:\ncpa.cpl
- D. c:\services.msc

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:31 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 262 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 262

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is a restriction being enforced in "white box testing?"

- A. Only the internal operation of a system is known to the tester
- B. The internal operation of a system is completely known to the tester**
- C. The internal operation of a system is only partly accessible to the tester
- D. Only the external operation of a system is accessible to the tester

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:31 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 264 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 264

Topic #: 8

[\[All 312-50 Questions\]](#)

When security and confidentiality of data within the same LAN is of utmost priority, which IPSec mode should you implement?

- A. AH Tunnel mode
- B. AH promiscuous
- C. ESP transport mode
- D. ESP confidential

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:32 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 270 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 270

Topic #: 8

[\[All 312-50 Questions\]](#)

A recent security audit revealed that there were indeed several occasions that the company's network was breached. After investigating, you discover that your

IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

- A. True Positive
- B. False Negative
- C. False Positive
- D. False Positive

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:32 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 272 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 272

Topic #: 8

[\[All 312-50 Questions\]](#)

What does a type 3 code 13 represent? (Choose two.)

- A. Echo request
- B. Destination unreachable
- C. Network unreachable
- D. Administratively prohibited
- E. Port unreachable
- F. Time exceeded

[Hide Answer](#)

Suggested Answer: BD

by [deleted] at April 4, 2025, 12:32 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 273 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 273

Topic #: 8

[\[All 312-50 Questions\]](#)

Destination unreachable administratively prohibited messages can inform the hacker to what?

- A. That a circuit level proxy has been installed and is filtering traffic
- B. That his/her scans are being blocked by a honeypot or jail
- C. That the packets are being malformed by the scanning software
- D. That a router or other packet-filtering device is blocking traffic
- E. That the network is functioning normally

[Hide Answer](#)

Suggested Answer: *D*

by [deleted] at April 4, 2025, 12:32 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 280 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 280

Topic #: 8

[\[All 312-50 Questions\]](#)

You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

- A. The zombie you are using is not truly idle.
- B. A stateful inspection firewall is resetting your queries.
- C. Hping2 cannot be used for idle scanning.
- D. These ports are actually open on the target system.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:32 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 281 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 281

Topic #: 8

[\[All 312-50 Questions\]](#)

While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor.

How can you modify your scan to prevent triggering this event in the IDS?

- A. Scan more slowly.
- B. Do not scan the broadcast IP.
- C. Spoof the source IP address.
- D. Only scan the Windows systems.

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:33 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 285 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 285

Topic #: 8

[\[All 312-50 Questions\]](#)

A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites.

77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

- A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
- B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
- C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
- D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:33 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 287 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 287

Topic #: 8

[\[All 312-50 Questions\]](#)

You have initiated an active operating system fingerprinting attempt with nmap against a target system:

```
[root@ceh NG]# /usr/local/bin/nmap -ST -O 10.0.0.1
Starting nmap 3.28 ( www.insecure.org/nmap/ ) at 2003-06-18 19:14 IDT
Interesting ports on 10.0.0.1:
(The 1628 ports scanned but not shown below are in state: closed)
```

```
Port      State  Service
21/tcp    filtered  ftp
22/tcp    filtered  ssh
25/tcp    open   smtp
80/tcp    open   http
135/tcp   open   loc-srv
139/tcp   open   netbios-ssn
389/tcp   open   LDAP
443/tcp   open   https
465/tcp   open   smtps
1029/tcp  open   ms-lsa
1433/tcp  open   ms-sql-s
2301/tcp  open   compaqdiag
5555/tcp  open   freeciv
5800/tcp  open   vnc-http
5900/tcp  open   vnc
6000/tcp  filtered X11
```

Remote operating system guess: Windows XP, Windows 2000, NT4 or 95/98/98SE Nmap
run completed -- 1 IP address (1 host up) scanned in 3.334 seconds

Using its fingerprinting tests nmap is unable to distinguish between different groups of Microsoft based operating systems - Windows XP, Windows 2000, NT4 or 95/98/98SE.

What operating system is the target host running based on the open ports shown above?

- A. Windows XP
- B. Windows 98 SE
- C. Windows NT4 Server
- D. Windows 2000 Server

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:33 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 289 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 289

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following command line switch would you use for OS detection in Nmap?

- A. -D
- B. -O**
- C. -P
- D. -X

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:33 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 292 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 292

Topic #: 8

[\[All 312-50 Questions\]](#)

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test.

While conducting a port scan she notices open ports in the range of 135 to 139.

What protocol is most likely to be listening on those ports?

- A. Finger
- B. FTP
- C. Samba
- D. SMB

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:33 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 297 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 297

Topic #: 8

[\[All 312-50 Questions\]](#)

What is the following command used for?

net use \targetipc\$ "" /u:""

- A. Grabbing the etc/passwd file
- B. Grabbing the SAM
- C. Connecting to a Linux computer through Samba.
- D. This command is used to connect as a null session
- E. Enumeration of Cisco routers

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:34 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 298 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 298

Topic #: 8

[\[All 312-50 Questions\]](#)

What is the proper response for a NULL scan if the port is closed?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST**
- F. No response

[Hide Answer](#)

Suggested Answer: E

by [deleted] at April 4, 2025, 12:34 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 309 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 309

Topic #: 8

[\[All 312-50 Questions\]](#)

Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.

What do you think Tess King is trying to accomplish? Select the best answer.

- A. A zone harvesting
- B. A zone transfer**
- C. A zone update
- D. A zone estimate

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:34 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 310 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 310

Topic #: 8

[\[All 312-50 Questions\]](#)

A zone file consists of which of the following Resource Records (RRs)?

- A. DNS, NS, AXFR, and MX records
- B. DNS, NS, PTR, and MX records
- C. SOA, NS, AXFR, and MX records
- D. SOA, NS, A, and MX records

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:34 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 314 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 314

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds

B. USER2SID

C. Cheops

D. SID2USER

E. DumpSec

[Hide Answer](#)

Suggested Answer: *BDE*

by [deleted] at April 4, 2025, 12:34 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 318 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 318

Topic #: 8

[\[All 312-50 Questions\]](#)

Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?

- A. Interceptor
- B. Man-in-the-middle**
- C. ARP Proxy
- D. Poisoning Attack

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:35 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 329 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 329

Topic #: 8

[\[All 312-50 Questions\]](#)

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

- A. SNMPUtil
- B. SNScan
- C. SNMPScan
- D. Solarwinds IP Network Browser
- E. NMap

[Hide Answer](#)

Suggested Answer: ABD

by [deleted] at April 4, 2025, 12:36 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 331 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 331

Topic #: 8

[\[All 312-50 Questions\]](#)

Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers. Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

- A. Hardware, Software, and Sniffing.
- B. Hardware and Software Keyloggers.
- C. Passwords are always best obtained using Hardware key loggers.
- D. Software only, they are the most effective.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:36 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 342 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 342

Topic #: 8

[\[All 312-50 Questions\]](#)

_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

- A. Trojan
- B. RootKit**
- C. DoS tool
- D. Scanner
- E. Backdoor

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:36 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 346 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 346

Topic #: 8

[\[All 312-50 Questions\]](#)

When discussing passwords, what is considered a brute force attack?

- A. You attempt every single possibility until you exhaust all possible combinations or discover the password
- B. You threaten to use the rubber hose on someone unless they reveal their password
- C. You load a dictionary of words into your cracking program
- D. You create hashes of a large number of words and compare it with the encrypted passwords
- E. You wait until the password expires

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:37 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 355 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 355

Topic #: 8

[\[All 312-50 Questions\]](#)

In the context of Windows Security, what is a 'null' user?

- A. A user that has no skills
- B. An account that has been suspended by the admin
- C. A pseudo account that has no username and password
- D. A pseudo account that was created for security administration purpose

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:37 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 357 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 357

Topic #: 8

[\[All 312-50 Questions\]](#)

What hacking attack is challenge/response authentication used to prevent?

- A. Replay attacks
- B. Scanning attacks
- C. Session hijacking attacks
- D. Password cracking attacks

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:37 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 371 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 371

Topic #: 8

[\[All 312-50 Questions\]](#)

In Trojan terminology, what is a covert channel?



- A. A channel that transfers information within a computer system or network in a way that violates the security policy
- B. A legitimate communication path within a computer system or network for transfer of data
- C. It is a kernel operation that hides boot processes and services to mask detection
- D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:38 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 376 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 376

Topic #: 8

[\[All 312-50 Questions\]](#)

Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?  
template=%2e%2e%2f%2e%2e%2f%2e%2f%65%74%63%2f%70%61%73%73%77%64  
This request is made up of:  
%2e%2e%2f%2e%2f%2e%2f = ../ .. / ..  
%65%74%63 = etc  
%2f = /  
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

- A. Configure the Web Server to deny requests involving "hex encoded" characters
- B. Create rules in IDS to alert on strange Unicode requests**
- C. Use SSL authentication on Web Servers
- D. Enable Active Scripts Detection at the firewall and routers

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:39 p.m.

Comments

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

EXAM 312-50 TOPIC 8 QUESTION 377 DISCUSSION

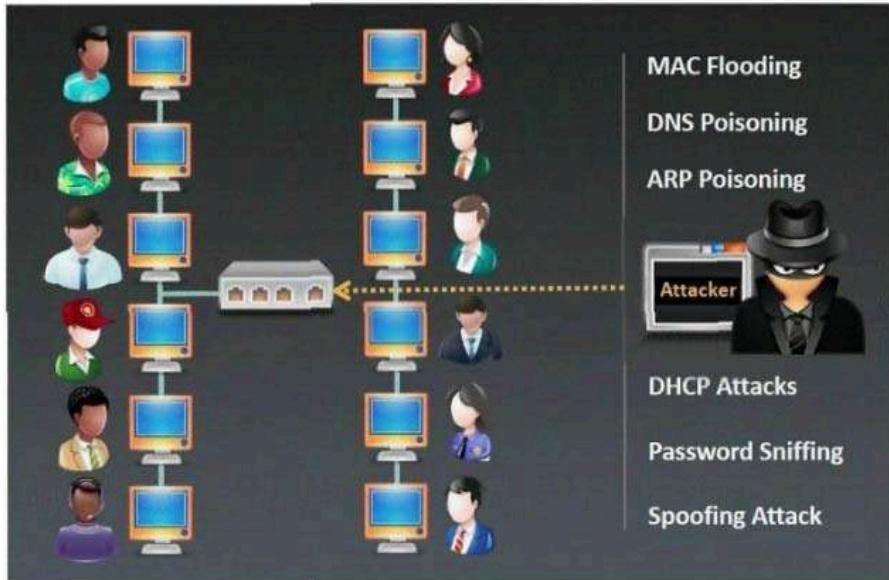
Actual exam question from ECCouncil's 312-50

Question #: 377

Topic #: 8

[\[All 312-50 Questions\]](#)

Which type of sniffing technique is generally referred as MiTM attack?



- A. Password Sniffing
- B. ARP Poisoning
- C. Mac Flooding
- D. DHCP Sniffing

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:39 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 17 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 17

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:41 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 32 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 32

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which Intrusion Detection System is the 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)

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:41 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 39 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 39

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:42 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 40 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 40

Topic #: 1

[\[All 312-50v10 Questions\]](#)

The "white box testing" methodology enforces what kind of restriction?

- A. Only the internal operation of a system is known to the tester.
- B. The internal operation of a system is completely known to the tester.
- C. The internal operation of a system is only partly accessible to the tester.
- D. Only the external operation of a system is accessible to the tester.

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:42 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 43 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 43

Topic #: 1

[\[All 312-50v10 Questions\]](#)

The following is part of a log file taken from the machine on the network with the IP address of 192.168.0.110:

Time:June 16 17:30:15 Port:20 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:17 Port:21 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:19 Port:22 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:21 Port:23 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:22 Port:25 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:23 Port:80 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:30 Port:443 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP

What type of activity has been logged?

- A. Teardrop attack targeting 192.168.0.110
- B. Denial of service attack targeting 192.168.0.105
- C. Port scan targeting 192.168.0.110
- D. Port scan targeting 192.168.0.105

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:42 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 47 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 47

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:42 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 49 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 49

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which of the following will perform an Xmas scan using NMAP?

- A. nmap -sA 192.168.1.254
- B. nmap -sP 192.168.1.254
- C. nmap -sX 192.168.1.254
- D. nmap -sV 192.168.1.254

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:42 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 57 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 57

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which of the following attacks exploits web age vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend?

- A. Command Injection Attacks
- B. File Injection Attack
- C. Cross-Site Request Forgery (CSRF)
- D. Hidden Field Manipulation Attack

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:42 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 58 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 58

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

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

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:42 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 60 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 60

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?

- A. None of these scenarios compromise the privacy of Alice's data
- B. Agent Andrew subpoenas Alice, forcing her to reveal her private key. However, the cloud server successfully resists Andrew's attempt to access the stored data
- C. Hacker Harry breaks into the cloud server and steals the encrypted data
- D. Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:42 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 79 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 79

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which of the following provides a security professional with most information about the system's security posture?

- A. Wardriving, warchalking, social engineering
- B. Social engineering, company site browsing, tailgating
- C. Phishing, spamming, sending trojans
- D. Port scanning, banner grabbing, service identification

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:43 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 107 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 107

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:43 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 117 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 117

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:44 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 118 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 118

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Sam is working as a pen-tester in an organization in Houston. He performs penetration testing on IDS in order to find the different ways an attacker uses to evade the IDS. Sam sends a large amount of packets to the target IDS that generates alerts, which enable Sam to hide the real traffic. What type of method is Sam using to evade IDS?

- A. Denial-of-Service
- B. False Positive Generation**
- C. Insertion Attack
- D. Obfuscating

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:44 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 124 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 124

Topic #: 1

[\[All 312-50v10 Questions\]](#)

How does the Address Resolution Protocol (ARP) work?

- A. It sends a request packet to all the network elements, asking for the domain name from a specific IP.
- B. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
- C. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
- D. It sends a reply packet for a specific IP, asking for the MAC address.

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:44 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 125 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 125

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. AH promiscuous
- B. ESP confidential
- C. AH Tunnel mode
- D. ESP transport mode

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:44 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 126 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 126

Topic #: 1

[\[All 312-50v10 Questions\]](#)

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

- A. Black-box
- B. Announced
- C. White-box
- D. Grey-box

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:44 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 129 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 129

Topic #: 1

[\[All 312-50v10 Questions\]](#)

If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

- A. Common
- B. Criminal
- C. Civil
- D. International

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:44 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 130 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 130

Topic #: 1

[\[All 312-50v10 Questions\]](#)

The company ABC recently contract 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. What is 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

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:44 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 133 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 133

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

TCP port 21 "" no response -

TCP port 22 "" no response -

TCP port 23 "" Time-to-live exceeded

- A. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
- B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
- C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall
- D. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:44 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 137 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 137

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:45 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 149 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 149

Topic #: 1

[\[All 312-50v10 Questions\]](#)

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.

What proxy tool will help you find web vulnerabilities?

- A. Burpsuite
- B. Maskgen
- C. Dimitry
- D. Proxychains

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:45 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 154 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 154

Topic #: 1

[\[All 312-50v10 Questions\]](#)

You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless.

When you verify the configuration of this Windows system you find two static routes. route add 10.0.0.0 mask 255.0.0.0 10.0.0.1 route add 0.0.0.0 mask 255.0.0.0 199.168.0.1

What is the main purpose of those static routes?

- A. Both static routes indicate that the traffic is external with different gateway.
- B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
- C. Both static routes indicate that the traffic is internal with different gateway.
- D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:45 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 158 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 158

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

- A. Application Layer
- B. Data tier
- C. Presentation tier
- D. Logic tier

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:45 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 159 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 159

Topic #: 1

[\[All 312-50v10 Questions\]](#)

An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors

24 hours. What is the best option to do this job?

- A. Use fences in the entrance doors.
- B. Install a CCTV with cameras pointing to the entrance doors and the street.
- C. Use an IDS in the entrance doors and install some of them near the corners.
- D. Use lights in all the entrance doors and along the company's perimeter.

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:45 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 173 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 173

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:46 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 180 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 180

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

- A. Nessus
- B. Metasploit**
- C. Maltego
- D. Wireshark

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:46 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 184 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 184

Topic #: 1

[\[All 312-50v10 Questions\]](#)

In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

- A. Both pharming and phishing attacks are identical.
- B. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS.
In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
- C. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS.
In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
- D. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:46 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 186 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 186

Topic #: 1

[\[All 312-50v10 Questions\]](#)

A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.

Which sort of trojan infects this server?

- A. Botnet Trojan
- B. Turtle Trojans
- C. Banking Trojans
- D. Ransomware Trojans

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:46 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 187 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 187

Topic #: 1

[\[All 312-50v10 Questions\]](#)

In order to have an anonymous Internet surf, which of the following is best choice?

- A. Use SSL sites when entering personal information
- B. Use Tor network with multi-node
- C. Use shared WiFi
- D. Use public VPN

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:46 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 188 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 188

Topic #: 1

[\[All 312-50v10 Questions\]](#)

In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.

Example:

allintitle: root passwd

- A. Maintaining Access
- B. Gaining Access
- C. Reconnaissance
- D. Scanning and Enumeration

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:46 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 192 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 192

Topic #: 1

[\[All 312-50v10 Questions\]](#)

In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?

- A. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
- B. Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.
- C. A blacklist of companies that have their mail server relays configured to be wide open.
- D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:46 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 193 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 193

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Emil uses nmap to scan two hosts using this command:

```
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
```

He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
53/tcp open  domain
80/tcp open  http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

```
Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

What is his conclusion?

- A. Host 192.168.99.7 is an iPad.
- B. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7
- C. Host 192.168.99.1 is the host that he launched the scan from.
- D. Host 192.168.99.7 is down.

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:46 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 200 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 200

Topic #: 1

[\[All 312-50v10 Questions\]](#)

```
#!/usr/bin/python
import socket
buffer=[“A”]
counter=50
while len(buffer) <=100:
    buffer.append(“A”*counter)
    counter=counter+50
com-
mands=[“HELP”, “STATS”, “RTIME”, “LTIME”, “:SRUN”, “:TRUN”, “:GMON”, “:GDOG”, “:KSTET”, “:GTER”, “:HTER”, “:LTER”, “:KSTAN”]
for command in commands:
    for buffstring in buffer:
        print “Exploiting” +command +”.”+str(len(buffstring))
        s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
        s.connect((“127.0.0.1”,9999))
        s.recv(50)
        s.send(command+buffstring)
        s.close()
```

What is the code written for?

- A. Buffer Overflow
- B. Encryption
- C. Denial-of-service (DoS)
- D. Brute-force

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:47 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 202 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 202

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:47 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 207 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 207

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file named "Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt". In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.

What type of malware has Jesse encountered?

- A. Worm
- B. Macro Virus
- C. Key-Logger
- D. Trojan

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:47 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 214 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 214

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:47 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 215 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 215

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

```
[eve@localhost ~]$ john secret.txt
Loaded 2 password hashes with no different salts (LM[DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO... SAMPLUI
0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4
0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837
0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 15917KC/s SHAGRN..SHENY9
```

What is she trying to achieve?

- A. She is using ftp to transfer the file to another hacker named John.
- B. She is using John the Ripper to crack the passwords in the secret.txt file**
- C. She is encrypting the file.
- D. She is using John the Ripper to view the contents of the file.

[Hide Answer](#)

Suggested Answer: B

by [deleted] at April 4, 2025, 12:47 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 216 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 216

Topic #: 1

[\[All 312-50v10 Questions\]](#)

What is the correct process for the TCP three-way handshake connection establishment and connection termination?

- A. Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: FIN, ACK-FIN, ACK
- B. Connection Establishment: ACK, ACK-SYN, SYN Connection Termination: FIN, ACK-FIN, ACK
- C. Connection Establishment: FIN, ACK-FIN, ACK Connection Termination: SYN, SYN-ACK, ACK
- D. Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: ACK, ACK-SYN, SYN

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:47 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 217 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 217

Topic #: 1

[\[All 312-50v10 Questions\]](#)

```
env x='(){ :};echo exploit' bash ""c ""~cat/etc/passwd'
```

What is the Shellshock bash vulnerability attempting to do 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

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:47 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 231 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 231

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

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

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:48 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 232 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 232

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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 reflects the changes.

Which type of vulnerability is present on this site?

A. Cookie Tampering

B. SQL Injection

C. Web Parameter Tampering

D. XSS Reflection

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:48 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 239 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 239

Topic #: 1

[\[All 312-50v10 Questions\]](#)

When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it. What should you do?

- A. Forward the message to your company's security response team and permanently delete the message from your computer.
- B. Reply to the sender and ask them for more information about the message contents.
- C. Delete the email and pretend nothing happened.
- D. Forward the message to your supervisor and ask for her opinion on how to handle the situation.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:48 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 240 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 240

Topic #: 1

[\[All 312-50v10 Questions\]](#)

The "Gray-box testing" methodology enforces what kind of restriction?

- A. Only the internal operation of a system is known to the tester.
- B. The internal operation of a system is completely known to the tester.
- C. The internal operation of a system is only partly accessible to the tester.**
- D. Only the external operation of a system is accessible to the tester.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:48 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 262 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 262

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: -Verifies success or failure of an attack "" Monitors system activities "" Detects attacks that a network-based IDS fails to detect. "" Near real-time detection and response ""

Does not require additional hardware "" Lower entry cost. Which type of IDS is best suited for Tremp's requirements?

- A. Network-based IDS
- B. Open source-based IDS
- C. Host-based IDS
- D. Gateway-based IDS

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:49 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 268 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 268

Topic #: 1

[\[All 312-50v10 Questions\]](#)

During the security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

- A. Create a procedures document
- B. Terminate the audit
- C. Conduct compliance testing
- D. Identify and evaluate existing practices

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:49 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 276 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 276

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:50 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 284 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 284

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Initiating an attack against targeted business and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits. What type of attack is outlined in the scenario?

- A. Heartbeat Attack
- B. Spear Phishing Attack
- C. Shellshock Attack
- D. Watering Hole Attack

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:50 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 293 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 293

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:50 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 294 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 294

Topic #: 1

[\[All 312-50v10 Questions\]](#)

You are monitoring the network of your organizations. You notice that:

1. There are huge outbound connections from your Internal Network to External IPs
2. On further investigation, you see that the external IPs are blacklisted
3. Some connections are accepted, and some are dropped
4. You find that it is a CnC communication

Which of the following solution will you suggest?

- A. Block the Blacklist IP's @ Firewall
- B. Update the Latest Signatures on your IDS/IPS
- C. Clean the Malware which are trying to Communicate with the External Blacklist IP's
- D. Block the Blacklist IP's @ Firewall as well as Clean the Malware which are trying to Communicate with the External Blacklist IP's.

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:50 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 295 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 295

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:50 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 296 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 296

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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.

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:51 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 304 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 304

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:51 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 307 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 307

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:51 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 314 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 314

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

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

[Hide Answer](#)

Suggested Answer: A

by [deleted] at April 4, 2025, 12:51 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 316 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 316

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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.

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 4, 2025, 12:51 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 317 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 317

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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`

[Hide Answer](#)

Suggested Answer: D

by [deleted] at April 4, 2025, 12:51 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 319 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 319

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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.

[Hide Answer](#)

Suggested Answer: *B*

by [deleted] at April 4, 2025, 12:51 p.m.

Comments

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

EXAM 312-50V10 TOPIC 1 QUESTION 5 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 5

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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", that 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

[Hide Answer](#)

Suggested Answer: D

by  [IT_Nerdz](#) at June 12, 2020, 6:18 a.m.

Comments

  [Nabjoe](#) 1 year, 5 months ago

In windows 10, location of hosts file is C:\Windows\System32\drivers\etc\hosts. This usually takes priority over DNS resolution.
upvoted 2 times

  [Joker20](#) 1 year, 9 months ago

D is correct

IP hostname1 [hostname2] [hostname3]

upvoted 1 times

  [IT_Nerdz](#) 2 years, 5 months ago

The host file is found on the local machine and you can modify this file to have a specific IP Address resolve to a website. This is the file that is commonly used to setup a web server to point an IP to a domain name.
upvoted 3 times

EXAM 312-50V10 TOPIC 1 QUESTION 4 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 4

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

- A. Full Disk encryption
- B. BIOS password
- C. Hidden folders
- D. Password protected files

[Hide Answer](#)

Suggested Answer: A

by  [IT_Nerdz](#) at June 12, 2020, 6:21 a.m.

Comments

 [IT_Nerdz](#) 5 years, 5 months ago

- A. Full Disk encryption - provides the solution required to protect the user data from unauthorized user that could gain access to the device.
- B. BIOS password - As we all know passwords can be brute forced and cracked with several different utilities so this simply slows the thief that is trying to gain access to the data on the drive.
- C. Hidden folders - These are very easy to identify and display with command line, powershell and even changing GUI settings inside of Windows. This just slows down the process but doesn't prevent access.
- D. Password protected files - As we all know passwords can be brute forced and cracked with several different utilities so this simply slows the thief that is trying to gain access to the data on the drive.

upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 1 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 1

Topic #: 1

[All 312-50v10 Questions]

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering

B. Tailgating

C. Piggybacking

D. Announced

Hide Answer

Suggested Answer: B

by  IT_Nerdz at June 12, 2020, 6:25 a.m.

Comments

 **mgadou** 2 years, 6 months ago

tailgating B

upvoted 1 times

 **thetha** 3 years ago

Tailgating, implies no consent like a car tailgating another, while "piggybacking" usually implies support of an authorized person. therefore it is tailgating.

upvoted 2 times

 **Matrix141** 4 years, 3 months ago

Answer is Tailgating B!

Piggybacking

Piggybacking usually implies entry into a building or security area with the consent of the authorized person. For example, an attacker might request an authorized person to unlock a security door, saying that they have forgotten their ID badge. In the interest of common courtesy, the authorized person will allow the attacker to pass through the door.

Tailgating

Tailgating implies accessing a building or secured area without the consent of the authorized person. It is the act of following an authorized person through a secure entrance, as a polite user would open and hold the door for those following them. An attacker, wearing a fake badge, might attempt to enter the secured area by closely following an authorized person through a door that requires key access. They then try to enter the restricted area while pretending to be an authorized person

upvoted 3 times

 **Jude2021** 4 years, 4 months ago

C no fake ID or badge involved

upvoted 1 times

 **tinex** 4 years, 9 months ago

From IPSpecialist & Matt Walkers All in One

Piggybacking and Tailgating is similar technique. Piggybacking is the technique in which unauthorized person waits for an authorized person to gain entry in a restricted area, whereas Tailgating is the technique in which unauthorized person gain access to the restricted area by following the authorized person. By using Fake IDs and close following while crossing the checkpoint, tailgating become easy.

Since the question does not state a badge or fake id , correct answer should be piggybacking

upvoted 2 times

 **_pasha** 4 years, 10 months ago

B. Tailgating

upvoted 1 times

✉️  **devag** 5 years ago

Matt Walkers All in One book states piggybacking = no badge and tail gaiting = with badge
upvoted 1 times

✉️  **misterelection** 5 years ago

According to All In One study guide the correct answer would be "Piggybacking". Another way to remember it is by saying pigs are "naked". That means when there is no badge (naked) its piggybacking. If you show a fake badge then you are tailgating
upvoted 1 times

✉️  **Snickers** 5 years ago

According the ECCouncil CEH v10 book, tailgating is without permission, and piggybacking is with permission. I'm going to go with the book of the people that write the exam.
upvoted 1 times

✉️  **m4dm4n** 5 years, 2 months ago

"Tailgating" implies no consent while "piggybacking" usually implies consent of the authorized person. This is the main difference.
upvoted 3 times

✉️  **Nicker92** 5 years, 2 months ago

Tailgating should be when you have a fake badge, while piggybacking when you don't have a badge and pass with someone pretending to have your hands full or to be at the phone. For me the right answer should be c because no badge was mentioned in the question.
upvoted 3 times

✉️  **MagicianRecon** 5 years ago

INCORRECT. Tailgating is without consent while piggybacking is with consent. So tailgating is the correct answer.
upvoted 3 times

✉️  **Joker20** 4 years, 9 months ago

you passed in Sec + and now will take CEH .
upvoted 1 times

✉️  **IT_Nerdz** 5 years, 5 months ago

This is a common way for someone to gather information about a company and their security procedures. Identify what measures are in place security guards, alarms, bio-metrics, and even observe other employees of how they login to machines and maybe even perform shoulder surfing or find a security badge to gain further access into secure areas of the building.
upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 8 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 8

Topic #: 1

[All 312-50v10 Questions]

Which of the following act requires employer's standard national numbers to identify them on standard transactions?

- A. SOX
- B. HIPAA
- C. DMCA
- D. PCI-DSS **Most Voted**

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

D (67%) B (33%)

by [IT_Nerdz](#) at June 12, 2020, 6:31 a.m.

Comments

[achugh053](#) 1 year, 1 month ago

answer is B. HIPAA
each employer has a standard national number which identifies them on standard transactions
upvoted 1 times

[Vincent_Lu](#) 2 years, 1 month ago

Selected Answer: B
<https://www.hhs.gov/hipaa/for-professionals/other-administration-simplification-rules/index.html>
upvoted 1 times

[BlackAdam](#) 2 years, 4 months ago

Selected Answer: D
PCI-DSS stands for Payment Card Industry Data Security Standard. It is a set of security standards established by major credit card companies to ensure the secure handling of payment card information. PCI-DSS aims to protect sensitive cardholder data during storage, transmission, and processing.

One of the requirements of PCI-DSS is the use of unique employer identification numbers, such as Employer Identification Numbers (EINs) or Tax Identification Numbers (TINs), to identify merchants and service providers involved in payment card transactions. These identification numbers help in standardizing and tracking transactions within the payment card industry.

upvoted 2 times

[Joker20](#) 4 years, 9 months ago

ans is correct

chk

HIPAA requires that health care providers have standard national numbers that identify them on standard transactions. The National Provider Identifier (NPI) is a unique identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses use the NPIs in the administrative transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

upvoted 3 times

[IT_Nerdz](#) 5 years, 5 months ago

HIPAA requires that employers have standard national numbers that identify them on standard transactions. The Employer Identification Number (EIN), issued by the Internal Revenue Service (IRS), was selected as the identifier for employers and was adopted effective July 30, 2002. Resource cited: <https://www.hhs.gov/hipaa/for-professionals/other-administration-simplification-rules/index.html#:~:text=HIPAA%20requires%20that%20employers%20have,adopted%20effective%20July%2030%2C%202002>.

upvoted 2 times

EXAM 312-50 TOPIC 4 QUESTION 4 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 4

Topic #: 4

[\[All 312-50 Questions\]](#)

From the two screenshots below, which of the following is occurring?

First one:

```
1 [10.0.0.253]# nmap -sP 10.0.0.0/24
2 Starting Nmap
3 Host 10.0.0.1 appears to be up.
4 MAC Address: 00:09:5B:29:FD:96 (Netgear)
5 Host 10.0.0.2 appears to be up.
6 MAC Address: 00:0F:B5:96:38:5D (Netgear)
7 Host 10.0.0.4 appears to be up.
8 Host 10.0.0.5 appears to be up.
9 Host 10.0.0.6 appears to be up.
10 Host 10.0.0.7 appears to be up.
11 Host 10.0.0.8 appears to be up.
12 Host 10.0.0.9 appears to be up.
13 Host 10.0.0.10 appears to be up.
14 Host 10.0.0.11 appears to be up.
15 Host 10.0.0.12 appears to be up.
16 Host 10.0.0.13 appears to be up.
17 Host 10.0.0.14 appears to be up.
18 Host 10.0.0.15 appears to be up.
19 Host 10.0.0.16 appears to be up.
20 Host 10.0.0.17 appears to be up.
21 Host 10.0.0.18 appears to be up.
22 Host 10.0.0.19 appears to be up.
23 Host 10.0.0.20 appears to be up.
24 Host 10.0.0.21 appears to be up.
25 Host 10.0.0.22 appears to be up.
26 Host 10.0.0.23 appears to be up.
27 Host 10.0.0.24 appears to be up.
28 Host 10.0.0.25 appears to be up.
29 Host 10.0.0.26 appears to be up.
30 Host 10.0.0.27 appears to be up.
31 Host 10.0.0.28 appears to be up.
32 Host 10.0.0.29 appears to be up.
33 Host 10.0.0.30 appears to be up.
34 Host 10.0.0.31 appears to be up.
35 Host 10.0.0.32 appears to be up.
36 Host 10.0.0.33 appears to be up.
37 Host 10.0.0.34 appears to be up.
38 Host 10.0.0.35 appears to be up.
39 Host 10.0.0.36 appears to be up.
40 Host 10.0.0.37 appears to be up.
41 Host 10.0.0.38 appears to be up.
42 Host 10.0.0.39 appears to be up.
43 Host 10.0.0.40 appears to be up.
44 Host 10.0.0.41 appears to be up.
45 Host 10.0.0.42 appears to be up.
46 Host 10.0.0.43 appears to be up.
47 Host 10.0.0.44 appears to be up.
48 Host 10.0.0.45 appears to be up.
49 Host 10.0.0.46 appears to be up.
50 Host 10.0.0.47 appears to be up.
51 Host 10.0.0.48 appears to be up.
52 Host 10.0.0.49 appears to be up.
53 Host 10.0.0.50 appears to be up.
54 Host 10.0.0.51 appears to be up.
55 Host 10.0.0.52 appears to be up.
56 Host 10.0.0.53 appears to be up.
57 Host 10.0.0.54 appears to be up.
58 Host 10.0.0.55 appears to be up.
59 Host 10.0.0.56 appears to be up.
60 Host 10.0.0.57 appears to be up.
61 Host 10.0.0.58 appears to be up.
62 Host 10.0.0.59 appears to be up.
63 Host 10.0.0.60 appears to be up.
64 Host 10.0.0.61 appears to be up.
65 Host 10.0.0.62 appears to be up.
66 Host 10.0.0.63 appears to be up.
67 Host 10.0.0.64 appears to be up.
68 Host 10.0.0.65 appears to be up.
69 Host 10.0.0.66 appears to be up.
70 Host 10.0.0.67 appears to be up.
71 Host 10.0.0.68 appears to be up.
72 Host 10.0.0.69 appears to be up.
73 Host 10.0.0.70 appears to be up.
74 Host 10.0.0.71 appears to be up.
75 Host 10.0.0.72 appears to be up.
76 Host 10.0.0.73 appears to be up.
77 Host 10.0.0.74 appears to be up.
78 Host 10.0.0.75 appears to be up.
79 Host 10.0.0.76 appears to be up.
80 Host 10.0.0.77 appears to be up.
81 Host 10.0.0.78 appears to be up.
82 Host 10.0.0.79 appears to be up.
83 Host 10.0.0.80 appears to be up.
84 Host 10.0.0.81 appears to be up.
85 Host 10.0.0.82 appears to be up.
86 Host 10.0.0.83 appears to be up.
87 Host 10.0.0.84 appears to be up.
88 Host 10.0.0.85 appears to be up.
89 Host 10.0.0.86 appears to be up.
90 Host 10.0.0.87 appears to be up.
91 Host 10.0.0.88 appears to be up.
92 Host 10.0.0.89 appears to be up.
93 Host 10.0.0.90 appears to be up.
94 Host 10.0.0.91 appears to be up.
95 Host 10.0.0.92 appears to be up.
96 Host 10.0.0.93 appears to be up.
97 Host 10.0.0.94 appears to be up.
98 Host 10.0.0.95 appears to be up.
99 Host 10.0.0.96 appears to be up.
100 Host 10.0.0.97 appears to be up.
101 Host 10.0.0.98 appears to be up.
102 Host 10.0.0.99 appears to be up.
103 Host 10.0.0.100 appears to be up.
104 Host 10.0.0.101 appears to be up.
105 Host 10.0.0.102 appears to be up.
106 Host 10.0.0.103 appears to be up.
107 Host 10.0.0.104 appears to be up.
108 Host 10.0.0.105 appears to be up.
109 Host 10.0.0.106 appears to be up.
110 Host 10.0.0.107 appears to be up.
111 Host 10.0.0.108 appears to be up.
112 Host 10.0.0.109 appears to be up.
113 Host 10.0.0.110 appears to be up.
114 Host 10.0.0.111 appears to be up.
115 Host 10.0.0.112 appears to be up.
116 Host 10.0.0.113 appears to be up.
117 Host 10.0.0.114 appears to be up.
118 Host 10.0.0.115 appears to be up.
119 Host 10.0.0.116 appears to be up.
120 Host 10.0.0.117 appears to be up.
121 Host 10.0.0.118 appears to be up.
122 Host 10.0.0.119 appears to be up.
123 Host 10.0.0.120 appears to be up.
124 Host 10.0.0.121 appears to be up.
125 Host 10.0.0.122 appears to be up.
126 Host 10.0.0.123 appears to be up.
127 Host 10.0.0.124 appears to be up.
128 Host 10.0.0.125 appears to be up.
129 Host 10.0.0.126 appears to be up.
130 Host 10.0.0.127 appears to be up.
131 Host 10.0.0.128 appears to be up.
132 Host 10.0.0.129 appears to be up.
133 Host 10.0.0.130 appears to be up.
134 Host 10.0.0.131 appears to be up.
135 Host 10.0.0.132 appears to be up.
136 Host 10.0.0.133 appears to be up.
137 Host 10.0.0.134 appears to be up.
138 Host 10.0.0.135 appears to be up.
139 Host 10.0.0.136 appears to be up.
140 Host 10.0.0.137 appears to be up.
141 Host 10.0.0.138 appears to be up.
142 Host 10.0.0.139 appears to be up.
143 Host 10.0.0.140 appears to be up.
144 Host 10.0.0.141 appears to be up.
145 Host 10.0.0.142 appears to be up.
146 Host 10.0.0.143 appears to be up.
147 Host 10.0.0.144 appears to be up.
148 Host 10.0.0.145 appears to be up.
149 Host 10.0.0.146 appears to be up.
150 Host 10.0.0.147 appears to be up.
151 Host 10.0.0.148 appears to be up.
152 Host 10.0.0.149 appears to be up.
153 Host 10.0.0.150 appears to be up.
154 Host 10.0.0.151 appears to be up.
155 Host 10.0.0.152 appears to be up.
156 Host 10.0.0.153 appears to be up.
157 Host 10.0.0.154 appears to be up.
158 Host 10.0.0.155 appears to be up.
159 Host 10.0.0.156 appears to be up.
160 Host 10.0.0.157 appears to be up.
161 Host 10.0.0.158 appears to be up.
162 Host 10.0.0.159 appears to be up.
163 Host 10.0.0.160 appears to be up.
164 Host 10.0.0.161 appears to be up.
165 Host 10.0.0.162 appears to be up.
166 Host 10.0.0.163 appears to be up.
167 Host 10.0.0.164 appears to be up.
168 Host 10.0.0.165 appears to be up.
169 Host 10.0.0.166 appears to be up.
170 Host 10.0.0.167 appears to be up.
171 Host 10.0.0.168 appears to be up.
172 Host 10.0.0.169 appears to be up.
173 Host 10.0.0.170 appears to be up.
174 Host 10.0.0.171 appears to be up.
175 Host 10.0.0.172 appears to be up.
176 Host 10.0.0.173 appears to be up.
177 Host 10.0.0.174 appears to be up.
178 Host 10.0.0.175 appears to be up.
179 Host 10.0.0.176 appears to be up.
180 Host 10.0.0.177 appears to be up.
181 Host 10.0.0.178 appears to be up.
182 Host 10.0.0.179 appears to be up.
183 Host 10.0.0.180 appears to be up.
184 Host 10.0.0.181 appears to be up.
185 Host 10.0.0.182 appears to be up.
186 Host 10.0.0.183 appears to be up.
187 Host 10.0.0.184 appears to be up.
188 Host 10.0.0.185 appears to be up.
189 Host 10.0.0.186 appears to be up.
190 Host 10.0.0.187 appears to be up.
191 Host 10.0.0.188 appears to be up.
192 Host 10.0.0.189 appears to be up.
193 Host 10.0.0.190 appears to be up.
194 Host 10.0.0.191 appears to be up.
195 Host 10.0.0.192 appears to be up.
196 Host 10.0.0.193 appears to be up.
197 Host 10.0.0.194 appears to be up.
198 Host 10.0.0.195 appears to be up.
199 Host 10.0.0.196 appears to be up.
200 Host 10.0.0.197 appears to be up.
201 Host 10.0.0.198 appears to be up.
202 Host 10.0.0.199 appears to be up.
203 Host 10.0.0.200 appears to be up.
204 Host 10.0.0.201 appears to be up.
205 Host 10.0.0.202 appears to be up.
206 Host 10.0.0.203 appears to be up.
207 Host 10.0.0.204 appears to be up.
208 Host 10.0.0.205 appears to be up.
209 Host 10.0.0.206 appears to be up.
210 Host 10.0.0.207 appears to be up.
211 Host 10.0.0.208 appears to be up.
212 Host 10.0.0.209 appears to be up.
213 Host 10.0.0.210 appears to be up.
214 Host 10.0.0.211 appears to be up.
215 Host 10.0.0.212 appears to be up.
216 Host 10.0.0.213 appears to be up.
217 Host 10.0.0.214 appears to be up.
218 Host 10.0.0.215 appears to be up.
219 Host 10.0.0.216 appears to be up.
220 Host 10.0.0.217 appears to be up.
221 Host 10.0.0.218 appears to be up.
222 Host 10.0.0.219 appears to be up.
223 Host 10.0.0.220 appears to be up.
224 Host 10.0.0.221 appears to be up.
225 Host 10.0.0.222 appears to be up.
226 Host 10.0.0.223 appears to be up.
227 Host 10.0.0.224 appears to be up.
228 Host 10.0.0.225 appears to be up.
229 Host 10.0.0.226 appears to be up.
230 Host 10.0.0.227 appears to be up.
231 Host 10.0.0.228 appears to be up.
232 Host 10.0.0.229 appears to be up.
233 Host 10.0.0.230 appears to be up.
234 Host 10.0.0.231 appears to be up.
235 Host 10.0.0.232 appears to be up.
236 Host 10.0.0.233 appears to be up.
237 Host 10.0.0.234 appears to be up.
238 Host 10.0.0.235 appears to be up.
239 Host 10.0.0.236 appears to be up.
240 Host 10.0.0.237 appears to be up.
241 Host 10.0.0.238 appears to be up.
242 Host 10.0.0.239 appears to be up.
243 Host 10.0.0.240 appears to be up.
244 Host 10.0.0.241 appears to be up.
245 Host 10.0.0.242 appears to be up.
246 Host 10.0.0.243 appears to be up.
247 Host 10.0.0.244 appears to be up.
248 Host 10.0.0.245 appears to be up.
249 Host 10.0.0.246 appears to be up.
250 Host 10.0.0.247 appears to be up.
251 Host 10.0.0.248 appears to be up.
252 Host 10.0.0.249 appears to be up.
253 Host 10.0.0.250 appears to be up.
```

Second one:

```
1 [10.0.0.252]# nmap -sO 10.0.0.2
2 Starting Nmap 4.01 at 2006-07-14 12:56 BST
3 Interesting protocols on 10.0.0.2:
4 (The 251 protocols scanned but not shown below are
5 in state: closed)
6 PROTOCOL STATE SERVICE
7 1 open icmp
8 2 open|filtered igmp
9 6 open tcp
10 17 open udp
11 255 open|filtered unknown
12 Nmap finished: 1 IP address (1 host up) scanned in
13 1.259 seconds
14 [10.0.0.253]# nmap -sP
15 [10.0.0.253]# nmap -sP
```

A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.

B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.

D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.253 is performing a port scan against 10.0.0.2.

[Hide Answer](#)

Suggested Answer: A

by  goayxh at June 20, 2020, 5:44 p.m.

Comments

  thinkinconcept 1 year ago

None of this is correct, must be some kind of terminology issue here, let's dig in.

.253 is nmap -sP .0/24

.252 is nmap -sO .2

Command: -sO is found here <https://nmap.org/book/scan-methods-ip-protocol-scan.html>

Command: -sP is found here <https://nmap.org/book/man-host-discovery.html>

So -sP is NOT a port scan and it's also not an IP protocol scan. But what is this "IP scan" mentioned in every answer? I would have to assume they mean "IP protocol scan" which is -sO. But none of the answers match correctly even with the terminology changed to the IP protocol scan. So then does "IP scan" mean any scan other than a port scan? If that's the case then none of the answers match either since 252 is NOT performing a port scan. SIGH, IDK...

upvoted 1 times

  bleepbl0p 3 years, 6 months ago

Answer A states the same information as Answer D does, but then also includes the correct information for the first scan, this is why A is correct.

upvoted 2 times

 **MoodyDork** 2 years, 8 months ago

While A is correct, your explanation is not. D does not have the /24
upvoted 1 times

 **goayxh** 3 years, 11 months ago

Should be D, -sO is IP protocol scan
upvoted 1 times

 **MoodyDork** 2 years, 8 months ago

you missed out the /24 information that makes A the correct answer.
upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 215 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 215

Topic #: 8

[\[All 312-50 Questions\]](#)

What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of \$300 given that the technician who charges \$10/ hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

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

[Hide Answer](#)

Suggested Answer: D

by  [cehbound](#) at July 11, 2019, 6:37 p.m.

Comments

  [IamStudying](#) 1 year, 2 months ago

The answer is 146. You have to calculate yearly costs, but HDD has a lifetime of 3 years, so you have to divide 440\$ per 3 years
upvoted 2 times

  [jasonderules](#) 2 years, 2 months ago

this questions doesn't say 3 YEARS
upvoted 3 times

  [cehbound](#) 2 years, 10 months ago

Should the answer be A \$440 since it is for 1 year
upvoted 4 times

  [Kev](#) 2 years, 7 months ago

Wouldn't it be 146?

First examine the EF = 100

Hard drive fails every 3 years so divide 100/3 which = 33.333... or 33% (rounded)

There's a 33% chance the hard drive will fail each year and it will definitely fail within 3 years.

So ARO = 33% or .33

And SLE = $300 + 14 * 10$

(\$300 for the hard drive plus \$14*10 for the worker)

Then we have $.33 * (300 + 14 * 10)$

Remember PEMDAS?

(Parenthesis, Exponent, Multiply, Divide, Add, Subtract)

So we multiply what's in the parenthesis first ($14 * 10$) which = 140

Then we add what's left in the parenthesis ($300 + 140$) which = 440

Lastly we multiply $.33 * 440$ which = 145.2

Closest answer is 146.

If you multiply $146 * 3$ (for 3 years) it = 438, close to 440.

If I'm off please let me know.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 13 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 13

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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 **Most Voted**
- C. Website defacement
- D. Web cache poisoning

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [deleted] at April 5, 2025, 3:25 a.m.

Comments

 **suraj028** 2 months ago

Selected Answer: B

Website Mirroring

upvoted 1 times

 **lopesjaf** 4 months ago

Selected Answer: B

B. Website mirroring: Copying the entire website locally for offline analysis. ✓ Matches the description.

upvoted 1 times

 **jonekool** 7 months, 1 week ago

Selected Answer: B

Copying an entire website to a local drive is website mirroring

upvoted 1 times

 **john7588** 7 months, 1 week ago

Selected Answer: B

This process involves creating a complete replica of a website, including its structure and content. Jane's action of copying the entire website to analyze it aligns perfectly with this definition.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 17 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 17

Topic #: 1

[All 312-50v13 Questions]

Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection.

What is the APT lifecycle phase that Harry is currently executing?

A. Initial intrusion **Most Voted**

- B. Persistence
- C. Cleanup
- D. Preparation

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [deleted] at April 5, 2025, 3:34 a.m.

Comments

[User icon](#) **besntakes** 1 month, 2 weeks ago

Selected Answer: A

At this stage, Harry is using techniques such as spear-phishing and exploiting vulnerabilities to gain access to the target organization's network. Successfully deploying malware and establishing an outbound connection indicates that he has compromised at least one system — marking the Initial intrusion phase of the APT (Advanced Persistent Threat) lifecycle.

upvoted 1 times

[User icon](#) **lopesjaf** 4 months ago

Selected Answer: A

A. Initial intrusion: Gaining initial access to the target network using spear-phishing and exploits. ✓ Matches the current step.

upvoted 1 times

[User icon](#) **d503c75** 6 months, 2 weeks ago

Selected Answer: A

This stage involves gaining unauthorized access to the target network. Attackers may use various methods such as spear-phishing, exploiting vulnerabilities, or installing malware.

upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 148 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 148

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: A

by  certmonk at July 9, 2020, 2:43 a.m.

Comments

  **Neela**  1 year, 2 months ago

key word - anonymous user : To upload files the user must have proper write file permissions.

upvoted 8 times

  **certmonk**  1 year, 4 months ago

The answer should be B. File system permission is not a vulnerability. And unauthorized file system permission change may require to elevate the permission. A process is also running in this case which means that privileges were escalated to run 'nc'

upvoted 7 times

EXAM 312-50V10 TOPIC 1 QUESTION 96 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 96

Topic #: 1

[\[All 312-50v10 Questions\]](#)

In Risk Management, how is the term "likelihood" related to the concept of "threat?"

- A. Likelihood is the likely source of a threat that could exploit a vulnerability.
- B. Likelihood is the probability that a threat-source will exploit a vulnerability.
- C. Likelihood is a possible threat-source that may exploit a vulnerability.
- D. Likelihood is the probability that a vulnerability is a threat-source.

[Hide Answer](#)

Suggested Answer: *B*

by  nsamuel204 at July 22, 2020, 9:06 a.m.

Comments

  nsamuel204 1 year, 4 months ago

likelihood. A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 98 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 98

Topic #: 1

[\[All 312-50v10 Questions\]](#)

What is the least important information when you analyze a public IP address in a security alert?

- A. ARP
- B. Whois
- C. DNS
- D. Geolocation

[Hide Answer](#)

Suggested Answer: A

by  [TrendMicroDLPSSucks](#) at *July 23, 2020, 12:05 p.m.*

Comments

  [TrendMicroDLPSSucks](#) 1 year, 4 months ago

ARP,, The mac address table is of course least important in this case,
upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 101 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 101

Topic #: 1

[\[All 312-50v10 Questions\]](#)

On performing a risk assessment, you need to determine the potential impacts when some of the critical business process of the company interrupt its service.

What is the name of the process by which you can determine those critical business?

- A. Risk Mitigation
- B. Emergency Plan Response (EPR)
- C. Disaster Recovery Planning (DRP)
- D. Business Impact Analysis (BIA)

[Hide Answer](#)

Suggested Answer: D

by  TrendMicroDLPSSucks at July 23, 2020, 12:19 p.m.

Comments

  **TrendMicroDLPSSucks** 1 year, 4 months ago

Risk mitigation is a strategy to prepare for and lessen the effects of threats faced by a data center. Comparable to risk reduction, risk mitigation takes steps to reduce the negative effects of threats and disasters on business continuity (BC). Threats that might put a business at risk include cyberattacks, weather events and other causes of physical or virtual damage to a data center.

upvoted 1 times

  **TrendMicroDLPSSucks** 1 year, 4 months ago

Business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuance plan;

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 108 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 108

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: D

by  TrendMicroDLPSSucks at July 25, 2020, 12:41 a.m.

Comments

  **TrendMicroDLPSSucks** 1 year, 4 months ago

his NIST SP 800-53 database represents the security controls and associated assessment procedures defined in NIST SP 800-53 Revision 4 Recommended Security Controls for Federal Information Systems and Organizations. Any discrepancies noted in the content between this NIST SP 800-53 database and the latest published NIST Special Publication SP 800-53 Revision 4, please refer to the official published documents that is posted on <http://csrc.nist.gov>.

upvoted 1 times

EXAM 312-50 TOPIC 2 QUESTION 18 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 18

Topic #: 2

[\[All 312-50 Questions\]](#)

An NMAP scan of a server shows port 69 is open. What risk could this pose?

- A. Unauthenticated access
- B. Weak SSL version
- C. Cleartext login
- D. Web portal data leak

[Hide Answer](#)

Suggested Answer: A

by  Morphei at Aug. 15, 2020, 9:56 a.m.

Comments

  Morphei  1 year, 3 months ago

TCP/UDP port 69 is used by the trivial file transfer protocol (TFTP).

upvoted 6 times

  Morphei  1 year, 3 months ago

Trivial File Transfer Protocol is very simple in design and has limited features as compared to File Transfer Protocol (FTP). TFTP provides no authentication and security while transferring files. As a result, it is usually used for transferring boot files or configuration files between machines in a local setup

upvoted 5 times

EXAM 312-50V10 TOPIC 1 QUESTION 235 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 235

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

A. Armitage

B. Nikto

C. Metasploit

D. Nmap

[Hide Answer](#)

Suggested Answer: *B*

by  [hasib125](#) at Aug. 17, 2020, 8:31 p.m.

Comments

  [jagadeesh666](#) 1 year, 2 months ago

Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Through one Metasploit instance, your team will: Use the same sessions. Share hosts, captured data, and downloaded files.

upvoted 1 times

  [hasib125](#) 1 year, 3 months ago

Nikto is a free software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 233 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 233

Topic #: 1

[\[All 312-50v10 Questions\]](#)

It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data. Which of the following terms best matches the definition?

A. Attack

B. Vulnerability

C. Threat

D. Risk

[Hide Answer](#)

Suggested Answer: C

by  [callmethefuz](#) at Aug. 20, 2020, 4:46 p.m.

Comments

  [sandman310323](#)  1 year, 3 months ago

keyword: potential
upvoted 6 times

  [TrendMicroDLPSSucks](#)  1 year, 3 months ago
threat

Abbreviation(s) and Synonym(s):

Cyber Threat

Definition(s):

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

upvoted 3 times

  [callmethefuz](#) 1 year, 3 months ago
why isn't this an Attack?
upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 234 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 234

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

- A. Use security policies and procedures to define and implement proper security settings.
- B. Use digital certificates to authenticate a server prior to sending data.
- C. Validate and escape all information sent to a server.
- D. Verify access right before allowing access to protected information and UI controls.

[Hide Answer](#)

Suggested Answer: C

by  [TrendMicroDLPSSucks](#) at Aug. 21, 2020, 2:44 a.m.

Comments

  [TrendMicroDLPSSucks](#) 1 year, 3 months ago

general, effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures:

Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input.
Encode data on output. At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
Use appropriate response headers. To prevent XSS in HTTP responses that aren't intended to contain any HTML or JavaScript, you can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend.
Content Security Policy. As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 243 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 243

Topic #: 1

[\[All 312-50v10 Questions\]](#)

>NMAP ""sn 192.168.11.200-215 The NMAP command above performs which of the following?

- A. A port scan
- B. A ping scan**
- C. An operating system detect
- D. A trace sweep

[Hide Answer](#)

Suggested Answer: *B*

by  [TrendMicroDLPSSucks](#) at Aug. 24, 2020, 12:59 a.m.

Comments

  [TrendMicroDLPSSucks](#) 1 year, 3 months ago

on earlier versions it is also called nmap -sP

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 247 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 247

Topic #: 1

[\[All 312-50v10 Questions\]](#)

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain. If the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

A. list domain=abccorp.local type=zone

B. ls ""d accorp.local

C. list server=192.168.10.2 type=all

D. lserver 192.168.10.2 ""t all

[Hide Answer](#)

Suggested Answer: B

by  TrendMicroDLPSSucks at Aug. 24, 2020, 1:50 a.m.

Comments

  **_pasha** 1 year, 4 months ago

Answer B

type "ls -d <URL>", if the domain is having DNS Zone Transfer Misconfiguration, then it will show up.

upvoted 1 times

  **TrendMicroDLPSSucks** 1 year, 9 months ago

nslookup -ls just sends a raw AXFR query to the remote nameserver, which will initiate a zone transfer if and only if the remote nameserver is dumb enough to respond to unsolicited, unauthorized AXFRs originating from random machines on the Internet.

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 251 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 251

Topic #: 1

[\[All 312-50v10 Questions\]](#)

This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering and it will tell you the

"landscape" looks like. What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

- A. network mapping
- B. footprinting**
- C. escalating privileges
- D. gaining access

[Hide Answer](#)

Suggested Answer: *B*

by  [TrendMicroDLPSSucks](#) at Aug. 24, 2020, 2:02 a.m.

Comments

  [TrendMicroDLPSSucks](#) 1 year, 3 months ago

Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.[1]

upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 114 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 114

Topic #: 1

[\[All 312-50v10 Questions\]](#)

In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.

Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system whose credentials are known. It was written by sysinternals and has been integrated within the framework. The penetration testers successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.

Which of the following is true hash type and sort order that is used in the psexec module's 'smbpass' option?

- A. LM:NT
- B. NTLM:LM
- C. NT:LM
- D. LM:NTLM Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Gibby_Toni](#) at Aug. 24, 2020, 7:07 a.m.

Comments

  [Vincent_Lu](#) 1 year, 1 month ago

Selected Answer: D

D. LM:NTLM

upvoted 1 times

  [Yebi](#) 1 year, 10 months ago

Selected Answer: D

Correct Answer should be :"D. LM:NTLM"

<https://marc.info/?l=metasploit-framework&m=120801903514927>

upvoted 2 times

  [datastream](#) 3 years, 11 months ago

The order is that undoubtedly LM is first. As regards NT or NTLM.....this is a Metasploit question and they call it NTLM

<https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/>

the order is undoubtedly that LM is first. As regards

upvoted 1 times

  [devag](#) 4 years ago

A is correct - <https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4>

upvoted 1 times

  [goodlife](#) 4 years, 2 months ago

Correct answer is D (see https://en.wikipedia.org/wiki/Pass_the_hash)

upvoted 1 times

 **hasib125** 4 years, 2 months ago

D: LM:NTLM also correct !

upvoted 1 times

 **Gibby_Toni** 4 years, 3 months ago

ermm... shouldnt the ans be D (LM:NTLM)

upvoted 2 times

EXAM 312-50 TOPIC 5 QUESTION 14 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 14

Topic #: 5

[All 312-50 Questions]

An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

- A. Unplug the network connection on the company's web server. **Most Voted**
- B. Determine the origin of the attack and launch a counterattack.
- C. Record as much information as possible from the attack.
- D. Perform a system restart on the company's web server.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by Sprasashu at Aug. 28, 2020, 1:48 a.m.

Comments

greeklover84 1 year, 5 months ago

Selected Answer: C

I suggest C it is the only answer that makes sense.

upvoted 1 times

YetiSpaghetti 2 years, 10 months ago

It's C. I'm too lazy to explain so look at this reddit thread.

https://www.reddit.com/r/CEH/comments/g0aa6u/conflicting_ceh_test_question/

upvoted 1 times

NikoTomas 1 year, 8 months ago

From above provided link:

"The CEH model says that you identify and analyze an incident before you contain or eradicate it. What's more, it's very rare that they'd want you to make a change to the system without using an integrated change management process.

If you're talking a small company or your own web server, unplugging it might make sense. But what's the maximum tolerable downtime for that server? How much damage is this unspecified hack going to do compared to the cost of shutting down the company's web presence?

But that's common sense/real-life talking. For CEH, just memorize the steps in their process (they have a blog article about their steps here):

Prepare
Identify
Contain
Eradicate
Recover
Lessons learned
"

upvoted 1 times

salei 3 years ago

Selected Answer: A

In the above scenario, the company's web server is hacked. As an IT security engineer, your first task is to unplug the network connection (cable) on the company's web server from the router and modem in order to prevent further attacks.

upvoted 2 times

Vermil 4 years, 11 months ago

C is the answer

upvoted 3 times

✉  **amal1302** 5 years, 1 month ago

the web server must be in a DMZ. It is a question from forensic perspective, he has to get as much info as he can to find the indice of compromision. If heunplug the server then he will not know how to fix the problem.

upvoted 2 times

✉  **Sprasashu** 5 years, 3 months ago

Answer is A

upvoted 3 times

✉  **hcakyol** 5 years, 2 months ago

If you are Polat ALEMDAR you can do it.

<https://www.youtube.com/watch?v=yLx9B3xVOw8>

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 300 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 300

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

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

[Hide Answer](#)

Suggested Answer: *D*

by  [TrendMicroDLPSSucks](#) at Aug. 28, 2020, 2:14 p.m.

Comments

  [TrendMicroDLPSSucks](#) 1 year, 3 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. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 87 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 87

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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** Most Voted
- D. Null byte

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [deleted] at April 10, 2025, 2:43 a.m.

Comments

 **lopesjaf** 4 months ago

Selected Answer: C

Variation refers to changing the syntax or using different representations (like 'or '1'='1' vs or 1=1) in an attempt to evade signature-based IDS/IPS systems.

upvoted 1 times

 **e30b32d** 6 months, 1 week ago

Selected Answer: C

Variation: An attacker uses this technique to easily evade any comparison statement

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 90 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 90

Topic #: 1

[\[All 312-50v13 Questions\]](#)

In this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?

- A. Evil twin
- B. Chop chop attack
- C. Wardriving
- D. KRACK Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

 D (100%)

by [deleted] at April 10, 2025, 2:52 a.m.

Comments

 **lopesjaf** 4 months ago

Selected Answer: D

The described attack involves tricking a victim into reinstalling an already-in-use key by manipulating and replaying handshake messages in a Wi-Fi network.

This is exactly the KRACK (Key Reinstallation Attack) vulnerability, which targets the WPA2 handshake.

It causes nonce and packet number resets, allowing attackers to decrypt and manipulate data.

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 197 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 197

Topic #: 1

[\[All 312-50v13 Questions\]](#)

An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?

- A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing

Most Voted

- B. Implementing sophisticated matches such as "OR john' = 'john" in place of classical matches like "OR 1=1"

- C. Manipulating white spaces in SQL queries to bypass signature detection

- D. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [deleted] at April 15, 2025, 5:42 a.m.

Comments

 **lopesjaf** 3 months, 4 weeks ago

Selected Answer: A

Signature-based IDS systems detect known attack patterns, such as specific SQL keywords or operators.

Advanced SQL injection evasion techniques often involve encoding or obfuscating payloads so they do not match signature patterns directly.

Using SQL functions like CHAR() to represent characters in hexadecimal or decimal form converts suspicious keywords into encoded forms that still execute but evade simple pattern matching.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 198 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 198

Topic #: 1

[\[All 312-50v13 Questions\]](#)

As the Chief Information Security Officer (CISO) at a large university, you are responsible for the security of a campus-wide Wi-Fi network that serves thousands of students, faculty, and staff. Recently, there has been a rise in reports of unauthorized network access, and you suspect that some users are sharing their login credentials. You are considering deploying an additional layer of security that could effectively mitigate this issue. What would be the most suitable measure to implement in this context?

- A. Implement network segmentation
- B. Deploy a VPN for the entire campus
- C. Enforce a policy of regularly changing Wi-Fi passwords
- D. Implement 802.1X authentication Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [deleted] at April 15, 2025, 5:46 a.m.

Comments

 **lopesjaf** 3 months, 4 weeks ago

Selected Answer: D

802.1X authentication is a port-based network access control protocol commonly used in enterprise and campus Wi-Fi networks.
upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 200 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 200

Topic #: 1

[\[All 312-50v13 Questions\]](#)

In the process of setting up a lab for malware analysis, a cybersecurity analyst is tasked to establish a secure environment using a sheep dip computer. The analyst must prepare the testbed while adhering to best practices. Which of the following steps should the analyst avoid when configuring the environment?

- A. Installing malware analysis tools on the guest OS
- B. Connecting the system to the production network during the malware analysis Most Voted
- C. Simulating Internet services using tools such as INetSim
- D. Installing multiple guest operating systems on the virtual machine(s)

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [deleted] at April 15, 2025, 5:50 a.m.

Comments

 **lopesjaf** 3 months, 4 weeks ago

Selected Answer: B

A sheep dip system is an isolated environment used to safely analyze potentially malicious files.

It should be completely isolated from production networks to prevent malware from spreading or communicating with external systems.

Connecting the sheep dip system to the production network risks infecting live systems or leaking sensitive data.
upvoted 1 times

 **JXC** 6 months, 2 weeks ago

Selected Answer: B

Should AVOID - Answer is B

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 204 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 204

Topic #: 1

[\[All 312-50v13 Questions\]](#)

While working as an intern for a small business, you have been tasked with managing the company's web server. The server is being bombarded with requests, and the company's website is intermittently going offline. You suspect that this could be a Distributed Denial of Service (DDoS) attack. As an ethical hacker, which of the following steps would be your first course of action to mitigate the issue?

- A. Contact your Internet Service Provider (ISP) for assistance Most Voted
- B. Install a newer version of the server software
- C. Implement IP address whitelisting
- D. Increase the server's bandwidth

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [deleted] at April 17, 2025, 12:50 a.m.

Comments

 **lopesjaf** 3 months, 4 weeks ago

Selected Answer: A

In a DDoS attack, the server is overwhelmed by massive traffic, often from many distributed sources.

Your own server resources (bandwidth, CPU) may not be sufficient to handle or filter this flood.

ISPs typically have the capacity and tools (such as traffic filtering, blackholing, or rate limiting) to help mitigate large-scale DDoS attacks upstream before the traffic reaches your server.

Contacting your ISP quickly can help reduce the impact.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 231 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 231

Topic #: 1

[All 312-50v13 Questions]

While performing a security audit of a web application, an ethical hacker discovers a potential vulnerability. The application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. The ethical hacker decides to exploit this vulnerability further. Which type of SQL Injection attack is the ethical hacker likely to use?

A. UNION SQL Injection

B. Error-based SQL Injection **Most Voted**

C. In-band SQL Injection

D. Blind/Inferential SQL Injection

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by [deleted] at April 17, 2025, 4:02 a.m.

Comments

✉ **lopesjaf** 3 months, 4 weeks ago

Selected Answer: B

This is classic for Error-based SQL Injection, where attackers exploit error messages to gain information about the database.

Error-based SQL Injection relies on the database returning error messages with useful info.

Blind/Inferential SQL Injection is used when error messages are hidden or generic.

UNION SQL Injection is a technique to combine results from multiple queries but often used after initial info gathering.

In-band SQL Injection is a general category that includes both error-based and UNION-based.

upvoted 3 times

✉ **lopesjaf** 3 months, 4 weeks ago

Selected Answer: A

The question is about bypassing detection of SYN packets on BSD-derived TCP/IP stacks using stealth scanning.

Maimon Scan is designed specifically for this, using a FIN/ACK probe which is less likely to be detected and effective against BSD TCP/IP stacks.

upvoted 1 times

✉ **KnightHeart** 6 months, 1 week ago

Selected Answer: B

"detailed error messages"

Answer :B

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 237 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 237

Topic #: 1

[\[All 312-50v13 Questions\]](#)

A security analyst is preparing to analyze a potentially malicious program believed to have infiltrated an organization's network. To ensure the safety and integrity of the production environment, the analyst decided to use a sheep dip computer for the analysis. Before initiating the analysis, what key step should the analyst take?

- A. Install the potentially malicious program on the sheep dip computer.
- B. Store the potentially malicious program on an external medium, such as a CD-ROM. Most Voted
- C. Run the potentially malicious program on the sheep dip computer to determine its behavior.
- D. Connect the sheep dip computer to the organization's internal network.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [deleted] at April 17, 2025, 4:28 a.m.

Comments

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

EXAM 312-50V13 TOPIC 1 QUESTION 239 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 239

Topic #: 1

[\[All 312-50v13 Questions\]](#)

Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However, you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?

- A. Switching all data transmission to the HTTPS protocol.
- B. Implementing SSL certificates on your company's web servers.
- C. Utilizing SSH for secure remote logins to the servers.
- D. Applying the Diffie-Hellman protocol to exchange the symmetric key. Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [deleted] at April 17, 2025, 4:42 a.m.

Comments

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

EXAM 312-50V13 TOPIC 1 QUESTION 245 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 245

Topic #: 1

[\[All 312-50v13 Questions\]](#)

An ethical hacker is testing a web application of a financial firm. During the test, a 'Contact Us' form's input field is found to lack proper user input validation, indicating a potential Cross-Site Scripting (XSS) vulnerability. However, the application has a stringent Content Security Policy (CSP) disallowing inline scripts and scripts from external domains but permitting scripts from its own domain. What would be the hacker's next step to confirm the XSS vulnerability?

- A. Utilize a script hosted on the application's domain to test the form Most Voted
- B. Try to disable the CSP to bypass script restrictions
- C. Inject a benign script inline to the form to see if it executes
- D. Load a script from an external domain to test the vulnerability

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [deleted] at April 17, 2025, 4:55 a.m.

Comments

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

EXAM 312-50V13 TOPIC 1 QUESTION 246 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 246

Topic #: 1

[\[All 312-50v13 Questions\]](#)

John, a security analyst, is analyzing a server suspected of being compromised. The attacker has used a non admin account and has already gained a foothold on the system. John discovers that a new Dynamic Link Library is loaded in the application directory of the affected server. This DLL does not have a fully qualified path and seems to be malicious. What privilege escalation technique has the attacker likely used to compromise this server?

- A. DLL Hijacking Most Voted
- B. Named Pipe Impersonation
- C. Spectre and Meltdown Vulnerabilities
- D. Exploiting Misconfigured Services

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [deleted] at April 17, 2025, 4:57 a.m.

Comments

 **Ma06RC** 2 months, 2 weeks ago

Selected Answer: A

See page 765 of the CEH v13 book

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 273 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 273

Topic #: 1

[\[All 312-50v13 Questions\]](#)

Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.

What is the encryption software employed by Sam for securing the email messages?

- A. PGP
- B. SMTP
- C. GPG Most Voted
- D. S/MIME

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [deleted] at April 19, 2025, 4:19 a.m.

Comments

  **lopesjaf** 3 months, 4 weeks ago

Selected Answer: C

GPG (GNU Privacy Guard) is a free and open-source implementation of the OpenPGP standard. It supports hybrid encryption, which combines:

Symmetric-key encryption: For encrypting the actual message (faster).

Asymmetric-key encryption: For encrypting the symmetric key and ensuring secure key exchange.

It is widely used for email encryption and secure communications, just like PGP, but GPG is open-source.

upvoted 1 times

  **e30b32d** 6 months, 1 week ago

Selected Answer: C

Free and open-source implementation of the OpenPGP standard.

Supports hybrid encryption (symmetric for message, asymmetric for key exchange).

Commonly used to encrypt emails, files, and communications.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 295 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 295

Topic #: 1

[\[All 312-50v13 Questions\]](#)

Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

Which of the following types of fault injection attack is performed by Robert in the above scenario?

- A. Frequency/voltage tampering
- B. Optical, electromagnetic fault injection (EMFI)
- C. Temperature attack
- D. Power/clock/reset glitching

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

 D (100%)

by [deleted] at April 19, 2025, 5:11 a.m.

Comments

 **e30b32d** 6 months, 1 week ago

Selected Answer: D

D. Power/clock/reset glitching
upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 298 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 298

Topic #: 1

[\[All 312-50v13 Questions\]](#)

Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility.

Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

- A. wash
- B. net view
- C. macof
- D. ntptrace

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [deleted] at April 19, 2025, 5:19 a.m.

Comments

 **e30b32d** 6 months, 1 week ago

[Selected Answer: A](#)

The tool, Wash can identify the WPS-enabled APs and detect if the AP is in locked or unlocked state.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 68 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 68

Topic #: 1

[All 312-50v13 Questions]

What is the port to block first in case you are suspicious that an IoT device has been compromised?

A. 22

B. 48101 **Most Voted**

C. 80

D. 443

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by  [hakeem4](#) at April 28, 2025, 9:21 p.m.

Comments

 [lopesjaf](#) 4 months ago

Selected Answer: B

Port 48101 is commonly used by many IoT devices (especially Chinese-manufactured ones) for remote communication with command-and-control (C2) servers.

If an IoT device is suspected to be compromised, this port is often used for backdoor access or to send data to attackers.

Blocking this port can interrupt malicious remote control and exfiltration activity.

upvoted 2 times

 [Luispe](#) 5 months, 2 weeks ago

Selected Answer: B

B is the correcto

upvoted 1 times

 [KnightHeart](#) 6 months ago

Selected Answer: A

B. 48101

Usage: This port is not a standard, well-known port (e.g., HTTP, SSH). Some proprietary IoT devices or malware may use arbitrary high ports, but it is not a universal target.

Without specific context, blocking a non-standard port like 48101 is less effective than targeting widely used, vulnerable ports (e.g., 22, 80).

A. 22 (SSH)

Usage: Secure Shell (SSH) is a protocol for remote login and command execution. Many IoT devices (e.g., routers, cameras) use SSH for management, and unsecured SSH ports are a common entry point for attackers.

upvoted 1 times

 [e30b32d](#) 6 months, 1 week ago

Selected Answer: B

The port to block first if you suspect an IoT device has been compromised is B. 48101.

upvoted 1 times

 [e30b32d](#) 6 months, 1 week ago

Selected Answer: B

correct answer option b 48101

upvoted 1 times

 hakeem4 7 months ago

Selected Answer: A

48101 is a specific port used by some IoT devices (e.g., cameras), but less standard — 22 is more critical.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 20 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 20

Topic #: 1

[\[All 312-50v13 Questions\]](#)

CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted.

What is the defensive technique employed by Bob in the above scenario?

A. Whitelist validation Most Voted

B. Output encoding

C. Blacklist validation

D. Enforce least privileges

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [e30b32d](#) at May 20, 2025, 2:04 a.m.

Comments

  [suraj028](#) 2 months ago

Selected Answer: A

Also called allow-listing
upvoted 1 times

  [lopesjaf](#) 4 months ago

Selected Answer: A

A. Whitelist validation: Only accepts input that meets predefined allowed criteria. ✓ Matches the scenario.
upvoted 1 times

  [e30b32d](#) 6 months, 1 week ago

Selected Answer: A

A is the correct answer
upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 37 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 37

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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 Most Voted

D. Desynchronization

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (100%)

by  [e30b32d](#) at May 20, 2025, 5:05 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: C

Obfuscating techniques involve intentionally encoding or altering the structure of data (such as URLs, payloads, or packets) so that intrusion detection systems (IDS) or security filters fail to recognize or properly analyze the malicious content, while the target system can still interpret it correctly.

upvoted 1 times

  [e30b32d](#) 6 months, 1 week ago

Selected Answer: C

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 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 54 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 54

Topic #: 1

[\[All 312-50v13 Questions\]](#)

Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network. What is the type of vulnerability assessment that Jude performed on the organization?

- A. Application assessment
- B. External assessment
- C. Passive assessment
- D. Host-based assessment

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [e30b32d](#) at May 20, 2025, 5:27 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: B

An External Assessment involves evaluating the network security posture from outside the organization's perimeter. This simulates an attacker's point of view and focuses on:

Firewalls

Routers

Public-facing servers (web, email, etc.)

DMZ configurations

Open ports and services

Public IP addresses

This is exactly what Jude was doing—testing from an external, outsider perspective.

upvoted 2 times

  [e30b32d](#) 6 months, 1 week ago

Selected Answer: B

Types of Vulnerability Assessment - External Assessment

External assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks from outside the organization. It determines the level of security of the external network and firewall. (P.527/511)

upvoted 2 times

  [e30b32d](#) 6 months, 1 week ago

Jude performed an evaluation of the organization's public-facing infrastructure — such as firewalls, routers, and servers — from an outsider's perspective (i.e., like a hacker). This type of assessment aims to:

Identify vulnerabilities visible to external attackers

Estimate the risk of network security attacks

Assess internet-facing systems

This is exactly what an external assessment involves.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 71 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 71

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

 D (100%)

by  [e30b32d](#) at May 21, 2025, 1:58 a.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: D

When you enter commands in a Linux shell (like Bash), they are stored in the .bash_history file by default. If during your penetration test you entered a login or password in plaintext on the command line, it would be stored in that file.

To remove traces of sensitive data, like passwords typed directly into the shell, you should clean or edit the .bash_history file.
upvoted 1 times

  [e30b32d](#) 6 months, 1 week ago

Selected Answer: D

My vote goes to bash_history.
upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 102 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 102

Topic #: 1

[\[All 312-50v13 Questions\]](#)

What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

A. AndroidManifest.xml Most Voted

B. classes.dex

C. APK.info

D. resources.asrc

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [e30b32d](#) at May 21, 2025, 5:07 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: A

In an Android application, the AndroidManifest.xml file is essential because it:

Declares components like:

Activities

Services

Broadcast receivers

Content providers

upvoted 2 times

  [e30b32d](#) 6 months, 1 week ago

Selected Answer: A

A. AndroidManifest.xml

upvoted 2 times

EXAM 312-50V13 TOPIC 1 QUESTION 121 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 121

Topic #: 1

[\[All 312-50v13 Questions\]](#)

During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.

Which of the following services is enumerated by Lawrence in this scenario?

- A. Remote procedure call (RPC)
- B. Telnet
- C. Server Message Block (SMB)**
- D. Network File System (NFS)

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (100%)

by  [e30b32d](#) at May 22, 2025, 1:46 a.m.

Comments

  [plig](#) 2 months ago

Selected Answer: C

Port 445 is a network port used by the Server Message Block (SMB) protocol for file sharing, printer sharing, and other network services. It allows applications on networked computers to read and write files and request services from

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 182 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 182

Topic #: 1

[\[All 312-50v13 Questions\]](#)

During an attempt to perform an SQL injection attack, a certified ethical hacker is focusing on the identification of database engine type by generating an ODBC error. The ethical hacker, after injecting various payloads, finds that the web application returns a standard, generic error message that does not reveal any detailed database information. Which of the following techniques would the hacker consider next to obtain useful information about the underlying database?

- A. Utilize a blind injection technique that uses time delays or error signatures to extract information Most Voted
- B. Try to insert a string value where a number is expected in the input field
- C. Attempt to compromise the system through OS-level command shell execution
- D. Use the UNION operator to combine the result sets of two or more SELECT statements

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [KnightHeart](#) at May 30, 2025, 7:08 a.m.

Comments

  [lopesjaf](#) 3 months, 4 weeks ago

Selected Answer: A

If error messages are generic, the attacker must infer data indirectly, which is exactly what blind SQL injection (especially time-based or Boolean-based) is designed for.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 91 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 91

Topic #: 1

[\[All 312-50v13 Questions\]](#)

After an audit, the auditors inform you that there is a critical finding that you must tackle immediately. You read the audit report, and the problem is the service running on port 389.

Which service is this and how can you tackle the problem?

- A. The service is NTP, and you have to change it from UDP to TCP in order to encrypt it.
- B. The service is LDAP, and you must change it to 636, which is LDAPS. Most Voted
- C. The findings do not require immediate actions and are only suggestions.
- D. The service is SMTP, and you must change it to SMIME, which is an encrypted way to send emails.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Luispe](#) at June 17, 2025, 9:32 a.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: B

Port 389 is the default port for LDAP (Lightweight Directory Access Protocol), which by default transmits data in plaintext.

The secure version of LDAP is LDAPS, which runs on port 636 and uses SSL/TLS to encrypt communication.

Changing to LDAPS helps protect credentials and data from interception.

upvoted 2 times

  [Luispe](#) 5 months, 2 weeks ago

Selected Answer: B

La respuesta correcta es B. The service is LDAP, and you must change it to 636, which is LDAPS.

upvoted 1 times

Exam 312-50 Topic 8 Question 267 Discussion

Actual exam question from ECCouncil's 312-50

Question #: 267

Topic #: 8

[All 312-50 Questions]

A hacker was able to easily gain access to a website. He was able to log in via the frontend user login form of the website using default or commonly used credentials. This exploitation is an example of what Software design flaw?

A. Insufficient security management Most Voted

B. Insufficient database hardening

C. Insufficient input validation

D. Insufficient exception handling

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

A (100%)

by  csevcs at Sept. 4, 2020, 3:15 p.m.

Comments

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

Actually, A is correct from my perspective, because using default credentials on the website is a security management problem
upvoted 5 times

 **Script_Kitty** Most Recent 1 year, 3 months ago

I feel the answer is most likely A. Database hardening (option B) is about securing the database from attacks, but the issue here is with the management of credentials, not the database structure or protection mechanisms. In this scenario, we have to assume the credentials were easy to guess, which shows weak security practices and policies to protect against unauthorized access.
There could be confusion between the specific use of security tokens and other security practices. For instance, if B mentioned a practice that's commonly misunderstood or conflated with the use of tokens, like encryption or specific types of authentication methods, it might seem like a good choice without understanding the distinct role and definition of security tokens.
upvoted 1 times

 **White_T_10** 2 years ago

ok, here is my theory after reading the question so many times. Using default credentials to log in is a database-hardening issue. If the question stated the attacker could gain access using SQL injection techniques, then yes, it would be input validation. So, I'd go with B.
upvoted 1 times

 **XX20Jim20XX** 1 year, 7 months ago

https://blog.netwrix.com/2022/12/21/database_security_hardening/
Remove default accounts.
upvoted 1 times

 **salei** 2 years, 4 months ago

Selected Answer: A
The B, C and D don't really make sense here
upvoted 1 times

 **Cww1** 3 years, 7 months ago

Answer is Correct
upvoted 1 times

 **btc** 4 years, 3 months ago

I strongly believe the answer should be C not B
upvoted 1 times

 **csevcs** 4 years, 8 months ago

The answer must be C, I think.

upvoted 1 times

✉️👤 **boboloboli** 4 years, 8 months ago

B is the correct answer. They are able to log in using the defaults. The first thing you do to harden a system is change the default passwords.

upvoted 1 times

✉️👤 **bleble00001** 4 years, 7 months ago

I am not sure if "Database Hardening" has anything to do with this. <https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/database-hardening-best>

Besides, by using a weak/default password, the hacker is only accessing the website. Nothing in the question mentions about accessing the database. You have access to a website does not necessarily mean you have access to a database. If you can manipulate/access data via the application once you gain access to the system, does not necessarily mean the database is not hardened.

upvoted 2 times

EXAM 312-50 TOPIC 8 QUESTION 249 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 249

Topic #: 8

[\[All 312-50 Questions\]](#)

You've just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access?

- A. Disable Key Services
- B. Create User Account
- C. Download and Install Netcat Most Voted
- D. Disable IPTables

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

 C (100%)

by  [boboloboli](#) at Sept. 7, 2020, 7:23 a.m.

Comments

  [Mkt_Bruno](#) 1 year, 4 months ago

Selected Answer: C

Install Netcat

upvoted 1 times

  [fishPSU21](#) 2 years, 2 months ago

The key part of this questions is what TOOL should you use. thus the answer has to be C since creating an account is not a "tool". if it didnt say tool then it would be creating a user account.

upvoted 2 times

  [boboloboli](#) 2 years, 8 months ago

This should be C. download and install netcat.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 48 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 48

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

 B (100%)

by  [lopesjaf](#) at July 30, 2025, 6:19 a.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: B

A Community Cloud is a cloud infrastructure that is shared by several organizations and supports a specific community with shared concerns, such as mission, security requirements, policy, or compliance considerations.

This model offers:

Shared infrastructure

Reduced cost compared to private cloud

More control and security than public cloud

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 63 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 63

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [lopesjaf](#) at July 30, 2025, 6:44 a.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: B

Nessus is a well-known vulnerability scanner that can perform comprehensive checks on Windows systems (and others), identifying missing patches, misconfigurations, and vulnerabilities.

It automates vulnerability discovery and produces detailed reports, making it the best approach for technical vulnerability assessment.
upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 74 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 74

Topic #: 1

[\[All 312-50v13 Questions\]](#)

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

- A. Remediation
- B. Verification
- C. Risk assessment
- D. Vulnerability scan

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [lopesjaf](#) at July 30, 2025, 8:57 p.m.

Comments

  [lopesjaf](#) 4 months ago

Selected Answer: A

Remediation – Apply fixes or patches to reduce or eliminate the vulnerabilities.

upvoted 1 times

EXAM 312-50V13 TOPIC 1 QUESTION 101 DISCUSSION

Actual exam question from ECCouncil's 312-50v13

Question #: 101

Topic #: 1

[\[All 312-50v13 Questions\]](#)

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

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [lopesjaf](#) at July 30, 2025, 9:45 p.m.

Comments

 [d503c75](#) 2 months, 2 weeks ago

Selected Answer: D

Alice uses Bryan's public key to encrypt the message

Bryan uses Alice's public key to confirm the digital signature

This follows the fundamental PKI principles: encrypt with the recipient's public key, sign with your own private key, and verify signatures with the sender's public key.

upvoted 1 times

 [lopesjaf](#) 4 months ago

Selected Answer: D

Alice needs to send a confidential document and also ensure authenticity using a digital signature. In a Public Key Infrastructure (PKI), the operations are:

Encryption for confidentiality:

Alice encrypts the message using Bryan's public key.

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 273 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 273

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: D

by  [mightyfei](#) at Oct. 3, 2020, 5:42 p.m.

Comments

  [mightyfei](#)  1 year, 1 month 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 resorting 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 5 times

EXAM 312-50 TOPIC 5 QUESTION 32 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 32

Topic #: 5

[\[All 312-50 Questions\]](#)

Which of the following is a characteristic of Public Key Infrastructure (PKI)?

- A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
- B. Public-key cryptosystems distribute public-keys within digital signatures.
- C. Public-key cryptosystems do not require a secure key distribution channel.
- D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

[Hide Answer](#)

Suggested Answer: *B*

by  [hackmenow](#) at Oct. 3, 2020, 11:45 p.m.

Comments

 [Alexei](#) 1 year, 1 month ago

I thought the digital signature would be created by encrypting a hash value using the senders' private key, and then the receiver should be able to verify the senders' identity by decrypting the cipher using the sender's public key

upvoted 2 times

 [hackmenow](#) 1 year, 1 month ago

Not sure if this is correct. I will think public keys are distributed using Digital certificates and not digital signature

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 311 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 311

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which of the following steps for risk assessment methodology refers to vulnerability identification?

- A. Assigns values to risk probabilities; Impact values
- B. Determines risk probability that vulnerability will be exploited (High, Medium, Low)
- C. Identifies sources of harm to an IT system (Natural, Human, Environmental)
- D. Determines if any flaws exist in systems, policies, or procedures

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  dotmt at Oct. 6, 2020, 8:24 p.m.

Comments

 **ffactor** 1 year, 2 months ago

B might be classification not identification.
upvoted 1 times

 **tom_braian11** 2 years, 2 months ago

Selected Answer: D
The answer is D.
upvoted 1 times

 **jinjection** 3 years, 1 month ago

B correct
upvoted 1 times

 **Pb1805** 3 years, 4 months ago

Think its D
upvoted 1 times

 **datastream** 3 years, 9 months ago

According to the official documentation, it's this....

Identifies the sources, causes, consequences, etc. of the internal and external risks affecting the security of the organization

Risk Identification

It is the initial step of the risk management plan. The main aim is to identify the risks - sources, causes, consequences, etc. of the internal and external risks affecting the security of the organization before they cause harm to the organization. The risk identification process depends on the skill set of the people and it differs from one organization to the other.

upvoted 2 times

 **datastream** 3 years, 9 months ago

So it is D.

B is Risk Assessment
upvoted 2 times

 **gizicudu** 4 years ago

It's B. Marked answer is BS.
upvoted 1 times

👤 **mightyfei** 4 years ago

should be B
upvoted 1 times

👤 **devag** 4 years ago

i think B also
upvoted 1 times

👤 **dotmt** 4 years, 1 month ago

i think B is the ans.
upvoted 1 times

EXAM 312-50 TOPIC 2 QUESTION 5 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 5

Topic #: 2

[All 312-50 Questions]

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 the 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:89

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

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

A (67%)

B (33%)

by  Halibay at Oct. 13, 2020, 9:54 a.m.

Comments

  Halibay Highly Voted 5 years, 1 month ago

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
```

  Booict Most Recent 10 months, 3 weeks ago

Selected Answer: B

B - Linux systems often have a variety of services running on different ports, which can make it challenging to determine the exact OS version based on open ports alone
upvoted 1 times

  smsoc 1 year, 1 month ago

Selected Answer: A

Port 139 (netbios-ssn): This port is commonly used by Windows machines for NetBIOS over TCP/IP (NBT) communication.
upvoted 1 times

  bic3p 1 year, 4 months ago

Selected Answer: A

Port 139 (netbios-ssn): This port is commonly used by Windows machines for NetBIOS over TCP/IP (NBT) communication.

Port 445 (not shown): Although not explicitly shown in the results, it's likely that port 445 is also open, as it's often used together with port 139 for SMB (Server Message Block) communication in Windows environments.

MAC Address: The MAC address (00:00:48:0D:EE:89) is within the range assigned to Microsoft Corporation, which further suggests that the host is a Windows machine.

While it's possible for other operating systems or devices to have these ports open, the combination of these factors makes it most likely that the target machine is running a Windows operating system. (hacker9pt)

upvoted 1 times

 EXAM 312-50V10 TOPIC 1 QUESTION 104 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 104

Topic #: 1

[All 312-50v10 Questions]

Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends "many" IP packets, based on the average number of packets sent by all origins and using some thresholds.

In concept, the solution developed by Bob is actually:

- A. Just a network monitoring tool
- B. A signature-based IDS
- C. A hybrid IDS
- D. A behavior-based IDS Most Voted

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

D (100%)

by  guidoleonardo at Oct. 29, 2020, 10:23 a.m.

Comments

 **4bd3116** 1 year, 4 months ago

Selected Answer: D

is a behavior-based
upvoted 1 times

 **ffactor** 2 years, 2 months ago

I'm guessing behavior based IDS. It is producing an alert when the traffic deviates from baseline.
upvoted 1 times

 **avd12345** 4 years ago

Monitor network and raise alerts -> so it should be IDS
upvoted 1 times

 **beowolf** 4 years, 4 months ago

Read the question. Answer is there in the question. Monitor network. Not IDS.
upvoted 1 times

 **guidoleonardo** 5 years, 1 month ago

I was pretty sure that the answer were "D"
upvoted 4 times

 **MagicianRecon** 5 years ago

seems to be IDS to me as well
upvoted 2 times

 **Castoret** 4 years, 11 months ago

I guess that an IDS is much more than a traffic monitoring but "in concept" I would also say "D"
upvoted 1 times

 **MeganONO** 4 years, 9 months ago

I would also have said "D".
upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 19 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 19

Topic #: 8

[\[All 312-50 Questions\]](#)

Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pre-test state.

Which of the following activities should not be included in this phase? (see exhibit)

Exhibit:

- I. Removing all files uploaded on the system
- II. Cleaning all registry entries
- III. Mapping of network state
- IV. Removing all tools and maintaining backdoor for reporting

A. III

B. IV **Most Voted**

C. III and IV

D. All should be included.

[Hide Answer](#)

Suggested Answer: A

The post-attack phase revolves around returning any modified system(s) to the pretest state. Examples of such activities:

- ⇒ Removal of any files, tools, exploits, or other test-created objects uploaded to the system during testing
- ⇒ Removal or reversal of any changes to the registry made during system testing

References: Computer and Information Security Handbook, John R. Vacca (2012), page 531

Community vote distribution

B (50%)

C (50%)

by  kevintoshi at Oct. 29, 2020, 11:53 a.m.

Comments

 **XX20Jim20XX** 1 year, 1 month ago

Selected Answer: C

why not C?

upvoted 1 times

 **Goki_28** 2 years, 5 months ago

Selected Answer: B

you should not be maintaining backdoor.

upvoted 1 times

 **Qwertyzloy** 3 years ago

A is the correct one, you should do all other - remove all, except the network mapping.

upvoted 1 times

 **IamStuding** 3 years, 9 months ago

It's not B. You are the tester and you are finished your work. Why you still to have access after you did your job? It is not legal.

upvoted 4 times

 **kevintoshi** 4 years, 1 month ago

Answer wrong .

it should be B.

upvoted 4 times

 **thebigdax** 4 years ago

exactly, backdoor should not be maintained

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 197 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 197

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

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

[Hide Answer](#)

Suggested Answer: C

by  **gizicudu** at Nov. 12, 2020, 12:12 a.m.

Comments

 **PT_Go_Hard_2** 1 year ago

I agree. CA does not validate an individual or organization. It validates the website domain and the web servers (Information systems) for secure communications. The owners or organization is not validated, their information systems is validated.

upvoted 1 times

 **gizicudu** 1 year, 6 months ago

Bad question. CA is the only option making sense but CA does not vouch for identity, just domain validation..

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 292 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 292

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which of the following is a component of a risk assessment?

- A. Administrative safeguards
- B. Physical security
- C. Logical interface
- D. DMZ

[Hide Answer](#)

Suggested Answer: A

by  **gizicudu** at Nov. 22, 2020, 12:32 a.m.

Comments

 **gizicudu** 1 year ago

A is correct

upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 289 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 289

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which of the following statements regarding ethical hacking is incorrect?

- A. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services
- B. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems
- Most Voted**
- C. Ethical hacking should not involve writing to or modifying the target systems.
- D. Testing should be remotely performed offsite.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Estevon916](#) at Nov. 28, 2020, 8:51 p.m.

Comments

  [Vincent_Lu](#) 1 year, 2 months ago

Selected Answer: B

Ethical hackers use the same methods and techniques to test/bypass the system's defenses, but rather than exploiting vulnerabilities found.
<http://searchsecurity.techtarget.com/definition/ethical-hacker>
upvoted 1 times

  [Estevon916](#) 4 years ago

Pretty sure the answer is C.
upvoted 1 times

  [chacha543](#) 3 years, 12 months ago

the answer is B, keyword 'incorrect'
upvoted 2 times

EXAM 312-50 TOPIC 3 QUESTION 19 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 19

Topic #: 3

[\[All 312-50 Questions\]](#)

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

- A. Firewall-management policy
- B. Acceptable-use policy Most Voted
- C. Remote-access policy
- D. Permissive policy

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by [Kelzz](#) at Dec. 2, 2020, 5:29 p.m.

Comments

swetty 1 year ago

https://en.wikipedia.org/wiki/Remote_access_policy
upvoted 1 times

salei 1 year, 1 month ago

Selected Answer: C
Definition of these policies are available here:
https://www.tutorialspoint.com/computer_security/computer_security_policies.htm#:~:text=Permissive%20Policy%20%E2%88%92%20It%20is%20a,exploits%20are%20taken%20in%20consideration.
upvoted 1 times

Darpan24 1 year, 5 months ago

Selected Answer: B
Dial-out modem is already installed on the system, to verify the use one should check if it is allowed or not. Hence Acceptable use policy.
upvoted 2 times

DaveyIRL 2 years, 7 months ago

Acceptable use pertains to the equipment implemented already, not for regulating what equipment can or cannot be implemented.
upvoted 1 times

Kelzz 2 years, 12 months ago

remote access policy? Should it not be Acceptable use since he is already on the network and not connecting remotely?
upvoted 4 times

Ajstars 2 years, 8 months ago

I quite agree that it should be acceptable use policy. except the installation is permissible for a business need, such shouldn't be allowed.
upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 11 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 11

Topic #: 1

[\[All 312-50v10 Questions\]](#)

PGP, SSL, and IKE are all examples of which type of cryptography?

- A. Hash Algorithm
- B. Digest
- C. Secret Key
- D. Public Key

[Hide Answer](#)

Suggested Answer: D

by  **Bal00** at Dec. 3, 2020, 1:57 p.m.

Comments

 **tinex** 1 year, 3 months ago

Because all these methods use both private and public key, both choices (private and public) key are correct. therefor, i would change the last option from "Private" to "Shared" key. This way the question is a lot less confusion

upvoted 1 times

 **Bal00** 1 year, 5 months ago

Would PGP not be considered to have Private as well? Or am I overthinking it?

upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 118 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 118

Topic #: 8

[\[All 312-50 Questions\]](#)

You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Network-based IDS

B. Firewall

C. Proxy

D. Host-based IDS

[Hide Answer](#)

Suggested Answer: A

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

References: <https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids>

by  Sasiron at Dec. 10, 2020, 3:10 p.m.

Comments

  Sasiron  3 years, 11 months ago

Hi admin, it would be nice if you can change the answers' order. All the correct answers to this point are " A " It has become a pattern. jumble the answers plz.

upvoted 10 times

  aids00123  1 year, 3 months ago

Agreed

upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 310 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 310

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: D

by  [lizano_](#) at Dec. 15, 2020, 2:59 a.m.

Comments

  [lizano_](#) 1 year, 5 months ago

SSL or TLS encryption takes place at the presentation layer, Layer 6 of the OSI model.

upvoted 3 times

EXAM 312-50 TOPIC 8 QUESTION 119 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 119

Topic #: 8

[\[All 312-50 Questions\]](#)

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

[Hide Answer](#)

Suggested 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>

by  [Lama_11](#) at Dec. 23, 2020, 12:13 a.m.

Comments

  [Grezavi](#) 1 year, 4 months ago

Transport later port numbers performed by network firewalls. Application headers by application firewalls.

upvoted 1 times

  [Lama_11](#) 1 year, 11 months ago

So based on the explanation the answer is D?

upvoted 2 times

EXAM 312-50 TOPIC 8 QUESTION 89 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 89

Topic #: 8

[\[All 312-50 Questions\]](#)

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 Web sites that trust the Web browser user by stealing the user's authentication credentials.
- B. Attempts by attackers to access the user and password information stored in the company's SQL database.
- 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.

[Hide Answer](#)

Suggested Answer: A

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

by [deleted] at Feb. 26, 2019, 6:26 p.m.

Comments

 **Sasiron** 11 months, 3 weeks ago

Definitely not D. Answer is A.

upvoted 2 times

 **brettonatkin** 2 years, 7 months ago

Had my 312-50 today, I looked for the questions that were in the exam and found this website, all the question from here appeared in the exam. I wish I could find this site before taking the exam :/

upvoted 4 times

EXAM 312-50 TOPIC 4 QUESTION 47 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 47

Topic #: 4

[\[All 312-50 Questions\]](#)

What statement is true regarding LM hashes?

- A. LM hashes consist in 48 hexadecimal characters.
- B. LM hashes are based on AES128 cryptographic standard.
- C. Uppercase characters in the password are converted to lowercase.
- D. LM hashes are not generated when the password length exceeds 15 characters.

[Hide Answer](#)

Suggested Answer: D

by  **cupcake** at Feb. 8, 2021, 7:30 p.m.

Comments

  **cupcake** 1 year, 3 months ago

c and d

upvoted 1 times

  **MeganONO** 1 year, 3 months ago

Not C, everything is converted to uppercase

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 94 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 94

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  czarul79 at Feb. 10, 2021, 7:26 a.m.

Comments

 **czarul79** Highly Voted 2 years, 9 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 12 months ago

Selected Answer: D
D is correct
upvoted 2 times

 **kiki533** 1 year ago

Answer is D
upvoted 1 times

 **Daniel8660** 1 year, 1 month 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** 2 years, 4 months ago

correct
upvoted 2 times

 EXAM 312-50V11 TOPIC 1 QUESTION 122 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 122

Topic #: 1

[All 312-50v11 Questions]

Why should the security analyst disable/remove unnecessary ISAPI filters?

- A. To defend against social engineering attacks
- B. To defend against webserver attacks **Most Voted**
- C. To defend against jailbreaking
- D. To defend against wireless attacks

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  czarul79 at Feb. 13, 2021, 8:46 a.m.

Comments

 **czarul79** **Highly Voted** 4 years, 3 months ago

B is correct 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** **Most Recent** 1 year, 4 months ago

Selected Answer: B

B is correct answer
upvoted 1 times

 **Daniel8660** 2 years, 7 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, 7 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, 8 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, 10 months ago

correct

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 20 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 20

Topic #: 4

[\[All 312-50 Questions\]](#)

A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

- A. -sO
- B. -sP
- C. -sS **Most Voted**
- D. -sU

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

C (100%)

by  [dimaste](#) at Feb. 17, 2021, 9:21 a.m.

Comments

 [a4687eb](#) 1 year, 4 months ago

-sO shows not port numbers but protocol numbers. User is not able to find our what PORTS are Open/Closed from nmap output that with -sO because it will show protocol numbers only. Correct answer is "C" of course it is not perfect answer because it will show only open ports for TCP not for UDP. So the options vs the question do not match perfectly.

upvoted 1 times

 [a4687eb](#) 1 year, 4 months ago

Selected Answer: C

-sO is protocol can not port

upvoted 1 times

 [Novmejst](#) 2 years, 7 months ago

Selected Answer: C

C. -sS (TCP SYN Scan)

upvoted 1 times

 [lau2123](#) 2 years, 9 months ago

NMAP switch "-sS" (Option C), which stands for "TCP SYN scan". This is one of the most popular and widely used NMAP scan techniques that sends SYN packets to each target port, and waits for a response from the target. This can help the hacker identify which ports are open and accepting connections.

Option A (-sO) is an IP protocol scan that can be used to identify which IP protocols are supported by the target system.

Option B (-sP) is a "ping" or "host discovery" scan that can be used to identify which hosts are up and responding to network traffic.

Option D (-sU) is a UDP scan that can be used to identify which UDP ports are open and accepting connections.

upvoted 2 times

 [PennyTester](#) 4 years, 1 month ago

The correct answer is -sS, I confirmed it using nmap. -sO is IP protocol scan, tells you if ICMP is open

upvoted 3 times

 [Hacker100](#) 4 years, 2 months ago

A. -sO is correct answer.

upvoted 1 times

 [EOL](#) 4 years, 6 months ago

A is a good answer

-sO: IP Protocol scan

-sP: Ping sweep scan

-sS: stealth scan

-sU: UDP scan

upvoted 2 times

✉️  **melante** 4 years, 7 months ago

Isn't C correct? -sO is protocol scan, it does not scan for ports!

upvoted 1 times

✉️  **dimaste** 4 years, 9 months ago

I suppose C is correct

<https://nmap.org/book/scan-methods-ip-protocol-scan.html>

upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 11 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 11

Topic #: 3

[\[All 312-50 Questions\]](#)

How can telnet be used to fingerprint a web server?

- A. telnet webserverAddress 80 HEAD / HTTP/1.0
- B. telnet webserverAddress 80 PUT / HTTP/1.0
- C. telnet webserverAddress 80 HEAD / HTTP/2.0
- D. telnet webserverAddress 80 PUT / HTTP/2.0

[Hide Answer](#)

Suggested Answer: A

by  [mind903](#) at Feb. 17, 2021, 5:09 p.m.

Comments

  [mind903](#) 1 year, 3 months ago

HTTP 2.0 is not text based. Therefore only HTTP1.0 is answer
upvoted 4 times

  [mind903](#) 1 year, 3 months ago

HTTP Command
- Put (inserting)
- Get (Return header + body)
- Head (Return Header)
- Post (Update)
- Delete (delete)
upvoted 4 times

 EXAM 312-50V11 TOPIC 1 QUESTION 97 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 97

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**
- C. Man-in-the middle attack
- D. Network sniffing

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  czarul79 at Feb. 20, 2021, 8:52 a.m.

Comments

 **czarul79** **Highly Voted** 2 years, 9 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** 2 years, 1 month ago

thank you. These are the kind of discussion people need.

upvoted 8 times

 **Snipa_x** 2 years ago

I'm just curious. Have you taken the exam yet?

upvoted 1 times

 **Seahorse66** **Highly Voted** 1 year, 6 months 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** 1 year, 1 month 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** 2 years, 4 months ago

correct

upvoted 3 times

EXAM 312-50 TOPIC 8 QUESTION 140 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 140

Topic #: 8

[\[All 312-50 Questions\]](#)

Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid.

What is this middle step called?

- A. Fuzzy-testing the code
- B. Third party running the code
- C. Sandboxing the code Most Voted
- D. String validating the code

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

C (100%)

by  [cupcake](#) at Feb. 20, 2021, 4:30 p.m.

Comments

  **Pragdeashwar** 1 year, 1 month ago

Selected Answer: C

Option C is correct, Sandboxing the code
upvoted 1 times

  **Pragdeashwar** 1 year, 1 month ago

Option C is correct, Sandboxing the code
upvoted 1 times

  **Grezavi** 3 years, 10 months ago

If fuzzy testing is right per the website then probably the middle steps takes place in a sandbox but what is done inside is the fuzzy testing that the question is looking for.
upvoted 1 times

  **cupcake** 4 years, 3 months ago

should be sandbox testing
upvoted 2 times

  **dimaste** 4 years, 3 months ago

agree, it's a sandbox testing
upvoted 2 times

EXAM 312-50V10 TOPIC 1 QUESTION 16 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 16

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: *B*

by  **Joker20** at March 3, 2021, 7:08 a.m.

Comments

 **Joker20** 1 year, 2 months ago

<https://www.fortinet.com/resources/cyberglossary/what-is-dmz>

correct

upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 349 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 349

Topic #: 8

[\[All 312-50 Questions\]](#)

While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

- A. Block port 25 at the firewall.
- B. Shut off the SMTP service on the server.
- C. Force all connections to use a username and password. **Most Voted**
- D. Switch from Windows Exchange to UNIX Sendmail.
- E. None of the above.

[Hide Answer](#)

Suggested Answer: E

Community vote distribution

C (100%)

by  [dimaste](#) at March 4, 2021, 3:25 p.m.

Comments

 [boog](#) 1 year ago

Selected Answer: C

By enforcing authentication using a username and password for SMTP connections, you can ensure that only authorized users are able to access the SMTP server. This can be achieved by implementing SMTP authentication mechanisms such as SMTP-AUTH or STARTTLS, which require clients to provide valid credentials before establishing a connection to the server.

Blocking port 25 at the firewall (option A) would indeed prevent telnet access to the SMTP server, but it would also affect legitimate email communication as port 25 is the standard SMTP port used for email delivery. Shutting off the SMTP service on the server (option B) would completely disable email functionality. Switching from Windows Exchange to UNIX Sendmail (option D) is not necessary to address the issue at hand and would involve a significant infrastructure change. ---ChatGPT

upvoted 1 times

 [gauravtewari](#) 2 years, 6 months ago

Blocking port 25 in the firewall or forcing all connections to use username and password would have the consequences that the server is unable to communicate with other SMTP servers. Turning off the SMTP service would disable the email function completely. All email servers use SMTP to communicate with other email servers and therefore changing email server will not help. So None of the above option is true.

upvoted 2 times

 [dimaste](#) 3 years, 2 months ago

Why not C

upvoted 1 times

 [fishPSU21](#) 3 years, 2 months ago

a hacker can just get the username and password from an employee and then it will be compromised. This wouldn't be an effective method.

upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 12 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 12

Topic #: 1

[\[All 312-50v10 Questions\]](#)

Which of the following is considered as one of the most reliable forms of TCP scanning?

- A. TCP Connect/Full Open Scan
- B. Half-open Scan
- C. NULL Scan
- D. Xmas Scan

[Hide Answer](#)

Suggested Answer: A

by  **fisfis** at March 5, 2021, 6:35 p.m.

Comments

 **fisfis** 1 year, 8 months ago

<http://etutorials.org/Networking/network+security+assessment/Chapter+4.+IP+Network+Scanning/4.2+TCP+Port+Scanning/>
upvoted 1 times

 **fisfis** 1 year, 8 months ago

B. Half-open Scan
upvoted 1 times

 **jinjection** 1 year, 1 month ago

wrong

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 1 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 1

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted
- D. Web form input validation

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (76%) A (24%)

by  noot at March 6, 2021, 5:56 p.m.

Comments

 **Daniel8660** Highly Voted 3 years, 1 month 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

 **jenna339** Highly Voted 4 years, 8 months ago

yes answer is correct, inducing user to click something they don't intend to is Cross Site Request Forgery

upvoted 5 times

 **aboru** Most Recent 3 months, 3 weeks ago

Selected Answer: C

Why CSRF fits:

- The victim was logged into online banking (session active in browser).
- Clicking the link opened another tab or session that sent a hidden HTTP request to the bank using the victim's cookies.
- The bank processed it as if the user authorized it.
- Result: Funds transferred without the victim's knowledge.

upvoted 1 times

 **hunain456** 3 months, 3 weeks ago

Selected Answer: C

Other mitigation strategies include:

SameSite Cookie Attribute: This attribute on cookies can prevent the browser from sending cookies with cross-site requests. Setting SameSite=Strict offers the strongest protection, but may break some legitimate functionality (like a user clicking a link from an email). SameSite=Lax is a more common and effective compromise.

Referer Header Validation: The server can check the Referer or Origin header to ensure the request is coming from the expected source (e.g., the same domain). However, this is not a foolproof defense as these headers can sometimes be missing or spoofed.

upvoted 1 times

👤 **yyj933125** 1 year, 8 months ago

Answer is C

upvoted 1 times

👤 **qtygbapjpesdayazko** 1 year, 10 months ago

is this questions still valid?

upvoted 2 times

👤 **SageCloud** 2 years, 2 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** 2 years, 3 months ago

Answer is C

upvoted 1 times

👤 **ostorgaf** 2 years, 3 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, 5 months ago

The answer is C

upvoted 1 times

👤 **Chucho_es_gay** 3 years ago

Answer is C

upvoted 3 times

👤 **studyin** 3 years, 1 month ago

Answer is C

upvoted 1 times

👤 **leandrosoares** 3 years, 1 month ago

C is the right for this one!

upvoted 1 times

👤 **antoclk** 3 years, 2 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 forged 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** 3 years, 2 months ago

Answer is C

upvoted 1 times

👤 **basel07019** 3 years, 3 months ago

Answer is C

upvoted 1 times

👤 **GowherMalik** 3 years, 7 months ago

CSRF CSRF CSRF CSRF

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 93 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 93

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted
- D. Black Hat

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [Qutie](#) at March 20, 2021, 3:49 p.m.

Comments

 [callmetodd](#) Highly Voted 2 years, 8 months ago

simplify ... you take a black hat ... mix it with a white hat... you get gray hat ;)
upvoted 8 times

 [tmp14r](#) Most Recent 1 year, 4 months 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, 7 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](#) 2 years ago

Selected Answer: C
Answer is C
upvoted 1 times

 [SquidyP](#) 2 years, 6 months 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, 8 months ago

C is correct
upvoted 1 times

 [Osen](#) 2 years, 8 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, 9 months ago

D or C??

upvoted 1 times

ANDRESCB1988 2 years, 10 months ago

Gray Hat is correct

upvoted 2 times

Kamal_SriLanka 2 years, 10 months ago

Answer is D

upvoted 1 times

beowolf 2 years, 11 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, 8 months ago

they are effectively known as purple hats :)

<https://ipcisco.com/types-of-hackers/>

upvoted 1 times

jnagl13 2 years, 11 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 3 years, 2 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

EXAM 312-50V10 TOPIC 1 QUESTION 189 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 189

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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.

[Hide Answer](#)

Suggested Answer: C

by  [Benojojo](#) at March 20, 2021, 4:41 p.m.

Comments

 [Benojojo](#) 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

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 131 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 131

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**

C. Command and control

D. Exploitation

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  Mdean at April 5, 2021, 11:05 a.m.

Comments

  Mdean **Highly Voted** 3 years, 7 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 3 years, 1 month ago

A prefect explanation. B Weaponization
upvoted 4 times

  Jude2021 **Highly Voted** 3 years, 4 months ago

option B, Weaponization
upvoted 8 times

  ostorgaf **Most Recent** 1 year, 3 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

  MK1230ne 1 year, 4 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, 6 months 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, 7 months ago

Selected Answer: B

B. Weaponization

upvoted 2 times

✉ **piccolopersiano** 1 year, 7 months ago

doc 50v11 pg 31. thus B

upvoted 1 times

✉ **Sri0908** 1 year, 8 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, 10 months ago

Selected Answer: B

coupling exploit with a backdoor into the deliverable payload...weaponization

upvoted 1 times

✉ **VOAKDO** 1 year, 10 months ago

Selected Answer: B

is "creating" right now.....B=weaponization.

upvoted 1 times

✉ **snemmani** 1 year, 11 months ago

Selected Answer: B

Weaponization it is since the victim has not received it.

upvoted 2 times

✉ **erpiri** 1 year, 11 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** 2 years ago

b is correct

upvoted 1 times

✉ **Daniel8660** 2 years, 1 month 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** 2 years, 2 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 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** 2 years, 1 month 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** 2 years, 2 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** 2 years, 2 months ago

Selected Answer: B

B is the correct answer
upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 170 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 170

Topic #: 1

[All 312-50v11 Questions]

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 FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.

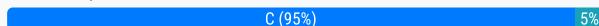
What is the port scanning technique used by Sam to discover open ports?

- A. Xmas scan
- B. IDLE/IPID header scan
- C. TCP Maimon scan Most Voted
- D. ACK flag probe scan

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (95%) 5%

by  [Mdean](#) at April 5, 2021, 1:02 p.m.

Comments

 [americaman80](#) Highly Voted 4 years, 7 months ago

C is the correct answer. Source:
<https://nmap.org/book/scan-methods-maimon-scan.html>
upvoted 18 times

 [naveedsajjad](#) 3 years, 9 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 FIN/ACK.
upvoted 2 times

 [Average_Joe](#) 3 years, 7 months ago

Did you even read what you posted?
upvoted 18 times

 [blacksheep6r](#) Highly Voted 4 years, 1 month 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 FIN/ACK. 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](#) 2 years, 4 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 1 year, 1 month ago

It is the TCP Maimon scan that uses FIN/ACK probe. The Ack flag probe scan uses Ack probe. Hence the Answer is C

upvoted 1 times

✉  **Vincent_Lu** 2 years, 3 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 FIN/ACK. 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, 6 months ago

Selected Answer: C

The correct option is C: tcp Maimon scan

upvoted 1 times

✉  **Bob_234** 2 years, 8 months ago

Selected Answer: D

it is D because he sends a ACK firts, 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** 3 years, 1 month ago

Selected Answer: C

TCP Maimon Scan - send FIN/ACK 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** 3 years, 2 months ago

Selected Answer: C

Correct answer is C, Maimon attack. Known for making use of FIN/ACK flags

upvoted 1 times

✉  **tinkerer** 3 years, 2 months ago

Selected Answer: C

Correct answer is C

upvoted 1 times

✉  **flinux** 3 years, 2 months ago

Selected Answer: C

The answer is C

upvoted 1 times

✉  **Fedrehopsu** 3 years, 3 months ago

Selected Answer: C

C is the answer

upvoted 1 times

✉  **cyberzzz** 3 years, 6 months ago

Selected Answer: C

That ' C for sure. Fin/Ack=Maimon

upvoted 2 times

✉  **andreigheorghiu** 3 years, 8 months ago

Selected Answer: C

answer is C

upvoted 1 times

✉  **Qudaz** 3 years, 9 months ago

Selected Answer: C

TCP Maimon Scan.

upvoted 1 times

✉  **APOLLO1113** 3 years, 10 months ago

it says FIN/ACK,, answer is TCP Maimon Scan

upvoted 1 times

✉  **egz21** 3 years, 10 months ago

the correct awnser is TCP-Maimon-Scan!!!

upvoted 1 times

 **cozy1970** 3 years, 10 months ago

Selected Answer: C

C is correct. Maimon Scan.

upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 1 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 1

Topic #: 3

[\[All 312-50 Questions\]](#)

Which of the following examples best represents a logical or technical control?

- A. Security tokens
- B. Heating and air conditioning
- C. Smoke and fire alarms
- D. Corporate security policy

[Hide Answer](#)

Suggested Answer: A

by  **Adbucket** at April 5, 2021, 4:51 p.m.

Comments

 **Sbowo** 1 year, 4 months ago

B and C are physical control, only A is technical control
upvoted 2 times

 **Dezmond22** 1 year, 10 months ago

The question is not umiversal
upvoted 1 times

 **Adbucket** 2 years, 1 month ago

Not clear
upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 185 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 185

Topic #: 1

[All 312-50v11 Questions]

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. **Most Voted**
- 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.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution



by [americanaman80](#) at April 15, 2021, 5:33 p.m.

Comments

[mil1989](#) **Highly Voted** 2 years, 9 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, 11 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** 11 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](#) 1 year ago

Selected Answer: D

Really, the correct option is D
upvoted 1 times

[victorfs](#) 1 year ago

Selected Answer: A

The correct option is A!
You need identify the virus type, signature, name, etc
upvoted 1 times

[victorfs](#) 1 year ago

No, sorry. The correct option is D
upvoted 1 times

[White_T_10](#) 1 year 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 1 year, 2 months 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 1 year, 3 months ago

Selected Answer: A

D cannot identify the connection make by virus

upvoted 1 times

👤 cristina22 1 year, 4 months 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

👤 Charpazo 1 year, 4 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, 5 months 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, 5 months 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, 7 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, 7 months ago

A. Virustotal

upvoted 1 times

👤 Ligeti15 1 year, 10 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

👤 baybay 1 year, 7 months ago

I agree with this explanation.

upvoted 1 times

👤 TroyMcLure 1 year, 8 months ago

The best explanation so far. I totally agree!

Correct Answer: A

upvoted 1 times

👤 DuncanTu 2 years, 1 month ago

Selected Answer: A

Should 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 2 years, 2 months ago

Selected Answer: A

Easiest things first, so VirusTotal seems to be the easiest thing.
upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 164 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 164

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**

B. Zero-day malware

C. Phishing malware

D. Logic bomb malware

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  cerzocusp1 at April 17, 2021, 1:56 p.m.

Comments

 cerzocusp1 **Highly Voted** 2 years, 7 months ago

IDS/IPS has not reported on any non-whitelisted programs.

File-less malware

upvoted 9 times

 Animal22 **Highly Voted** 1 year, 5 months 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** 1 year, 1 month 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

 pinguin666 1 year, 4 months 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, 11 months ago

A. File-less malware

upvoted 1 times

 martco 2 years 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** 2 years, 1 month ago

No sense it can be a zero-day malware too.....

upvoted 3 times

✉ **whysoserious1199** 2 years, 3 months ago

File less malware and zero day both are correct.. depends on which answer ec council likes more..

upvoted 3 times

✉ **brdweek** 2 years, 1 month ago

IDS/IPS has not reported on any non-whitelisted programs

upvoted 2 times

✉ **M4E_55** 2 years, 3 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** 2 years, 1 month ago

in some cases it can detect based on behavior

upvoted 1 times

✉ **spydog** 2 years, 1 month 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** 2 years, 3 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** 2 years, 4 months ago

correct

upvoted 1 times

✉ **Grezavi** 2 years, 4 months ago

<https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html>

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 182 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 182

Topic #: 1

[All 312-50v11 Questions]

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?

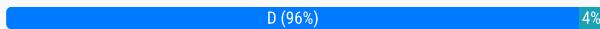
- A. Out of band and boolean-based
- B. Union-based and error-based
- C. Time-based and union-based
- D. Time-based and boolean-based

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by cerzocusp1 at April 18, 2021, 11:24 a.m.

Comments

noosa0707 **Highly Voted** 3 years, 4 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

cerzocusp1 **Highly Voted** 4 years, 1 month ago

D. Time-based and boolean-based

upvoted 21 times

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

Selected Answer: D

D. Time-based and boolean-based

upvoted 1 times

CHCHCHC 1 year, 9 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, 9 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, 10 months ago

Selected Answer: D

it is time based and boolean based

upvoted 1 times

👤 Naveen0x 1 year, 10 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, 10 months ago

Selected Answer: D

D. Time-based and boolean-based

upvoted 1 times

👤 victorfs 2 years ago

Selected Answer: D

The correct óptimo is D:

Time-based and boolean-based

upvoted 1 times

👤 Cokamaniako 2 years, 3 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 2 years, 4 months ago

Selected Answer: D

Answer is D, time based and boolean based

upvoted 2 times

👤 Examdaddy69 2 years, 4 months ago

Selected Answer: D

D is correct

upvoted 1 times

👤 kiki533 2 years, 7 months ago

D is correct

upvoted 1 times

👤 Daniel8660 2 years, 7 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, 8 months ago

Selected Answer: D

D.Time-based and boolean-based, is the answer

upvoted 2 times

👤 sn30 2 years, 8 months ago

Selected Answer: D

Answer is D, time based and boolean based

upvoted 1 times

👤 Fedrehopsu 2 years, 9 months ago

Selected Answer: D

Time and Boolean

upvoted 1 times

👤 CybeXRay 2 years, 10 months ago

Selected Answer: D

Time-based and boolean-based

upvoted 1 times

Exam 312-50V11 Topic 1 Question 194 Discussion

Actual exam question from ECCouncil's 312-50v11

Question #: 194

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**

B. Blind hijacking

C. UDP hijacking

D. Forbidden attack

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (74%)  B (26%)

by  cerzocusp1 at April 18, 2021, 12:50 p.m.

Comments

  cerzocusp1 **Highly Voted** 4 years, 1 month 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, 7 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

  BallCS **Most Recent** 10 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, 5 months 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, 9 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, 10 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** 2 years ago

Selected Answer: A

The correct option is A
TCP/IP hijacking
upvoted 1 times

✉ **Bob_234** 2 years, 2 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, 6 months 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, 6 months 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, 7 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, 7 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, 8 months ago

Keyword is predict so its blind
upvoted 2 times

✉ **Aisha86** 2 years, 8 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, 9 months ago

Selected Answer: A

the answer is A
upvoted 2 times

✉ **cazzobsb** 3 years, 1 month ago

Selected Answer: A

correct
upvoted 2 times

✉ **josek19** 3 years, 2 months ago

Selected Answer: A

See definitions. Blind is where the attacker does not see the responses
upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 214 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 214

Topic #: 1

[\[All 312-50v11 Questions\]](#)

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities.

Which phase of the vulnerability-management life cycle is David currently in?

A. Remediation Most Voted

B. Verification

C. Risk assessment

D. Vulnerability scan

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  cerzocusp1 at April 18, 2021, 2:11 p.m.

Comments

  cerzocusp1 Highly Voted 2 years, 7 months ago

Remediation

Remediation is the process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities.

upvoted 9 times

  Daniel8660 Most Recent 1 year, 1 month ago

Selected Answer: A

Vulnerability-Management Life Cycle

The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited.

4. Remediation - applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. (P.515/499)

upvoted 3 times

  ANDRESCB1988 2 years, 4 months ago

correct

upvoted 3 times

 EXAM 312-50V11 TOPIC 1 QUESTION 172 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 172

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**
- D. Exploiting SS7 vulnerability

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [Mento](#) at April 25, 2021, 5:23 p.m.

Comments

  [armangua](#) **Highly Voted**  2 years, 1 month 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**  1 year, 1 month 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

  [Khedyo007](#) 1 year, 4 months ago

C is correct answer

CEH Module 17 Page 2480

upvoted 2 times

  [ANDRESCB1988](#) 2 years, 4 months ago

correct

upvoted 1 times

  [Mento](#) 2 years, 7 months ago

<https://borwell.com/2018/09/06/ios-trustjacking/>

C indeed.

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 123 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 123

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Which of the following is a component of a risk assessment?

A. Administrative safeguards Most Voted

B. Physical security

C. DMZ

D. Logical interface

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [deleted] at May 24, 2021, 7:13 p.m.

Comments

 **Average_Joe** Highly Voted 1 year, 1 month 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

 **fhamke** Most Recent 1 year, 1 month 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, 10 months ago

correct, option A

upvoted 1 times

 **UrItem** 1 year, 3 months ago

why? don't say CORRECT, explain please!

upvoted 5 times

EXAM 312-50V11 TOPIC 1 QUESTION 7 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 7

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [noxspill](#) at June 2, 2021, 4:07 p.m.

Comments

✉  [aboru](#) 3 months, 3 weeks ago

Selected Answer: D

PKI (Public Key Infrastructure) is a framework used to manage digital certificates and public-private key pairs.

Purpose: It establishes trust online by verifying identities, enabling secure encryption, and ensuring integrity in data exchange.

upvoted 1 times

✉  [hunain456](#) 3 months, 3 weeks ago

Selected Answer: D

A Public Key Infrastructure (PKI) is a framework of policies, procedures, hardware, and software that enables the secure exchange of information. It uses asymmetric cryptography, also known as public-key cryptography, to verify and authenticate the identity of individuals and systems.

upvoted 1 times

✉  [Rafi9599](#) 1 year, 5 months ago

Selected Answer: D

PKI is the correct answer.

upvoted 1 times

✉  [Daniel8660](#) 1 year, 7 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, 9 months ago

Selected Answer: D

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

upvoted 2 times

✉  [Pranay_Doge](#) 1 year, 10 months ago

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

upvoted 3 times

✉  [Dnd](#) 2 years, 9 months ago

Agreed,

PKI are use verify and authenticate the identity of individuals within the enterprise
upvoted 1 times

 **noxspill** 2 years, 12 months ago

D is correct.

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 115 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 115

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**
- D. Ask students to use the wireless network

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  noxspill at June 2, 2021, 4:44 p.m.

Comments

  **beowulf** **Highly Voted** 3 years, 5 months 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** **Highly Voted** 3 years, 2 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** 1 year, 4 months ago

Scryptic, every comment you write is clear and correct. Big up man, I'm a fan.

upvoted 1 times

  **Daniel8660** **Most Recent** 2 years, 1 month 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

  **Sax80** 3 years, 1 month 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** 3 years, 4 months ago

correct, option C

upvoted 2 times

✉  **gtluscia** 3 years, 5 months ago

C - access control, not A because the professors and authorised visitors need to have access

upvoted 3 times

✉  **ANDRESCB1988** 3 years, 5 months 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 autentiquen para validar si tienen permisos de usar la red o no.

upvoted 5 times

✉  **Osen** 3 years, 1 month 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, 5 months ago

Why not A?

upvoted 1 times

✉  **noxspill** 3 years, 5 months ago

Why not the answer is A. Disable unused ports in the switches?

upvoted 2 times

✉  **TMoch** 3 years, 3 months ago

Disabling unused ports can prevent authorized users such as professors from connecting to the wifi

upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 27 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 27

Topic #: 3

[\[All 312-50 Questions\]](#)

What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

- A. Blue Book
- B. ISO 26029
- C. Common Criteria
- D. The Wassenaar Agreement

[Hide Answer](#)

Suggested Answer: C

by  [Indushack](#) at June 5, 2021, 4:43 p.m.

Comments

  [dorinh](#) 12 months ago

Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) in a Security Target (ST), and may be taken from Protection Profiles (PPs). Vendors can then implement or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 39 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 39

Topic #: 4

[\[All 312-50 Questions\]](#)

Smart cards use which protocol to transfer the certificate in a secure manner?

- A. Extensible Authentication Protocol (EAP)
- B. Point to Point Protocol (PPP)
- C. Point to Point Tunneling Protocol (PPTP)
- D. Layer 2 Tunneling Protocol (L2TP)

[Hide Answer](#)

Suggested Answer: A

by  [Indushack](#) at June 6, 2021, 3:08 a.m.

Comments

  [Indushack](#) 11 months, 4 weeks ago

The Extensible Authentication Protocol (EAP) is a protocol for wireless networks that expands the authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the internet. EAP is used on encrypted networks to provide a secure way to send identifying information to provide network authentication. It supports various authentication methods, including as token cards, smart cards, certificates, one-time passwords and public key encryption.

upvoted 3 times

EXAM 312-50 TOPIC 4 QUESTION 73 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 73

Topic #: 4

[\[All 312-50 Questions\]](#)

Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP

B. Nikto

C. Ike-scan

D. Arp-scan

[Hide Answer](#)

Suggested Answer: C

by  [Indushack](#) at June 6, 2021, 3:59 a.m.

Comments

  [Indushack](#) 11 months, 3 weeks ago

ike-scan is a command-line IPSec VPN Scanner & Testing Tool for discovering, fingerprinting and testing IPsec VPN systems. It constructs and sends IKE Phase-1 packets to the specified hosts, and displays any responses that are received.

upvoted 3 times

EXAM 312-50 TOPIC 4 QUESTION 74 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 74

Topic #: 4

[\[All 312-50 Questions\]](#)

What is a successful method for protecting a router from potential smurf attacks?

- A. Placing the router in broadcast mode
- B. Enabling port forwarding on the router
- C. Installing the router outside of the network's firewall
- D. Disabling the router from accepting broadcast ping messages

[Hide Answer](#)

Suggested Answer: D

by  Indushack at June 6, 2021, 4:02 a.m.

Comments

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

EXAM 312-50V11 TOPIC 1 QUESTION 239 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 239

Topic #: 1

[All 312-50v11 Questions]

John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to one of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation.

What is the type of vulnerability assessment tool employed by John in the above scenario?

A. Agent-based scanner Most Voted

B. Network-based scanner

C. Cluster scanner

D. Proxy scanner

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (78%) B (22%)

by Suksitt at June 6, 2021, 5:43 a.m.

Comments

Ryan2019 Highly Voted 3 years, 5 months ago

Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.
upvoted 18 times

Haythem026 Highly Voted 3 years, 2 months ago

By referring to CEH V11 documentation the correct answer is : A

o Network-Based Scanner: Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.

o Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.

o Proxy Scanner: Proxy scanners are the network-based scanners that can scan networks from any machine on the network.

o Cluster scanner: Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network.

upvoted 15 times

MH2 Most Recent 1 year, 2 months ago

Selected Answer: A

Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.
upvoted 2 times

victorfs 1 year, 6 months ago

Selected Answer: A

The correct option is A.

Agent-based

upvoted 1 times

Daniel8660 2 years, 1 month ago

Selected Answer: A

Location and Data Examination Tools

Agent-based scanners reside on a single machine but can scan several machines on the same network. (P.538/522)

upvoted 2 times

👤 **Blueteam** 2 years, 2 months ago

The Correct answer is Network based scan. You install the scanner on one machine and scan all the systems on the subnet through that scanner. Agent based scanner has an agent that is installed on each machine on the network.

upvoted 2 times

👤 **BIOLORENZ** 2 years, 3 months ago

Selected Answer: A

From CEHv11 material:

Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.

upvoted 1 times

👤 **StormCloak4Ever** 2 years, 4 months ago

Selected Answer: B

Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities.

NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

upvoted 2 times

👤 **Jong1** 2 years, 8 months ago

Selected Answer: A

A. - CEH p.538. It's clear

upvoted 1 times

👤 **TheDark** 2 years, 10 months ago

Another crappy CEH question - I wonder if we would need this info in our practical life

upvoted 7 times

👤 **Nassman** 3 years ago

You can install your agent on any machine and that scanner can scan the network or other machines. Nessus agent scanner works like this. Agent scanners can be installed on machines in networks that are behind firewalls or IDS that prohibit the scan through them. The agent would do the scan and return the results to the Nessus manager.

upvoted 1 times

👤 **ANDRESCB1988** 3 years, 4 months ago

the correct answer is B: Network based scanner

upvoted 4 times

👤 **Uchiha_Itachi8** 3 years, 4 months ago

simply Agent-based Nessus Scanner

upvoted 1 times

👤 **Kamal_SriLanka** 3 years, 4 months ago

Answer is B

upvoted 2 times

👤 **Uchiha_Itachi8** 3 years, 4 months ago

Wrong. Think in Nessus scanner

upvoted 1 times

👤 **Suksitt** 3 years, 5 months ago

I think Agent-based scanner is to install agent on host and scan vulnerabilities of the host send back to scanner, in this case attacker scanner entire network, The answer should be Network Scanner?

upvoted 2 times

👤 **Nassman** 3 years ago

You can install your agent on any machine and that scanner can scan the network or other machines. Nessus agent scanner works like this.

Agent scanners can be installed on machines in networks that are behind firewalls or IDS that prohibit the scan through them. The agent would do the scan and return the results to the Nessus manager.

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 167 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 167

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [ripple](#) at June 6, 2021, 9:30 a.m.

Comments

  [Daniel8660](#) 1 year, 1 month 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](#) 2 years, 4 months ago

correct

upvoted 2 times

  [ripple](#) 2 years, 5 months ago

D: Textbook example of a Honeypot

upvoted 2 times

EXAM 312-50 TOPIC 2 QUESTION 7 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 7

Topic #: 2

[\[All 312-50 Questions\]](#)

Which of the following lists are valid data-gathering activities associated with a risk assessment?

A. Threat identification, vulnerability identification, control analysis Most Voted

B. Threat identification, response identification, mitigation identification

C. Attack profile, defense profile, loss profile

D. System profile, vulnerability identification, security determination

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [Luukman](#) at June 10, 2021, 6:53 p.m.

Comments

  **dtwostar** 1 year, 2 months ago

Selected Answer: A

RISK = Threats x Vulnerabilities x Impact

The impact of an event on an information asset is the product of vulnerability in the asset and the asset's value to its stakeholders.
upvoted 1 times

  **Sbowo** 3 years, 4 months ago

I think its C because the question is risk assessment not risk identification, so C is the only option without identification term inside
upvoted 1 times

  **Luukman** 3 years, 11 months ago

Can anybody tell me why B is wrong?

upvoted 1 times

  **salei** 2 years, 4 months ago

I think identify what are the mitigation (tasks, tools, methods etc.) is beyond Risk Assessment

upvoted 1 times

EXAM 312-50 TOPIC 2 QUESTION 10 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 10

Topic #: 2

[\[All 312-50 Questions\]](#)

Which of the following is a component of a risk assessment?

- A. Physical security
- B. Administrative safeguards
- C. DMZ
- D. Logical interface

[Hide Answer](#)

Suggested Answer: B

by  Luukman at June 10, 2021, 7:06 p.m.

Comments

  HeyacedoGomez 1 year, 4 months ago

B is correct!

upvoted 1 times

  syntax3r 1 year, 7 months ago

">

upvoted 3 times

  dorinh 2 years, 6 months ago

The HIPAA Privacy Rule provides federal protections for the individually identifiable health information held by covered entities and their business associates and gives patients an array of rights to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other necessary purposes. The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to ensure the confidentiality, integrity, and availability of electronically protected health information

upvoted 4 times

EXAM 312-50 TOPIC 3 QUESTION 3 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 3

Topic #: 3

[\[All 312-50 Questions\]](#)

At a Windows Server command prompt, which command could be used to list the running services?

- A. Sc query type= running
- B. Sc query \\servername
- C. Sc query
- D. Sc config

[Hide Answer](#)

Suggested Answer: C

by  **Luukman** at June 10, 2021, 7:36 p.m.

Comments

 **Chogi_** 1 year, 3 months ago

Why not A.SC query type = running?
since list the running services?

upvoted 1 times

 **Luukman** 4 years, 5 months ago

Correct, see <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/sc-query>
upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 132 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 132

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**
- C. High
- D. Low

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Alex0921](#) at June 14, 2021, 11:51 a.m.

Comments

 [Scryptic](#) **Highly Voted** 2 years, 2 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, 5 months 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** 1 year, 1 month 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](#) 2 years ago

This question was in the exam from Oct 2021

upvoted 5 times

 [Snipa_x](#) 2 years ago

@Silascarter did you pass?

upvoted 2 times

 [ANDRESCB1988](#) 2 years, 4 months ago

correct

upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 57 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 57

Topic #: 3

[\[All 312-50 Questions\]](#)

The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

- A. Asymmetric
- B. Confidential
- C. Symmetric
- D. Non-confidential

[Hide Answer](#)

Suggested Answer: A

by  [Luukman](#) at June 14, 2021, 3:43 p.m.

Comments

  [asadeyemo](#) 1 year, 5 months ago

Https uses TLS/SSL protocol to establish handshake and that relies on asymmetric (2 pairs of keys). However, during a TLS handshake, the client and server agree upon new keys to use for symmetric encryption, called "session keys". Each new communication session will start with a new TLS handshake and use new session keys.

upvoted 1 times

  [Luukman](#) 2 years, 11 months ago

Strange question.. think it should be: what type of encryption is used...
then the answer is symmetric. (Only the sessionkey is done with asymmetric)

upvoted 2 times

  [Acidscars](#) 1 year, 6 months ago

Agreed, a very poorly worded question. The second part seems to hint that the answer is symmetric, but the first part clearly says certificate which is asymmetric. It's pretty much a coin toss, but what's clear is the person who wrote this question should be maimed beyond recognition.
upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 32 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 32

Topic #: 1

[\[All 312-50v11 Questions\]](#)

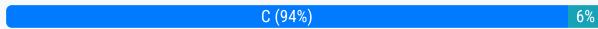
Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

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

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by [beowulf](#) at June 15, 2021, 3:54 a.m.

Comments

alodha100 1 year, 2 months ago

Except c all others are valid
upvoted 1 times

DataTraveler 1 year, 8 months ago

Selected Answer: C
See Appendix B p.3339/3355
upvoted 1 times

akailah88 1 year, 9 months ago

C correct , the question say least-likely physical characteristic to be used
the lest is heigh and weight
upvoted 1 times

Jshears 2 years ago

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

xXMikeXx 2 years, 1 month ago

Selected Answer: C
Height and Weight don't define how you are
upvoted 3 times

Chamod_Ridmal 2 years, 2 months ago

Selected Answer: C
Height and Weight is correct
upvoted 2 times

kiki533 2 years, 7 months ago

Selected Answer: C
C is the answer
upvoted 2 times

Isharafaz 2 years, 8 months ago

Selected Answer: C
C is correct

upvoted 2 times

✉  **baskan** 2 years, 9 months ago

C, Read carefully.

upvoted 1 times

✉  **45382456** 2 years, 9 months ago

Selected Answer: C

C is correct, height and weight can change

upvoted 3 times

✉  **ritviksharma3** 2 years, 10 months ago

Selected Answer: C

C is correct

upvoted 1 times

✉  **darkos73** 2 years, 10 months ago

Selected Answer: C

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

upvoted 2 times

✉  **ag6ag** 2 years, 10 months ago

Selected Answer: D

height and weight might change

upvoted 1 times

✉  **gogo78** 3 years, 3 months ago

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

upvoted 1 times

✉  **peace_iron** 3 years, 4 months ago

C is correct

upvoted 1 times

✉  **jtan97** 3 years, 6 months ago

H & W changes overtime.

upvoted 2 times

✉  **Brinhosa** 3 years, 9 months ago

Height and Weight could cause a sense of discrimination and could easily change from time to time.

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 88 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 88

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: A

by  [Nufforabing](#) at June 28, 2021, 3:36 p.m.

Comments

  [Nufforabing](#)  2 years, 11 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](#)  1 year, 2 months 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, 10 months ago

correct

upvoted 4 times

  [marcoatv](#) 1 year, 9 months ago

All you say is "Correct" and have nothing to contribute

upvoted 9 times

  [MyName7](#) 1 year, 9 months ago

you made my day with your second comment!

upvoted 4 times

EXAM 312-50V11 TOPIC 1 QUESTION 121 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 121

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**

C. Shared

D. Root

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Nufforabing](#) at June 28, 2021, 5:40 p.m.

Comments

  [Nufforabing](#) **Highly Voted** 3 years, 11 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

  [Seahorse66](#) **Highly Voted** 3 years 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** 1 year, 4 months ago

Selected Answer: B

B is correct answer

upvoted 1 times

  [juliosc](#) 2 years, 2 months ago

There is no sense of exposing a public Key

upvoted 1 times

  [Daniel8660](#) 2 years, 7 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, 6 months 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, 10 months ago

correct

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 120 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 120

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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 **Most Voted**
- B. Network sniffer
- C. Intrusion Prevention System (IPS)
- D. Vulnerability scanner

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [ms200](#) at July 5, 2021, 1:38 p.m.

Comments

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

Great job you are doing in all your explanations. Thanks
upvoted 7 times

  **Daniel8660** **Highly Voted**  1 year, 1 month 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

  **UrItemm** **Most Recent**  1 year, 9 months ago

WireShark is enough for all tasks....
upvoted 2 times

  **ANDRESCB1988** 2 years, 4 months ago

correct
upvoted 1 times

  **Tara8595** 2 years, 4 months ago

Protocol analyzer = Packet sniffer
upvoted 4 times

  **brdweek** 2 years, 3 months ago

yea
Protocol analyzer is in Packet sniffer
hmm
upvoted 1 times

  **ms200** 2 years, 4 months ago

Not network sniffer?

upvoted 2 times

 **spydog** 2 years, 1 month 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

EXAM 312-50V11 TOPIC 1 QUESTION 30 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 30

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted

D. Non-Disclosure Agreement

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [baneador](#) at July 6, 2021, 4:33 a.m.

Comments

✉  **Daniel8660** 1 year, 1 month ago

Selected Answer: C

Rules of Engagement (ROE)

Formal permission to conduct penetration testing.

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

upvoted 4 times

✉  **CodexFT** 1 year, 4 months ago

Selected Answer: C

For pentesting is Rule of Engagement.

upvoted 1 times

✉  **EngrSu** 1 year, 5 months ago

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

upvoted 1 times

✉  **davidjec** 1 year, 7 months ago

I will suggest D: NDA

upvoted 1 times

✉  **baneador** 2 years, 4 months ago

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

upvoted 2 times

✉  **study_Somuch** 2 years, 3 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** 2 years, 3 months ago

Actually, I take that back, perhaps B is more appropriate? C seems too general
upvoted 1 times

 **Mr_Gray** 2 years, 2 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

EXAM 312-50 TOPIC 4 QUESTION 46 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 46

Topic #: 4

[\[All 312-50 Questions\]](#)

After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

- A. SHA1
- B. Diffie-Helman
- C. RSA
- D. AES

[Hide Answer](#)

Suggested Answer: A

by  [tailoredsuit](#) at July 9, 2021, 10:28 a.m.

Comments

-   **dorinh** 12 months ago
Since you have the password hashes, the only hashing algorithm present in the answers is SHA1
upvoted 1 times
-   **tailoredsuit** 1 year, 4 months ago
is this question for real?
upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 119 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 119

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Jude2021](#) at July 18, 2021, 2:12 a.m.

Comments

  [Daniel8660](#) 1 year, 1 month 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, 5 months 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](#) 2 years, 4 months ago

correct

upvoted 2 times

  [Jude2021](#) 2 years, 4 months ago

correct

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 81 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 81

Topic #: 1

[All 312-50v11 Questions]

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. **Most Voted**
- 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.

[Hide Answer](#)

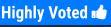
Suggested Answer: B

Community vote distribution

B (100%)

by  ANDRESCB1988 at July 23, 2021, 5:30 a.m.

Comments

  **Jong1**  2 years, 2 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**  1 year, 3 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, 10 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 90 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 90

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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.

Most Voted

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.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  ANDRESCB1988 at July 23, 2021, 5:31 a.m.

Comments

 **VOAKDO** 1 year, 10 months ago

Selected Answer: A

at least audits,... never is enough security.

upvoted 2 times

 **brdweek** 3 years, 2 months ago

A is correct

upvoted 2 times

 **study_Somuch** 3 years, 2 months ago

It seems A is the best answer. No sec config is perfect.

upvoted 3 times

 **brdweek** 3 years, 3 months ago

Why not B?

upvoted 1 times

 **shiftry** 3 years ago

There is not such thing like "complete restrict access". You have the Datacenter operators and technicians, even people from the company. All of them can be insider threats. You need to test periodical this security, for that you need to audit.

upvoted 1 times

 **AjaxFar** 2 years, 10 months ago

You be comedian, why it go be B

upvoted 1 times

 **Keapa_a** 1 year, 9 months ago

Hahaha....Bros! I tire o

upvoted 1 times

 **Brinhosa** 3 years, 3 months ago

Why not D?

upvoted 1 times

✉  **nick526** 2 years, 9 months ago

thats what i thought, i guess option D comes after implementing option A

upvoted 4 times

✉  **JT95** 1 year, 9 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

✉  **Forrest43** 1 year, 4 months 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

✉  **ANDRESCB1988** 3 years, 4 months ago

correct

upvoted 1 times

✉  **kianzz** 2 years, 4 months ago

your input provide no contribution.

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 91 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 91

Topic #: 1

[All 312-50v11 Questions]

PGP, SSL, and IKE are all examples of which type of cryptography?

- A. Digest
- B. Secret Key
- C. Public Key **Most Voted**
- D. Hash Algorithm

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  ANDRESCB1988 at July 23, 2021, 5:34 a.m.

Comments

 **Average_Joe** **Highly Voted** 1 year, 7 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** 11 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** 11 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** 11 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** 1 year, 1 month 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, 8 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** 2 years, 4 months ago

correct

upvoted 2 times

✉️👤 **marcoaty** 1 year, 3 months ago

Of course you are correct, as always

upvoted 7 times

✉️👤 **MyName7** 1 year, 3 months ago

oh my God, can't stop laughing at your 3rd comment, you're great

upvoted 5 times

EXAM 312-50V11 TOPIC 1 QUESTION 95 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 95

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by ANDRESCB1988 at July 23, 2021, 5:35 a.m.

Comments

peace_iron Highly Voted 2 years, 10 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 Most Recent 1 year, 5 months 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, 6 months ago

Selected Answer: D

The option correct is D: Cloud-based
upvoted 1 times

qovert 1 year, 8 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, 9 months ago

Selected Answer: D

it's D
upvoted 2 times

josevirtual 2 years ago

Selected Answer: D

Cloud-based, it is done in cloud, not on-premise
upvoted 2 times

-  **baskan** 2 years, 3 months ago
D. Cloud base .
upvoted 1 times
-  **noblethic** 2 years, 5 months ago
Selected Answer: D
The actual analysis is performed in the provider's cloud.
upvoted 2 times
-  **noblethic** 2 years, 5 months ago
Selected Answer: C
C. The actual analysis is performed in the provider's cloud.
upvoted 1 times
-  **Grey975** 2 years, 4 months ago
That is answer D.
upvoted 3 times
-  **cazzobsb** 2 years, 7 months ago
Selected Answer: D
Correct
upvoted 1 times
-  **iqrhaq** 2 years, 8 months ago
Selected Answer: D
If you google, a lot of the information points to Cloud-based.
upvoted 2 times
-  **Jong1** 2 years, 8 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, 9 months ago
Selected Answer: A
It sound like a xRD to me, so i will say A.
upvoted 2 times
-  **martco** 3 years 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** 3 years ago
SO what is the answer now A or D
upvoted 1 times
-  **blacksheep6r** 3 years, 1 month 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, 11 months ago
does this answer has something to do with the actual question?
upvoted 3 times
-  **Mr_Gray** 3 years, 1 month ago
what makes this correct? do you have any basis? why not Hueristic since that detection is smart enough to think.
upvoted 1 times
-  **spydog** 3 years, 1 month ago
The key here is that question saying the "analysis of the file is done on provider environment", not locally on the system. Heuristic is done locally.
upvoted 8 times
-  **Mr_Gray** 3 years, 1 month ago

good point. Thank you spydog
upvoted 2 times

 EXAM 312-50V11 TOPIC 1 QUESTION 96 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 96

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**

B. Nessus

C. OpenVAS

D. tcptraceroute

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  ANDRESCB1988 at July 23, 2021, 5:36 a.m.

Comments

  **kiki533** 1 year ago

tcptrace

upvoted 1 times

  **StormCloak4Ever** 1 year, 4 months 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

  **Seahorse66** 1 year, 6 months 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 received, 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** 2 years, 1 month ago

please give insight

upvoted 1 times

  **spydog** 2 years, 1 month 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** 2 years, 4 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 99 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 99

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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.

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  ANDRESCB1988 at July 23, 2021, 5:36 a.m.

Comments

  AleksVAnd 1 year, 2 months 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 1 year, 2 months ago

Selected Answer: D

correct

upvoted 1 times

  ANDRESCB1988 1 year, 10 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 100 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 100

Topic #: 1

[All 312-50v11 Questions]

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.

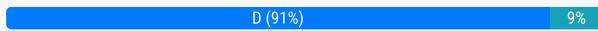
What should you do?

- 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. **Most Voted**

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by ANDRESCB1988 at July 23, 2021, 5:36 a.m.

Comments

Bwutch **Highly Voted** 1 year, 11 months ago

I can't even believe folks are suggesting anything other than D lol
upvoted 11 times

thamior666 **Most Recent** 1 year, 6 months 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, 6 months ago

Selected Answer: D
There is not any other possibility that go to the legal authorities immediately.
upvoted 3 times

Gerasz87 2 years, 1 month 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

djaBSNYVXSHGX 2 years, 1 month ago

is D, human traffic can't be superseeded by business ! Don't tell me something different !
upvoted 3 times

davidjec 2 years, 1 month 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 2 years, 1 month ago

Selected Answer: D
law should have the first priority
upvoted 2 times

✉️  **LexxxD** 2 years, 2 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, 6 months ago

Absolutely not!!!
You should tell the police ASAP. The sooner you do it, the better for the victims.
upvoted 2 times

✉️  **mrhaky** 2 years, 4 months ago

I believe he signed an NDA so the best answer is C
upvoted 2 times

✉️  **AleksVAnd** 2 years, 2 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, 5 months ago

The NDA should mention some exceptions...in this case Human trafficking is an exception.
upvoted 1 times

✉️  **study4test** 1 year, 7 months ago

If the activity is illegal, it is not covered by the NDA
upvoted 2 times

✉️  **Gerasz87** 2 years, 1 month 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, 10 months ago

correct
upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 102 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 102

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted
- C. RST
- D. SYN-ACK

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  ANDRESCB1988 at July 23, 2021, 5:37 a.m.

Comments

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

1. SYN -- client to server
 2. SYN-ACK --- server to client
 3. ACK --- client to server
- upvoted 8 times

 **avatar23** Most Recent 12 months ago

Selected Answer: B
Three way handshake:
SYN
SYN-ACK
ACK
upvoted 4 times

 **Daniel8660** 1 year, 1 month 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, 7 months ago

B is correct answer.
upvoted 2 times

 **ANDRESCB1988** 2 years, 4 months ago

correct
upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 103 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 103

Topic #: 1

[All 312-50v11 Questions]

Which type of security feature stops vehicles from crashing through the doors of a building?

A. Bollards **Most Voted**

B. Receptionist

C. Mantrap

D. Turnstile

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  ANDRESCB1988 at July 23, 2021, 5:37 a.m.

Comments

 **kdktrackers** **Highly Voted** 3 years, 3 months ago

And what does this has to do with Ethical Hacking :|
upvoted 15 times

 **lovalim** 3 years, 1 month ago

exactly
upvoted 1 times

 **Nagato** 3 years, 3 months ago

You hack it. Of course ethically.
upvoted 2 times

 **Forrest43** 1 year, 4 months ago

hacking bollards? lol
upvoted 1 times

 **noosa0707** 3 years ago

Probably in order to introduce a concept of safeguarding network
upvoted 1 times

 **ProveCert** 2 years, 11 months ago

Physical security is also a matter of concern from both malicious hackers and penetration tester's point of view
upvoted 5 times

 **Lee20** **Highly Voted** 2 years, 5 months 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** 1 year ago

Selected Answer: A

Bollards is correct. Physical security is important.
upvoted 1 times

 **AleksVAnd** 2 years, 8 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** 2 years ago

For me this question is about language, not about security
upvoted 2 times

 **ANDRESCB1988** 3 years, 4 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 104 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 104

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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 Most Voted
- 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

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  ANDRESCB1988 at July 23, 2021, 5:37 a.m.

Comments

  **S_raj** 1 year, 2 months 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, 8 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, 5 months ago

because the question is about the integrity of the file

upvoted 2 times

  **TRZ** 1 year, 11 months ago

Selected Answer: A

Correct - A

upvoted 1 times

  **artillery** 2 years, 1 month ago

Selected Answer: A

'A' is the best answer

upvoted 2 times

  **ANDRESCB1988** 2 years, 10 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 105 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 105

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted
- C. To provide a place to put the honeypot
- D. To contain the network devices you wish to protect

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  ANDRESCB1988 at July 23, 2021, 5:37 a.m.

Comments

 **victorfs** 1 year 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, 7 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, 11 months ago

Selected Answer: B

Correct - B

upvoted 3 times

 **ANDRESCB1988** 2 years, 10 months ago

correct

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 106 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 106

Topic #: 1

[All 312-50v11 Questions]

Which of the following Linux commands will resolve a domain name into IP address?

A. >host -t a hackeddomain.com **Most Voted**

B. >host -t ns hackeddomain.com

C. >host -t soa hackeddomain.com

D. >host -t AXFR hackeddomain.com

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  ANDRESCB1988 at July 23, 2021, 5:37 a.m.

Comments

 **spydog**  2 years, 1 month 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

 **Daniel8660**  1 year, 1 month ago

Selected Answer: A

host -t a hackeddomain.com

With option "-t" you can specify the type of the DNS request.

upvoted 4 times

 **Novmejst** 1 year, 11 months ago

A. host -t a hackeddomain.com

upvoted 3 times

 **AjaxFar** 1 year, 11 months ago

A host -a i e for ipvs4 type

upvoted 2 times

 **ANDRESCB1988** 2 years, 4 months ago

correct

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 108 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 108

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by  ANDRESCB1988 at July 23, 2021, 5:38 a.m.

Comments

  **msnarf** Highly Voted 2 years, 1 month ago

Is this a relevant question for non US citizens?
upvoted 5 times

  **victorfs** 1 year ago

Not, but is include in the exam!
You need know It!
upvoted 1 times

  **Daniel8660** Most Recent 1 year, 7 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, 6 months ago

NIST SP 800-53 is Assessing Security and Privacy Controls in Federal Information Systems and Organizations.
upvoted 2 times

  **ANDRESCB1988** 2 years, 10 months ago

correct
upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 113 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 113

Topic #: 1

[All 312-50v11 Questions]

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

- A. nessus
- B. tcpdump **Most Voted**
- C. ethereal
- D. jack the ripper

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by ANDRESCB1988 at July 23, 2021, 5:39 a.m.

Comments

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

Selected Answer: B

Keyword - command line - B is correct answer. Ethereal has a GUI like wireshark not CLI
upvoted 5 times

Urldenm 2 years, 3 months ago

totally agree!
upvoted 1 times

Yovecio **Most Recent** 1 year, 1 month 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, 6 months ago

Selected Answer: B
Tcpdump is correct
upvoted 1 times

Daniel8660 1 year, 7 months ago

Selected Answer: B
Tcpdump and Wireshark, to capture and analyze the packets. (P.2294/2278)
upvoted 2 times

TroyMcLure 1 year, 8 months ago

Selected Answer: B
No doubt
upvoted 1 times

romeo69 2 years, 3 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** 2 years, 4 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** 2 years, 4 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** 2 years, 4 months ago

Selected Answer: C

Answer is C. tcpdump is not GUI.

upvoted 1 times

✉ **SeaHOrse66** 2 years ago

The question is asking a Command Line Interface which tcpdump is, so tcpdump is correct

upvoted 3 times

✉ **peace_iron** 2 years, 4 months ago

The correct answer is Ethereal.

upvoted 2 times

✉ **peace_iron** 2 years, 4 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, 5 months ago

Tcpdump is just like wireshark only it works in cli so ethereal doe but different frt wireshark a bit

upvoted 1 times

✉ **eddyedward** 2 years, 5 months ago

Answer is C Ethereal. tcpdump is command line, and not the correct answer.

upvoted 2 times

✉ **mdmdmd** 1 year, 4 months 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, 10 months ago

correct

upvoted 3 times

 EXAM 312-50V11 TOPIC 1 QUESTION 116 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 116

Topic #: 1

[All 312-50v11 Questions]

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` Most Voted

B. `tcp.port == 23`

C. `tcp.port == 21 || tcp.port == 22`

D. `tcp.port != 21`

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  ANDRESCB1988 at July 23, 2021, 5:39 a.m.

Comments

 **cyberdonkey72** Highly Voted 3 years, 4 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** Highly Voted 3 years, 9 months ago

File Transfer Protocol Runs on port 21
`eq ==` Equal
upvoted 5 times

 **qwertyst100** Most Recent 1 year, 3 months ago

Selected Answer: A

A. `tcp.port == 21`
upvoted 1 times

 **MyName7** 2 years, 9 months ago

Note to me: Read the WHOLE question CAREFULLY!
upvoted 2 times

 **andrewdh** 3 years, 5 months ago

its c telnet (23) and ftp (21) are both unencrypted || is 'OR' Operator
upvoted 1 times

 **andrewdh** 3 years, 5 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, 10 months ago

correct
upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 125 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 125

Topic #: 1

[All 312-50v11 Questions]

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 **Most Voted**
- D. Bob is partially right. DMZ does not make sense when a stateless firewall is available

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by ANDRESCB1988 at July 23, 2021, 5:47 a.m.

Comments

M4E_55 **Highly Voted** 4 years, 3 months ago

Bob needs to find a new job soon. Correct answer C
upvoted 76 times

WillyWallace333 2 years, 1 month ago

CORRECT, LOL
upvoted 1 times

Snipa_x 4 years ago

Lmaoo....
upvoted 3 times

YourFriendlyNeighborhoodSpider 2 years ago

hahaha
upvoted 1 times

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

Bob probably got his certification using only the dumps. You see the irony here.
upvoted 51 times

CanORage 4 years, 2 months ago

Lol, brilliant comment
upvoted 5 times

blehbleh **Most Recent** 12 months 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 2 years, 1 month 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, 6 months 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, 6 months 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, 8 months ago

Selected Answer: C

C is correct
upvoted 1 times

✉ **Shin_Frankie** 2 years, 9 months ago

Selected Answer: C

DMZ separates network
upvoted 1 times

✉ **karloska2015** 3 years ago

Correct answer is C ...
upvoted 1 times

✉ **jartavia05** 3 years, 1 month 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** 3 years, 2 months ago

Selected Answer: C

The official answer needs to be fixed ASAP.
upvoted 5 times

✉ **Escltn** 3 years, 2 months ago

Selected Answer: C

A DMZ is always relevant when it comes to protecting an internal network
upvoted 2 times

✉ **Mileke** 3 years, 6 months ago

Selected Answer: C

Correct answer is C
upvoted 2 times

✉ **cazzobsb** 3 years, 7 months ago

Selected Answer: C

Correct.
upvoted 2 times

✉ **LexxxD** 3 years, 8 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

✉ **semeslim** 3 years, 9 months ago

Selected Answer: B

Correct answer B
upvoted 2 times

✉ **cozy1970** 3 years, 10 months ago

Bob can not prevent lateral movement.
C is correct.

upvoted 3 times

 EXAM 312-50V11 TOPIC 1 QUESTION 140 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 140

Topic #: 1

[All 312-50v11 Questions]

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 > Most Voted

C. nmap -sn -PA < target IP address >

D. nmap -sn -PP < target IP address >

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  ANDRESCB1988 at July 23, 2021, 5:50 a.m.

Comments

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

Just remember the "S" in -PS for SYN for this question.
upvoted 29 times

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

nmap -sn -PS < target IP address > is the right answer
upvoted 11 times

  **Daniel8660** Most Recent 1 year, 1 month 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, 5 months ago

Selected Answer: B

correct
upvoted 2 times

  **martco** 2 years 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** 2 years, 3 months ago

correct
upvoted 3 times

  **ANDRESCB1988** 2 years, 4 months ago

correct
upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 177 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 177

Topic #: 1

[All 312-50v11 Questions]

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 | grep site.com

B. curl -s https://site.com | grep | grep site.com | cut -d \> -f 2 **Most Voted**

C. dirb https://site.com | grep site

D. wget https://site.com | cut -d \http>

[Hide Answer](#)

Suggested Answer: B

Community vote distribution



by ANDRESCB1988 at July 23, 2021, 6:13 a.m.

Comments

ronxz **Highly Voted** 1 year, 11 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** 1 year ago

Selected Answer: B

The correct option is B

upvoted 1 times

victorfs 1 year ago

The correct option is B

upvoted 1 times

crimson_18 1 year, 2 months ago

Selected Answer: B

should be B

upvoted 1 times

flinux 1 year, 9 months ago

Selected Answer: B

the answer is B

upvoted 2 times

👤 **bsto** 1 year, 10 months ago

Selected Answer: B

Is the B.

upvoted 1 times

👤 **juan201061** 1 year, 10 months ago

Selected Answer: B

Is the B.

upvoted 2 times

👤 **Seahorse66** 2 years ago

Selected Answer: A

wget | grep "< a href=*http" | grep "site.com"

upvoted 1 times

👤 **cazzobsb** 2 years, 1 month ago

Selected Answer: B

correct

upvoted 1 times

👤 **Gilo** 2 years, 2 months ago

Selected Answer: B

Defo B

upvoted 1 times

👤 **UrItemm** 2 years, 2 months ago

I prefer B.

You will see whole list on your screen, just try it.

upvoted 1 times

👤 **gokhansah1n** 2 years, 3 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** 2 years, 3 months ago

Probably B

upvoted 1 times

👤 **SH_** 2 years, 3 months ago

Selected Answer: B

Try this out and see that the answer is B.

upvoted 1 times

👤 **spydog** 2 years, 3 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

👤 **andreiar** 2 years, 4 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, 5 months ago

Selected Answer: A

wget | grep "< a href=*http" | grep "site.com"

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 226 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 226

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Sam, a professional hacker, targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS IAM credentials and further compromise the employee's account.

What is the technique used by Sam to compromise the AWS IAM credentials?

- A. Insider threat
- B. Social engineering Most Voted
- C. Password reuse
- D. Reverse engineering

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  ANDRESCB1988 at July 23, 2021, 6:25 a.m.

Comments

 **Genesis777** 12 months ago

Social engineering is the correct answer. Reverse engineering is the process of analyzing and extracting the source code of a software or application and, if needed, regenerating it with required modifications.

upvoted 1 times

 **Daniel8660** 1 year, 1 month ago

Selected Answer: B

Pretends to be legitimate or an authorized person, and send an legitimate email acquire user account information.

upvoted 3 times

 **4everdzc9** 1 year, 6 months ago

D REVERSE ENGEENERING

upvoted 1 times

 **dinonino** 1 year, 2 months ago

social engineering

upvoted 2 times

 **ANDRESCB1988** 2 years, 4 months ago

correct

upvoted 4 times

EXAM 312-50V11 TOPIC 1 QUESTION 250 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 250

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Which of these is capable of searching for and locating rogue access points?

- A. NIDS
- B. HIDS
- C. WISS
- D. WIPS Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  ANDRESCB1988 at July 23, 2021, 6:30 a.m.

Comments

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

Source EC-Council C|EH v11 Courseware, page 2374:

WatchGuard WIPS

Source: <https://www.watchguard.com> WatchGuard WIPS defends against unauthorized devices and rogue Aps, prevents evil twins, and shuts down malicious attacks such as DoS attacks with close to zero false positives while ensuring high-performance wireless connectivity.

upvoted 11 times

  **Daniel8660** Most Recent 1 year, 1 month ago

Selected Answer: D

Wireless Security Tools - Wi-Fi IPSs

Wi-Fi IPSs block wireless threats by automatically scanning, detecting, and classifying unauthorized wireless access and rogue traffic to the network, thereby preventing neighboring users or skilled hackers from gaining unauthorized access to the Wi-Fi networking resources. (P.2374/2358)

upvoted 3 times

  **blacksheep6r** 2 years, 1 month ago

Wireless Intrusion Prevention Systems A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum to detect APs (intrusion detection) without the host's permission in nearby locations. It can also implement countermeasures automatically. WIPSs protect networks against wireless threats and provide administrators the ability to detect and prevent various network attacks.

EC-Council C|EH v11 Courseware, page 2369

upvoted 4 times

  **adespino** 2 years, 3 months ago

WIPS: Wireless Intrusion Prevention System

upvoted 3 times

  **ANDRESCB1988** 2 years, 4 months ago

correct

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 253 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 253

Topic #: 1

[All 312-50v11 Questions]

An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and

Virtual Private Networks (VPN) over a Frame Relay network.

Which AAA protocol is the most likely able to handle this requirement?

A. RADIUS **Most Voted**

B. Kerberos

C. DIAMETER

D. TACACS+

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  ANDRESCB1988 at July 23, 2021, 6:30 a.m.

Comments

 **Dam0s** 1 year, 5 months ago

A similar questions which I don't understand the answer to:

What can an Internet Service Provider (ISP) use to authenticate users?

A: Proxy Gateway

B: Content filter

C: Packet filter

D: Border router

Answer: B

I cannot see how content filter provides authentication, I would have said A: Proxy gateway

upvoted 1 times

 **Muli_70** 1 year, 6 months ago

The Diameter protocol is also an AAA protocol like RADIUS and TACACS+, but it is designed to overcome some of the limitations of RADIUS, particularly in terms of security and scalability. Diameter is an IETF standard protocol that supports a wide range of authentication, authorization, and accounting (AAA) applications, including network access and mobile IP. It has features such as Transport Layer Security (TLS) encryption, dynamic discovery of servers, and a flexible message structure that allow for greater security and scalability. Therefore, Diameter can also handle the requirement described in the question

upvoted 1 times

 **wenorex222** 1 year, 7 months ago

AAA services provided by the Diameter Protocol form the basis for service administration within the telecommunications industry, such as deciding which services a user can access, at what quality of service (QoS), and at what cost.

The Diameter Protocol focuses on the application layer. AAA nodes receive positive or negative acknowledgment for each message exchanged between nodes and TCP and SCTP ensure reliability.

A variety of LTE and IMS network functions make use of the Diameter Protocol, including the Policy and Charging Rules Function (PCRF), Home Subscriber Server (HSS), and Online Charging System (OCS) elements.

upvoted 1 times

 **Daniel8660** 2 years, 1 month ago

Selected Answer: A

Wi-Fi Authentication Process Using a Centralized Authentication Server

Wi-Fi authentication process, a centralized authentication server known as Remote Authentication Dial-in User Service (RADIUS) sends authentication keys to both the AP and the clients that attempt to authenticate with the AP. This key enables the AP to identify a particular wireless client. (P.2192/2176)

upvoted 1 times

✉️👤 **blacksheep6r** 3 years, 1 month ago

Remote Authentication Dial-In User Service (RADIUS) is an authentication protocol that provides centralized authentication, authorization, and accounting (AAA) for the remote access servers to communicate with the central server

Radius Authentication Steps: 1. The client initiates the connection by sending an Access-Request packet to the server

2. The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the Accept-Accept message along with the Access-Challenge to the client for additional authentication, otherwise it sends back the Accept-Reject message

upvoted 4 times

✉️👤 **ANDRESCB1988** 3 years, 4 months ago

correct

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 254 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 254

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

- A. Cannot deal with encrypted network traffic
- B. Requires vendor updates for new threats
- C. Can identify unknown attacks Most Voted
- D. Produces less false positives

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  ANDRESCB1988 at July 23, 2021, 6:30 a.m.

Comments

  **Daniel8660** 1 year, 1 month ago

Selected Answer: C

How an IDS Detects an Intrusion?

Anomaly Detection - Anomaly detection, or "not-use detection," differs from signature recognition. An anomaly is detected when an event occurs outside the tolerance threshold of normal traffic. Therefore, any deviation from regular use is an attack. Anomaly detection detects intrusions based on the fixed behavioral characteristics of the users and components in a computer system. (P.1480/1464)

upvoted 3 times

  **TroyMcLure** 1 year, 2 months ago

Selected Answer: C

An anomaly-based intrusion detection system, is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.

upvoted 1 times

  **egz21** 1 year, 10 months ago

thats correct!!!

upvoted 2 times

  **ANDRESCB1988** 2 years, 4 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 255 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 255

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Cross-site request forgery involves:

- A. A request sent by a malicious user from a browser to a server
- B. A server making a request to another server without the user's knowledge
- C. Modification of a request by a proxy between client and server.
- D. A browser making a request to a server without the user's knowledge

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  ANDRESCB1988 at July 23, 2021, 6:30 a.m.

Comments

  **Muli_70** 1 year ago

So, A is correct!?

A request sent by a malicious user from a browser to a server.

upvoted 1 times

  **Daniel8660** 1 year, 7 months ago

Selected Answer: D

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 4 times

  **Amios1** 2 years, 3 months ago

A browser is a client making a request to server. D

upvoted 3 times

  **egz21** 2 years, 4 months ago

I agree with the answer!!!

upvoted 1 times

  **Bot001** 2 years, 7 months ago

i agree

upvoted 2 times

  **ANDRESCB1988** 2 years, 10 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 256 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 256

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

- A. Maltego
- B. Wireshark
- C. Nessus
- D. Metasploit Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  ANDRESCB1988 at July 23, 2021, 6:30 a.m.

Comments

  Daniel8660 1 year, 1 month ago

Selected Answer: D

Web Server Attack Tools - Metasploit

The Metasploit Framework is an exploit development platform that supports fully automated exploitation of web servers, by abusing known vulnerabilities. (P.1680/1664)

upvoted 3 times

  pyw 1 year, 5 months ago

Selected Answer: D

since there is an EXPLOIT so the answer is Metasploit.

upvoted 2 times

  ANDRESCB1988 2 years, 4 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 259 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 259

Topic #: 1

[\[All 312-50v11 Questions\]](#)

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity. What tool would you most likely select?

A. Snort **Most Voted**

B. Cain & Abel

C. Nessus

D. Nmap

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  ANDRESCB1988 at July 23, 2021, 6:31 a.m.

Comments

  **Daniel8660** 1 year, 1 month ago

Selected Answer: A

Intrusion Detection Tools: Snort

Snort is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. Uses of Snort:1. Straight packet sniffer such as tcpdump2. Packet logger (useful for network traffic debugging, etc.)3. Network intrusion prevention system (P.1518/1502)

upvoted 3 times

  **ANDRESCB1988** 2 years, 4 months ago

correct

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 262 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 262

Topic #: 1

[\[All 312-50v11 Questions\]](#)

You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible

Intrusion Detection System. What is the best approach?

- A. Use Alternate Data Streams to hide the outgoing packets from this server.
- B. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.
- C. Install Cryptcat and encrypt outgoing packets from this server. Most Voted
- D. Install and use Telnet to encrypt all outgoing traffic from this server.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  ANDRESCB1988 at July 23, 2021, 6:32 a.m.

Comments

  **andrewdh** Highly Voted 3 years, 1 month ago

CryptCat is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol while encrypting the data being transmitted.
upvoted 9 times

  **Vincent_Lu** Most Recent 1 year, 1 month ago

Selected Answer: C

Explanation
Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish
upvoted 1 times

  **Hackeram** 1 year, 5 months ago

awesome thanks guys
upvoted 1 times

  **Daniel8660** 2 years, 1 month ago

Selected Answer: C
Employ a crypter such as BitCrypter to encrypt the Trojan to evade detection by firewalls/IDS. (P.904/888)
upvoted 4 times

  **ANDRESCB1988** 3 years, 4 months ago

correct
upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 274 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 274

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

A. PEM

B. ppp

C. IPSEC Most Voted

D. SET

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  ANDRESCB1988 at July 23, 2021, 6:34 a.m.

Comments

  **Daniel8660** 1 year, 1 month ago

Selected Answer: C

Internet Protocol Security (IPsec) uses Encapsulation Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) to secure communication between virtual private network (VPN) end points by authenticating and encrypting each IP packet of a communication session. 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 2 times

  **ANDRESCB1988** 2 years, 4 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 282 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 282

Topic #: 1

[All 312-50v11 Questions]

Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did Chandler use in this context?

A. Heuristic Analysis

B. Code Emulation Most Voted

C. Scanning

D. Integrity checking

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  ANDRESCB1988 at July 23, 2021, 6:35 a.m.

Comments

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

Virus Detection Methods

Scanning: Once a virus is detected, it is possible to write scanning programs that look for signature string characteristics of the virus

Integrity Checking: Integrity checking products work by reading the entire disk and recording integrity data that act as a signature for the files and system sectors

Interception: The interceptor monitors the operating system requests that are written to the disk

Code Emulation: In code emulation techniques, the antivirus executes the malicious code inside a virtual machine to simulate CPU and memory activities. These techniques are considered very effective in dealing with encrypted and polymorphic viruses if the virtual machine mimics the real machine

Heuristic Analysis: Heuristic analysis can be static or dynamic. In static analysis, the antivirus analyses the file format and code structure to determine if the code is viral. In dynamic analysis, the antivirus performs a code emulation of the suspicious code to determine if the code is viral

CEH: Malware Threats

upvoted 6 times

 **Daniel8660** Most Recent 1 year, 1 month ago

Selected Answer: B

Virus Detection Methods - Code Emulation

In code emulation techniques, the antivirus executes the malicious code inside a virtual machine to simulate CPU and memory activities. These techniques are considered very effective in dealing with encrypted and polymorphic viruses if the virtual machine mimics the real machine.
(P.1042/1026)

upvoted 3 times

 **AleksVAnd** 1 year, 7 months ago

Code Emulation is correct. The method described in the question is one of two. The other is to use a VM. Module 7 page 1026
However there's something to point out: heuristic analysis - dynamic analysis includes code emulation. So it is also a correct answer. Just not the best answer.

upvoted 4 times

 **ANDRESCB1988** 2 years, 4 months ago

correct

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 284 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 284

Topic #: 1

[All 312-50v11 Questions]

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned.

Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

- A. GET /restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1 Host: westbank.com
- B. GET /restricted/\r\n\%0account%00Ned%00access HTTP/1.1 Host: westbank.com
- C. GET /restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com Most Voted
- D. GET /restricted/ HTTP/1.1 Host: westbank.com

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  ANDRESCB1988 at July 23, 2021, 6:35 a.m.

Comments

  **BigMomma4752** Highly Voted 2 years, 8 months ago

The correct answer is C.

-GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com-
upvoted 14 times

  **Scryptic** 2 years, 8 months ago

Thanks for cleaning up the mess BugMomma
upvoted 3 times

  **Scryptic** 2 years, 8 months ago

BIGMomma. Sheesh, not BUGMomma!
upvoted 8 times

  **harp0202** Highly Voted 2 years, 3 months ago

Answer is C.

A. -GET /restricted/goldtransfer?to=Rob&from=1 or 1=1- HTTP/1.1 Host: westbank.com-
B. -GET /restricted/\r\n\%0account%00Ned%00access HTTP/1.1 Host: westbank.com-
C. -GET /restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com-
D. -GET /restricted/ HTTP/1.1 Host: westbank.com
upvoted 6 times

  **Muli_70** Most Recent 1 year ago

I think B is correct!!!!

The request that best illustrates an attempt to exploit an insecure direct object reference vulnerability is option B: "GET /restricted/rn\%0account%00Ned%00access HTTP/1.1 Host: westbank.com".

This request contains a null byte ("rn") that separates the "account" from "Ned" in the URL. This could potentially fool the application into treating "Ned" as an access control parameter, allowing Rob to access Ned's account without proper authorization. This technique is also known as a null byte injection attack.

Option A is an example of SQL injection, where an attacker tries to modify the query to retrieve unauthorized data. Option C is an example of parameter tampering, where an attacker tries to modify a parameter value to gain access to unauthorized data. Option D is an example of a generic request that does not appear to be targeting a specific resource or attempting to exploit a vulnerability.

upvoted 1 times

  **Daniel8660** 1 year, 7 months ago

Selected Answer: C

Bypassing IDOR via Parameter Pollution

Insecure direct object reference (IDOR) is a vulnerability that arises when developers disclose references to internal data enforcement objects such as database keys, directories, and other files, that can be exploited by an attacker to modify the references and gain unauthorized access to data.

EX: api.xyz.com/profile/user_id=654&user_id=321 (P.1950/1934)

upvoted 3 times

 **ANDRESCB1988** 2 years, 10 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 291 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 291

Topic #: 1

[All 312-50v11 Questions]

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed.

Which security policy must the security analyst check to see if dial-out modems are allowed?

- A. Firewall-management policy
- B. Acceptable-use policy
- C. Permissive policy
- D. Remote-access policy Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by ANDRESCB1988 at July 23, 2021, 6:36 a.m.

Comments

martco Highly Voted 3 years, 6 months ago

in my own experience this specific item is listed in the AUP, I'm reading one for a large govt dept right now lol

however in the CEH v11 materials...

"Remote-access policy -- defines who can have remote access and the access medium and remote access security controls" which says modem to me and

"Acceptable-use policy -- defines the acceptable use of system resources" which could be virtually anything incl use of modems

so for me both could be correct but if you're in the CEH gang it's "Remote-access policy"

upvoted 10 times

Spam_Protection Most Recent 1 year, 2 months ago

Selected Answer: D

You dial out to someone/something somewhere outside the network. The receiving end of the dial out device has access to the internal network.

upvoted 1 times

YourFriendlyNeighborhoodSpider 1 year, 6 months ago

Selected Answer: D

ChatGPT Answer:

D. Remote-access policy

The Remote-access policy typically outlines the rules and guidelines for remote connections to the network. Dial-out modems fall under the category of remote access, as they allow users to connect to the network from a remote location. Checking the Remote-access policy is crucial to determine whether the use of dial-out modems is permitted or prohibited according to the organization's security policies.

upvoted 1 times

sudowhoami 1 year, 7 months ago

Selected Answer: D

Remote Access Policy is the correct answer. Did some research and came up with this conclusion.

upvoted 2 times

Rocko1 1 year, 11 months ago

Selected Answer: D

Remote Access Policy: This type of policy typically covers any form of remote connection to the network, and a dial-out modem certainly falls under that category. It should outline what types of remote connections are allowed, under what circumstances, and who can approve them.

upvoted 2 times

✉ **victorfs** 2 years ago

Selected Answer: B

Could be "B"

upvoted 1 times

✉ **victorfs** 2 years ago

Selected Answer: D

The correct option is D or B, i think D!!

upvoted 1 times

✉ **victorfs** 2 years ago

But ... Could be "B" too

upvoted 1 times

✉ **avalon21** 2 years, 2 months ago

Sélect D

upvoted 1 times

✉ **josevirtual** 2 years, 4 months ago

Selected Answer: B

It says that the modem is installed, but no reference to the remote connection. Even if the modem is not used, it is not accepted, so so it should be Acceptable-use policy, that refers to the device itself

upvoted 1 times

✉ **cristina22** 2 years, 4 months ago

Selected Answer: B

Remote Access is a term used to describe the ability of someone outside of your organization to gain Access to your systems.

upvoted 1 times

✉ **heeren** 2 years, 7 months ago

Which security policy must the security analyst check to see if dial-out modems are allowed? Firewall-management policy. Remote-access policy. Permissive policy.

upvoted 1 times

✉ **Daniel8660** 2 years, 7 months ago

Selected Answer: D

Examples of Security Policies

Remote-access Policy - Defines who can have remote access, and the access medium and remote access security control. (P.3343/3327)

upvoted 3 times

✉ **xXMikeXx** 1 year, 8 months ago

Modem Dial-out can permit an inbound connection? I think this is the question. If dial-out permit inbound connection the i think is the D, but if not, Remote-access policy does not belong to any possibility.

upvoted 1 times

✉ **dinonino** 2 years, 8 months ago

IPsec talks about remote access policy via dialup

upvoted 2 times

✉ **Blueteam** 2 years, 9 months ago

Correct Answer is Acceptable-use policy.

Remote access policy is a document that outlines acceptable methods of remotely connecting to the internal network not out of the internal network.

upvoted 2 times

✉ **pyw** 2 years, 11 months ago

Selected Answer: D

remote policy is the answer

upvoted 1 times

✉ **mileke2** 3 years ago

Selected Answer: B

Answer is acceptable use policy

upvoted 2 times

✉ **Gerasz87** 3 years, 1 month ago

Selected Answer: B

"user from the IT department had a dial-out modem installed" --> is like to BYOD. And if it is, then the answer should be: "B", because the BYOD is under the AUP

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 295 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 295

Topic #: 1

[\[All 312-50v11 Questions\]](#)

On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service.

What is the name of the process by which you can determine those critical businesses?

A. Emergency Plan Response (EPR)

B. Business Impact Analysis (BIA) Most Voted

C. Risk Mitigation

D. Disaster Recovery Planning (DRP)

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  ANDRESCB1988 at July 23, 2021, 6:37 a.m.

Comments

  **Daniel8660** 1 year, 1 month ago

Selected Answer: B

Business Impact Analysis (BIA)

BIA is a systematic process that determines and evaluates the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency. (P.3384/3368)

upvoted 3 times

  **dinonino** 1 year, 2 months ago

The answer is in the question. BIA

upvoted 1 times

  **ANDRESCB1988** 2 years, 4 months ago

correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 301 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 301

Topic #: 1

[All 312-50v11 Questions]

Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

- A. msfpayload
- B. msfcli
- C. msfd
- D. msfencode **Most Voted**

[Hide Answer](#)

Suggested Answer: D

Community vote distribution



by ANDRESCB1988 at July 23, 2021, 6:38 a.m.

Comments

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

ok, MSFencode

but not a great question

tools like MSFencode (and MSFPayload) were replaced waaaay back in 2015 by MSFVenom

also I doubt very much that using MSFencode to bind your backdoor rig up to something ordinarily honest like Putty.exe would fool any modern AV context, really?

what timezone are we in here

upvoted 7 times

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

Please don't say 'correct', no one knows you

upvoted 6 times

victorfs **Most Recent** 1 year ago

Selected Answer: D

The correct option is D!

Msfencode

upvoted 1 times

Daniel8660 1 year, 7 months ago

Selected Answer: D

<https://kknews.cc/zh-tw/code/8vojl34.html>

upvoted 4 times

LoneStarChief 2 years, 7 months ago

The answer is correct: msfencode is an effective tool which encodes the shellcodes and makes them less detectable to antivirus.

upvoted 4 times

ANDRESCB1988 2 years, 10 months ago

correct

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 303 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 303

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

A. -T5 Most Voted

B. -O

C. -T0

D. -A

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  ANDRESCB1988 at July 23, 2021, 6:38 a.m.

Comments

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

-T5 = fastest scan (not to be confused with -F (fast scan) as it is fast because it scans for fewer ports.)

Make sure you know the other ones too.

-O = Operating System detection

-A = Aggressive Scan

-T0 = Paranoid Scan (Slowest)

upvoted 11 times

  **Daniel18660** Most Recent 1 year, 1 month ago

Selected Answer: A

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.

Nmap -T5 (-T<0-5>: Set timing template (higher is faster)) (P.332/316)

upvoted 4 times

  **Scryptic** 2 years, 2 months ago

Please don't say 'correct', no one knows you

upvoted 1 times

  **jinjection** 2 years, 2 months ago

-T5 Insane speed

upvoted 2 times

  **Yeeeeee** 2 years, 2 months ago

-T<0-5>: Set timing template (higher is faster)

upvoted 2 times

  **ANDRESCB1988** 2 years, 4 months ago

correct

upvoted 3 times

EXAM 312-50V10 TOPIC 1 QUESTION 15 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 15

Topic #: 1

[\[All 312-50v10 Questions\]](#)

You have successfully gained access to a Linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by

Network-Based Intrusion Detection Systems (NIDS).

What is the best way to evade the NIDS?

- A. Out of band signaling
- B. Protocol Isolation
- C. Encryption
- D. Alternate Data Streams

[Hide Answer](#)

Suggested Answer: C

by  [Jude2021](#) at July 30, 2021, 1:06 a.m.

Comments

  [Jude2021](#) 1 year, 4 months ago

C because encrypted are not inspected
upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 321 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 321

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: A

by  [RolandTam](#) at Sept. 17, 2021, 3:05 p.m.

Comments

  [RolandTam](#) 1 year, 2 months ago

329 questions?

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 319 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 319

Topic #: 1

[All 312-50v11 Questions]

Josh has finished scanning a network and has discovered multiple vulnerable services. He knows that several of these usually have protections against external sources but are frequently susceptible to internal users. He decides to draft an email, spoof the sender as the internal IT team, and attach a malicious file disguised as a financial spreadsheet. Before Josh sends the email, he decides to investigate other methods of getting the file onto the system.

For this particular attempt, what was the last stage of the cyber kill chain that Josh performed?

A. Weaponization **Most Voted**

B. Delivery

C. Reconnaissance

D. Exploitation

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (51%)

C (31%)

B (18%)

by  [8jinjection](#) at Sept. 27, 2021, 10:22 p.m.

Comments

 [Average_Joe](#) **Highly Voted** 3 years, 1 month ago

Talk about poorly written question. This shit's so unclear.
upvoted 20 times

 [Unitel21](#) **Highly Voted** 3 years, 6 months ago

The correct answer is C, the question asks for this particular attempt, what was the "last stage" of the cyber kill chain that Josh performed? First, he weaponized it but before delivering it, he decides to look for different methods of getting the file into the system (that's the last stage that he performed which is known as recon).

upvoted 11 times

 [AAronEE](#) 2 years, 10 months ago

Wrong. He was planning to, but did not achieve it before the stage weaponization. So weaponization is the best answer. I do get where you are going though.
upvoted 4 times

 [gayhat_hacker](#) **Most Recent** 9 months, 3 weeks ago

Selected Answer: A

Weaponization. He never attempted to send the email, so he didn't reach the Delivery stage. The last stage he completed was Weaponization. He is now in a new Reconnaissance stage, true, but the question asks about his particular attempt, and the only specific action we know of is drafting the email, which falls under Weaponization. Since the question refers to the last particular attempt, it wouldn't be Reconnaissance, as he is currently doing that, and we don't have any specific details about it.

upvoted 1 times

 [francislt9](#) 1 year, 1 month ago

Is C. It means "Before Josh sends the email, he decides to investigate ...", and then: "For this particular attempt, what was the last stage of...". So he goes back to Reconnaissance phase, C.
upvoted 1 times

 [YourFriendlyNeighborhoodSpider](#) 1 year, 6 months ago

Selected Answer: A

Weaponization

I think its the stage before sending the payload which is "weaponization" because they appointed that he drafted the email so he still in the "weaponization" stage didn't get to the "delivery" stage yet.

upvoted 2 times

✉️ **Cizzla7049** 1 year, 7 months ago

poorly worded question but seems like delivery to me. He is looking for other ways to deliver the malware since phishing might not work
upvoted 1 times

✉️ **Cizzla7049** 1 year, 7 months ago

On a 2nd thought, its probably recon because he has to investigate for weaknesses in their telemetry to hash out his delivery method
upvoted 1 times

✉️ **Ciruuss_** 1 year, 8 months ago

Selected Answer: A

Weaponization "Before Josh sends the email, he decides to investigate other methods of getting the file onto the system" He is not in delivery stage yet
upvoted 2 times

✉️ **victorf8** 2 years ago

Selected Answer: A

The correcto option is A. Weaponization
upvoted 2 times

✉️ **HadiCyA** 2 years, 1 month ago

I think its the stage before sending the payload which is "weaponization" because they appointed that he drafted the email so he still in the "weaponization" stage didn't get to the "delivery" stage yet.
upvoted 1 times

✉️ **Lemanico** 2 years, 1 month ago

Selected Answer: C

B or C. It's a bit confusing but he needs to reconnaise again to find new ways to delivery. So my answer is C
upvoted 1 times

✉️ **ounuomi** 2 years, 1 month ago

not clear what last stage means...
upvoted 1 times

✉️ **VOAKDO** 2 years, 4 months ago

Selected Answer: B

B: delivery
he is looking for the way of sending the file: " ..Before Josh sends the email, he decides to investigate other methods of getting the file onto the system"
upvoted 4 times

✉️ **mdmdmd** 2 years, 4 months ago

Selected Answer: B

Confused as well....but will still go with Delivery...he was looking for a way to get the file into the system I believe.
upvoted 3 times

✉️ **mdmdmd** 2 years, 4 months ago

Correction...The answer A is Weaponization...he was looking...never send it.....the last stage was that....
upvoted 2 times

✉️ **VOAKDO** 2 years, 4 months ago

B: delivery
he is looking for the way of sending the file: " ..Before Josh sends the email, he decides to investigate other methods of getting the file onto the system"
upvoted 1 times

✉️ **VOAKDO** 2 years, 4 months ago

B
keys: Before Josh sends the email, he decides to investigate other methods of getting the file onto the system (...DELIVERING WAYS...)
upvoted 1 times

✉️ **Kehsihba** 2 years, 5 months ago

Selected Answer: C

Recon is best answer
upvoted 3 times

✉️ **Gregman380** 2 years, 5 months ago

Selected Answer: C

I think this is C Reconnaissance. Before he sends the email he goes back to look for other ways to infiltrate the organization.
<https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/>
upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 327 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 327

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints.

What is the technique followed by Peter to send files securely through a remote connection?

A. VPN **Most Voted**

B. SMB signing

C. DMZ

D. Switch network

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [8 jinjection](#) at Sept. 27, 2021, 10:26 p.m.

Comments

  [Daniel8660](#) 1 year, 1 month ago

Selected Answer: A

VPN

Once the connection is established the client can securely access the company's network. (P.3365/3349)

upvoted 2 times

  [jinjection](#) 2 years, 2 months ago

Correct VPN

upvoted 4 times

EXAM 312-50V11 TOPIC 1 QUESTION 321 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 321

Topic #: 1

[All 312-50v11 Questions]

A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.

Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

A. .stm **Most Voted**

B. .cms

C. .rss

D. .html

[Hide Answer](#)

Suggested Answer: A

Community vote distribution



by [Scryptic](#) at Sept. 28, 2021, 12:57 a.m.

Comments

[Scryptic](#) **Highly Voted** 2 years, 8 months ago

A Web page with an ".stm" extension is an .HTM file that contains server side includes (SSI). These "includes" are directives that are processed by the Web server when the page is accessed by a user. They are used to generate dynamic content. SSI Web pages can be viewed as a standard HTML page in any browser.

upvoted 12 times

[victorfs](#) **Most Recent** 1 year ago

Selected Answer: A

The correct option is A.

Stm is asp files and they are vulns to SSI attacks

html is basic files!

upvoted 1 times

[GummyBear95](#) 1 year, 2 months ago

Got this question on the exam 21.02.23

upvoted 4 times

[Daniel18660](#) 1 year, 7 months ago

Selected Answer: A

Defend Against Injection Attacks - Server-Side Include Injection

Avoid using pages with file name extensions such as .stm, .shtm, and .shtml to prevent attacks. (P.1986/1970)

upvoted 4 times

[Benoit_G](#) 1 year, 8 months ago

Selected Answer: A

.stm

Correct answer

upvoted 1 times

[Benoit_G](#) 1 year, 8 months ago

"Another way to discover if the application is vulnerable is to verify the presence of pages with extension .stm, .shtm and .shtml"

[https://owasp.org/www-community/attacks/Server-](https://owasp.org/www-community/attacks/Server-SideIncludes_(SSI)_Injection#:~:text=The%20Server%2DSide%20Includes%20attack,use%20through%20user%20input%20fields)

[Side_Includes_\(SSI\)_Injection#:~:text=The%20Server%2DSide%20Includes%20attack,use%20through%20user%20input%20fields](https://owasp.org/www-community/attacks/Server-SideIncludes_(SSI)_Injection#:~:text=The%20Server%2DSide%20Includes%20attack,use%20through%20user%20input%20fields)

upvoted 1 times

👤 **Gerasz87** 2 years, 1 month ago

Selected Answer: A

stm

In order for a web server to recognize an SSI-enabled HTML file and therefore carry out these instructions, either the filename should end with a special extension, by default .shtml, .stm, .shtm, or, if the server is configured to allow this, set the execution bit of the file

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

[https://owasp.org/www-community/attacks/Server-Side_Includes_\(SSI\)_Injection](https://owasp.org/www-community/attacks/Server-Side_Includes_(SSI)_Injection)
upvoted 1 times

👤 **Li8tleOwl** 2 years, 2 months ago

Selected Answer: A

Avoid using pages with file name extensions such as .stm, .shtm, and .shtml to prevent attacks pg 1970 CEH official guide
upvoted 4 times

👤 **harp0202** 2 years, 3 months ago

A is correct.

The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields.
Another way to discover if the application is vulnerable is to verify the presence of pages with extension .stm, .shtm and .shtml.
(Reference: [https://owasp.org/www-community/attacks/Server-Side_Includes_\(SSI\)_Injection#:~:text=The%20Server%2DSide%20Includes%20attack,use%20through%20user%20input%20fields](https://owasp.org/www-community/attacks/Server-Side_Includes_(SSI)_Injection#:~:text=The%20Server%2DSide%20Includes%20attack,use%20through%20user%20input%20fields))
upvoted 4 times

👤 **B4RK3** 2 years, 3 months ago

Selected Answer: A

correct
upvoted 1 times

👤 **egz21** 2 years, 4 months ago

Selected Answer: D

Option is D) but .stm is an extensiom of html file
upvoted 1 times

👤 **egz21** 2 years, 5 months ago

thats correct , I share the next explanation:

[https://owasp.org/www-community/attacks/Server-Side_Includes_\(SSI\)_Injection#:~:text=The%20Server%2DSide%20Includes%20attack,use%20through%20user%20input%20fields](https://owasp.org/www-community/attacks/Server-Side_Includes_(SSI)_Injection#:~:text=The%20Server%2DSide%20Includes%20attack,use%20through%20user%20input%20fields).
upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 323 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 323

Topic #: 1

[All 312-50v11 Questions]

Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.

What is the encryption software employed by Sam for securing the email messages?

- A. PGP
- B. SMTP
- C. GPG **Most Voted**
- D. S/MIME

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  Scryptic at Sept. 28, 2021, 1:01 a.m.

Comments

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

C- GPG is likely the answer.

PGP is a software replacement of PGP and free implementation of the OpenPGP standard.
it uses both symmetric key cryptography and asymmetric key cryptography.

upvoted 15 times

 **Daniel8660** **Highly Voted** 1 year, 7 months ago

Selected Answer: C

GNU Privacy Guard (GPG) is a software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data.

GPG is also called a hybrid encryption software program, as it uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange, which is achieved using the receiver's public key for encrypting the session key. (P.3093/3077)

upvoted 5 times

 **victorfs** **Most Recent** 1 year ago

Selected Answer: C

The correct option is C

PGP

upvoted 1 times

 **pinguin666** 1 year, 10 months ago

Answer C: Page 3077 in Official EC council material .

GNU Privacy Guard (GPG) GNU Privacy Guard (GPG) is a software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data. GPG is also called a hybrid encryption software program, as it uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange, which is achieved using the receiver's public key for encrypting the session key. GPG also supports S/MIME and Secure Shell (SSH). The latest version of GPG supports most cryptographic functions such as elliptic curve cryptography (ECDSA, ECDH, and EdDSA), and it also supports the cryptography library Libgcrypt.

upvoted 1 times

 **stettin12** 2 years, 2 months ago

Selected Answer: C

PGP isn't free while GPG is.

upvoted 2 times

👤 **Cammie** 2 years, 2 months ago

GNU Privacy Guard (GPG) is a software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data. GPG is also called a hybrid encryption software program, as it uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange, which is achieved using the receiver's public key for encrypting the session key.

Ref: CEHv11 page 3077

upvoted 2 times

👤 **Qudaz** 2 years, 3 months ago

Selected Answer: C

Definitely GPG....

upvoted 2 times

👤 **nirankar69** 2 years, 5 months ago

Selected Answer: C

c IS THE CORRECT ANSWER WHICH USES both symmetric key and asymmetric key

upvoted 1 times

👤 **egz21** 2 years, 5 months ago

C. is the correct answer

upvoted 1 times

👤 **ProveCert** 2 years, 5 months ago

Selected Answer: C

GNU Privacy Guard (GnuPG or GPG) is a free-software replacement for Symantec's PGP cryptographic software suite. It is compliant with RFC 4880, the IETF standards-track specification of OpenPGP.

upvoted 1 times

👤 **leon8731** 2 years, 5 months ago

Selected Answer: C

C.GPG is correct

upvoted 1 times

👤 **critows** 2 years, 6 months ago

GPG is also called hybrid encryption software

upvoted 2 times

👤 **gtluscia** 2 years, 6 months ago

Selected Answer: C

Agree with Sam_Fyl and others that the answer is C

upvoted 3 times

👤 **martco** 2 years, 6 months ago

its GPG

wording of the scenario precisely per the official CEH v11 courseware

upvoted 3 times

👤 **Silascarter** 2 years, 6 months ago

GPG, or GnuPG, stands for GNU Privacy Guard. GPG is a different implementation of the Open PGP standard and a strong alternative to Symantec's official PGP software.

GPG is defined by RFC 4880 (the official name for the Open PGP standard). The GPG Project provides the tools and libraries to allow users to interface with a GUI or command line to integrate encryption with emails and operating systems like Linux. GPG can open and decrypt files encrypted by PGP or Open PGP, meaning it works well with other products.

C is Correct.

upvoted 2 times

👤 **alissonloyola** 2 years, 6 months ago

C. GPG is a software replacement of PGP and free implementation of the OpenPGP standard. Module 20 Page 3077.

upvoted 3 times

👤 **brdweek** 2 years, 6 months ago

C. GPG

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 330 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 330

Topic #: 1

[All 312-50v11 Questions]

Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks.

What is the technique employed by Kevin to improve the security of encryption keys?

A. Key stretching **Most Voted**

B. Public key infrastructure

C. Key derivation function

D. Key reinstallation

Hide Answer

Suggested Answer: A

Community vote distribution

A (100%)

by  **Scryptic** at Sept. 28, 2021, 1:17 a.m.

Comments

✉  **Scryptic** **Highly Voted** 3 years, 2 months ago

In cryptography, key stretching techniques are used to make a possibly weak key, typically a password or passphrase, more secure against a brute-force attack by increasing the resources (time and possibly space) it takes to test each possible key. Passwords or passphrases created by humans are often short or predictable enough to allow password cracking, and key stretching is intended to make such attacks more difficult by complicating a basic step of trying a single password candidate. Key stretching also improves security in some real-world applications where the key length has been constrained, by mimicking a longer key length from the perspective of a brute-force attacker.[1] https://en.wikipedia.org/wiki/Key_stretching#:~:text=In%20cryptography%2C%20key%20stretching%20techniques,to%20test%20each%20possible%20key.

upvoted 8 times

✉  **12787** **Most Recent** 1 year, 1 month ago

The technique employed by Kevin to improve the security of encryption keys, based on the information provided, is typically referred to as "Key Derivation." Key derivation is a cryptographic process used to derive a stronger and more secure key from an initial key or a passphrase. The goal is to create keys that are resistant to brute-force attacks and other cryptographic vulnerabilities. Answer is C

upvoted 2 times

✉  **steffBarj** 1 year, 4 months ago

C. Key Derivation function

upvoted 3 times

✉  **victorfs** 1 year, 6 months ago

Selected Answer: A

The correct option is A.

A. Key stretching

upvoted 1 times

✉  **Ayeshar** 1 year, 7 months ago

Key stretching is a technique used to enhance the security of cryptographic keys. It involves applying a one-way function, such as a hash function or a key derivation function, to a key multiple times in order to increase the time and resources required for an attacker to brute-force or guess the original key.

The idea behind key stretching is to make the key stronger by increasing its length and making it more random-looking. This makes it more difficult for an attacker to guess the original key, even if they have access to the encrypted data and the algorithm used to encrypt it.

upvoted 1 times

✉  **Bobbypizza** 2 years ago

Selected Answer: A

Described in other comments

upvoted 1 times

✉ **Daniel8660** 2 years, 1 month ago

Selected Answer: A

Key Stretching

Key stretching refers to processes used to make a weak key stronger, usually by making it longer. This technique helps in defending against brute-force attacks. In the key stretching technique, the initial key is given as input to an algorithm that generates an enhanced key. The key must be sufficiently resistant to brute-force attacks. (P.3137/3121)

upvoted 2 times

✉ **uday1985** 2 years, 1 month ago

A. Key stretching

key stretching (uncountable) (cryptography) Techniques used to make a key more secure against brute force attacks by increasing the resources needed to test each possible key.

upvoted 1 times

✉ **atsagar** 2 years, 2 months ago

Selected Answer: A

Key Stretching in correct answer.

check CEH v11 Module 20 Page 3121

upvoted 1 times

✉ **djaBSNYVXSHGX** 2 years, 7 months ago

Selected Answer: A

Key streching

upvoted 1 times

✉ **mrhaky** 2 years, 10 months ago

C he encrypted the checksum no the message to verify the content

upvoted 1 times

✉ **jinjection** 3 years, 2 months ago

Correct A

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 342 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 342

Topic #: 1

[All 312-50v11 Questions]

Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks.

What is the type of threat intelligence collected by Arnold in the above scenario?

- A. Strategic threat intelligence
- B. Operational threat intelligence Most Voted
- C. Technical threat intelligence
- D. Tactical threat intelligence

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [jinjection](#) at Sept. 28, 2021, 8:45 a.m.

Comments

  [AmadSyahir](#) Highly Voted 2 years ago

Tactical threat intelligence is the most basic form of threat intelligence. These are your common indicators of compromise (IOCs). Tactical intelligence is often used for machine-to-machine detection of threats and for incident responders to search for specific artifacts in enterprise networks.

Operational threat intelligence provides insight into actor methodologies and exposes potential risks. It fuels more meaningful detection, incident response, and hunting programs. Where tactical threat intelligence gives analysts context on threats that are already known, operational intelligence brings investigations closer to uncovering completely new threats.

Strategic threat intelligence provides a big picture look at how threats and attacks are changing over time. Strategic threat intelligence may be able to identify historical trends, motivations, or attributions as to who is behind an attack. Knowing the who and why of your adversaries also provides clues to their future operations and tactics. This makes strategic intelligence a solid starting point for deciding which defensive measures will be most effective.

upvoted 10 times

  [Daniel8660](#) Highly Voted 1 year, 1 month ago

Selected Answer: B

Cyber Threat Intelligence - Operational Threat Intelligence provides information about specific threats against the organization. It provides contextual information about security events and incidents that help defenders disclose potential risks, provide greater insight into attacker methodologies, identify past malicious activities, and perform investigations on malicious activity in a more efficient way. Operational threat intelligence generally appears as a report that contains identified malicious activities, recommended courses of action, and warnings of emerging attacks. (P.76/60)

upvoted 5 times

  [Silascarter](#) Most Recent 2 years ago

B is correct.

Operational threat intelligence is about uncovering specific incoming attacks before they happen. Most operational threat intelligence comes from closed sources, although some threat actors discuss their plans via social media or public chat rooms.

upvoted 2 times

  [jinjection](#) 2 years, 2 months ago

Correct

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 361 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 361

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Elante company has recently hired James as a penetration tester. He was tasked with performing enumeration on an organization's network. In the process of enumeration, James discovered a service that is accessible to external sources. This service runs directly on port 21.

What is the service enumerated by James in the above scenario?

- A. Network File System (NFS)
- B. Remote procedure call (RPC)
- C. Border Gateway Protocol (BGP)
- D. File Transfer Protocol (FTP)

[Hide Answer](#)

Suggested Answer: D

by  [jinyection](#) at Sept. 28, 2021, 9:33 a.m.

Comments

  [tc5899](#) 1 year, 1 month ago

FTP Port 21

upvoted 2 times

  [jinyection](#) 2 years, 8 months ago

Correct

upvoted 4 times

EXAM 312-50V11 TOPIC 1 QUESTION 365 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 365

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server.

Which of the following tools is used by Jack to perform vulnerability scanning?

- A. Infoga
- B. NCollector Studio
- C. Netsparker Most Voted
- D. WebCopier Pro

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (100%)

by  [jinyection](#) at Sept. 28, 2021, 9:35 a.m.

Comments

  [Scryptic](#) Highly Voted 2 years, 2 months ago

Netsparker is an automated, yet fully configurable, web application security scanner that enables you to scan websites, web applications and web services, and identify security flaws. Netsparker can scan all types of web applications, regardless of the platform or the language with which they are built.

upvoted 8 times

  [stettin12](#) Highly Voted 1 year, 8 months ago

Netsparker no longer exists. It is now Invicti.

upvoted 5 times

  [Daniel8660](#) Most Recent 1 year, 1 month ago

Selected Answer: C

Web Server Attack Methodology - Vulnerability Scanning

Vulnerability scanning is performed to identify vulnerabilities and misconfigurations in a target web server or network. Vulnerability scanning reveals possible weaknesses in a target server to exploit in a web server attack.

Vulnerability scanning tools: Acunetix / Fortify WebInspect / tenable.io / ImmuniWeb / Netsparker (P.1669/1653)

upvoted 5 times

  [jinyection](#) 2 years, 2 months ago

Correct

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 370 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 370

Topic #: 1

[All 312-50v11 Questions]

Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit.

Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

- A. CAST-128
- B. RC5
- C. TEA
- D. Serpent Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [jinjection](#) at Sept. 28, 2021, 9:38 a.m.

Comments

 [andrewdh](#) Highly Voted 2 years, 7 months ago

Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES) contest, where it was ranked second to Rijndael. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen. Like other AES submissions, Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits. The cipher is a 32-round substitution-permutation network operating on a block of four 32-bit words. Each round applies one of eight 4-bit to 4-bit S-boxes 32 times in parallel. Serpent was designed so that all operations can be executed in parallel

upvoted 12 times

 [darthcomptia](#) 1 year, 3 months ago

<https://quizlet.com/603117187/module-20-tools-and-concepts-flash-cards/>

upvoted 2 times

 [GummyBear95](#) Most Recent 1 year, 2 months ago

This was on the exam 21.02.23

upvoted 2 times

 [Daniel8660](#) 1 year, 7 months ago

Selected Answer: D

Ciphers - Serpent

Serpent uses a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits. It can be integrated into software or hardware programs without any restrictions. Serpent involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. (P.3033/3017)

upvoted 3 times

 [jinjection](#) 2 years, 8 months ago

Correct serpent

upvoted 4 times

EXAM 312-50V11 TOPIC 1 QUESTION 375 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 375

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Shiela is an information security analyst working at HiTech Security Solutions. She is performing service version discovery using Nmap to obtain information about the running services and their versions on a target system.

Which of the following Nmap options must she use to perform service version discovery on the target host?

- A. -sN
- B. -sV **Most Voted**
- C. -sX
- D. -sF

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [jinjection](#) at Sept. 28, 2021, 9:42 a.m.

Comments

  [victorfs](#) 1 year ago

Selected Answer: B

The correct option is B.

The flag -sV

upvoted 1 times

  [Daniel8660](#) 1 year, 7 months ago

Selected Answer: B

Service Version discovery

Service version detection helps attackers to obtain information about running services and their versions on a target system. Obtaining an accurate service version number allows attackers to determine the vulnerability of target system to particular exploits.

Nmap -sV <target IP address>, -sV: Probe open ports to determine service/version info. (P.330/314)

upvoted 3 times

  [jinjection](#) 2 years, 8 months ago

Correct -sV (scan version)

upvoted 2 times

EXAM 312-50V11 TOPIC 1 QUESTION 385 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 385

Topic #: 1

[All 312-50v11 Questions]

Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens.

Which of the following tools is used by Gregory in the above scenario?

- A. Wireshark
- B. Nmap
- C. Burp Suite **Most Voted**
- D. CxSAST

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [jinyection](#) at Sept. 28, 2021, 9:54 a.m.

Comments

 [jinyection](#) **Highly Voted**  2 years, 2 months ago

correct

upvoted 5 times

 [Daniel8660](#) **Most Recent**  1 year, 1 month ago

Selected Answer: C

WebSite Footprinting Tools: Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Proxy allows attackers to intercept all requests and responses between the browser and the target web application and obtain information such as web server used, its version, and web-application-related vulnerabilities. (P.190/174)

upvoted 3 times

 [Inumike](#) 1 year, 8 months ago

Burpsuite is a proxy interceptor

upvoted 3 times

 EXAM 312-50V11 TOPIC 1 QUESTION 389 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 389

Topic #: 1

[All 312-50v11 Questions]

_____ is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information.

- A. Spear phishing
- B. Vishing
- C. Whaling **Most Voted**
- D. Phishing

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [jinjection](#) at Sept. 28, 2021, 9:55 a.m.

Comments

 [Vincent_Lu](#) 1 year, 2 months ago

Selected Answer: C

Phishing - Hackers send emails with malicious links to make victim click on them out of concern, worry, or curiosity
Vishing - Hackers make phone calls to engage in conversations with users.

Smishing - Hackers send short messages requesting that you click on malicious links or call provided phone numbers.

Pharming - Hackers use malicious URLs to redirect users to fake websites when attempting to access legitimate ones.

Spear Phishing - Hackers send tailored emails specifically crafted for organizations or individuals, often targeting high-level executives or finance employees.

Whaling - Similar to spear phishing, but targets senior executives of corporate organizations.

upvoted 2 times

 [Daniel8660](#) 2 years, 1 month ago

Selected Answer: C

Computer-based Social Engineering: Phishing

A whaling attack is a type of phishing that targets high profile executives like CEO, CFO, politicians, and celebrities who have complete access to confidential and highly valuable information. (P.1242/1226)

upvoted 3 times

 [khaled_2321](#) 2 years, 1 month ago

Selected Answer: C

correct

upvoted 1 times

 [ebuAkif](#) 2 years, 1 month ago

Selected Answer: C

from CEH material "An attacker targets high profile executives like CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information. The attacker tricks the victim into revealing critical corporate and personal information through email or website spoofing"

upvoted 2 times

 [jinjection](#) 3 years, 2 months ago

correct

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 395 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 395

Topic #: 1

[All 312-50v11 Questions]

John, a security analyst working for an organization, found a critical vulnerability on the organization's LAN that allows him to view financial and personal information about the rest of the employees. Before reporting the vulnerability, he examines the information shown by the vulnerability for two days without disclosing any information to third parties or other internal employees. He does so out of curiosity about the other employees and may take advantage of this information later.

What would John be considered as?

A. Cybercriminal

B. White hat

C. Gray hat **Most Voted**

D. Black hat

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (48%)

A (43%)

10%

by  [8jinjection](#) at Sept. 28, 2021, 10 a.m.

Comments

 [Silascarter](#) **Highly Voted** 4 years ago

If he works as a Security Analyst for the Company that means he had the authority to find the vulnerability. Then he told the company 2 Days Later.. That makes him White Hat. However, he can use the financial records later for personal gains, That makes him Black Hat.

White Hat + Black Hat = Gray Hat. So answer is Correct.

upvoted 13 times

 [blehbleh](#) **Most Recent** 11 months, 4 weeks ago

Selected Answer: A

I would say this is A, the reason being at the very end of the question it states "and may take advantage of this information later." So the information he is gaining about his co workers he may take advantage of later, that would be cybercriminal. I think people are to hung up on that he works there and that he found a vulnerability. Read the end where he may take advantage of the information and that would be a criminal act.

upvoted 1 times

 [tyw82](#) 1 year, 1 month ago

Selected Answer: C

The way CEH defines these hackers seem to be whether the hacking is for offensive or defensive purposes:

- Black hat - offensive
- White hat - defensive
- Grey hat - both

In this case, he had both a defensive objective (protect the organization's vulnerability by reporting it) and offensive objective (may take advantage of the info later). So strictly by CEH definition, it should be C. (Honestly, I don't understand why this matters. The important thing to convey is what actions are ethical or not rather than how to classify them..)

Per CEHv12 P40:

Black Hats: Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes..

- White Hats: White hats or penetration testers are individuals who use their hacking skills for defensive purposes...

- Gray Hats: Gray hats are the individuals who work both offensively and defensively at various times..

upvoted 1 times

 [PP_20](#) 1 year, 10 months ago

Selected Answer: A

Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.

Gray hats exist in an ambiguous ethical hacking area between white and black. These hackers infiltrate systems without their targets' consent, but they don't exploit vulnerabilities to cause harm. Instead, they inform the victims of the hack in order to help them improve their security. But gray hat hackers don't always share this information for free. While gray hats inform companies that they've been hacked, they sometimes ask for a fee in exchange for the details. In these cases, the victims must pay if they want to know their system's vulnerabilities. But if they refuse to pay, gray hat hackers will not attempt to retaliate and cause harm.

upvoted 1 times

✉️  **YourFriendlyNeighborhoodSpider** 2 years ago

Selected Answer: C

ChatGPT:

Answer: C. Gray hat

Explanation:

Cybercriminal (option A): A cybercriminal engages in malicious activities for personal gain or with the intent to cause harm. John's actions, while unethical, are not driven by personal gain or harm.

White hat (option B): White hat hackers are ethical hackers who use their skills to help organizations by finding and fixing security vulnerabilities. John's actions do not align with the ethical behavior expected of a white hat.

Gray hat (option C): Gray hat hackers fall somewhere between white hat and black hat hackers. They may violate ethical standards, but their actions are not explicitly malicious. John's curiosity-driven exploration of the vulnerability without immediate disclosure puts him in a gray hat category.

upvoted 1 times

✉️  **sudowhoami** 2 years ago

Selected Answer: A

Definitely not a Black or White hat. Those of you who claimed Gray hat is also incorrect because he is not discovering vulnerability, but rather accessing sensitive info. As a result, it appears he is a cybercriminal.

upvoted 1 times

✉️  **Vincent_Lu** 2 years, 2 months ago

Selected Answer: A

Cybercriminal

upvoted 1 times

✉️  **Vincent_Lu** 2 years, 2 months ago

Gray hats generally refer to those who discover and report vulnerabilities, rather than those who actively exploit vulnerabilities or gain unauthorized access to sensitive information. In this connection, John's behavior exceeds the definition of gray hat because he goes beyond decision-making to reveal, but instead examines sensitive information and may exploit it illegally.

upvoted 1 times

✉️  **waleedkhalid** 2 years, 3 months ago

Selected Answer: C

Gray hat is correct

upvoted 1 times

✉️  **Genesis777** 2 years, 4 months ago

The glaring details is with this statement - "He does so out of curiosity about the other employees and may take advantage of this information later." . Gray Hats is this: Gray hat hackers represent the middle ground between white hat hackers, who operate on behalf of those maintaining secure systems, and black hat hackers who act maliciously to exploit vulnerabilities in systems. One of the most common examples given of a gray hat hacker is someone who exploits a security vulnerability in order to spread public awareness that the vulnerability exists. Do you think if organization finds out that an employee exploits the system and has plans to exploit the information he discovers for his advantage would make him a "Gray Hat"? If an employee has a security clearance he's already in violation of security policy, two he didn't report it upon discovery, his plan to take advantage of the information later after 2 days. Employee is a Cybercriminal.

upvoted 1 times

✉️  **Lapiro** 2 years, 5 months ago

John, a security analyst working for an organization...

...Before reporting the vulnerability,...

Above 2 comment make him a gray hat or a white hat. cos it is his job to safe guide the company.

upvoted 1 times

✉️  **Rocko1** 2 years, 5 months ago

Selected Answer: A

I would go with Cybercriminal here, he does an action without disclosure.

upvoted 1 times

✉️  **victorfs** 2 years, 6 months ago

Selected Answer: C

The correct option is C.

Gray hat

upvoted 1 times

 **mdmdmd** 2 years, 10 months ago

Selected Answer: C

He has access.....and withholding it...that is a grey hacker for me...Option C
upvoted 1 times

 **jenovaaaa** 2 years, 10 months ago

D. Black Hat
"may take advantage of this information later"
upvoted 1 times

 **josevirtual** 2 years, 11 months ago

Selected Answer: A

You have to report this IMMEDIATELY. Besides, it says "He does so out of curiosity about the other employees and may take advantage of this information later". This is criminal activity, so I think the best answer is "cyber criminal", his behavior is not justified.
upvoted 2 times

 **Acidscars** 2 years, 11 months ago

So now he's a criminal engaged in criminal activity on something he may or may not do later? Hey may take advantage of it, he may not. He may go black hat, he may go white hat; mix them together, boom Grey hat.
upvoted 2 times

 **josevirtual** 2 years, 10 months ago

He found a "critical vulnerability" on his own organization. Even if he finally don't take advantage of it, it may be helping to other hackers to exploit them. Besides, the only thought of "taking advantage of this information later" is clearly criminal from MHO.
upvoted 1 times

 **Daniel8660** 3 years, 1 month ago

Selected Answer: C

Hacker Classes - Gray Hats

Gray hats are the individuals who work both offensively and defensively at various times. Gray hats might help hackers to find various vulnerabilities in a system or network and, at the same time, help vendors to improve products (software or hardware) by checking limitations and making them more secure. (P.46/30)

upvoted 1 times

 **Daniel8660** 3 years, 2 months ago

Selected Answer: C

Gray Hats

Individuals who work both offensively and defensively at various times. (P.46)

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 304 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 304

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

- A. Bluesmacking
- B. BlueSniffing
- C. Bluejacking Most Voted
- D. Bluesnarfing

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [Scryptic](#) at Sept. 29, 2021, 1:22 a.m.

Comments

  [Daniel8660](#) 1 year, 1 month ago

Selected Answer: C

Bluetooth Hacking - Bluejacking

Bluejacking is the use of Bluetooth to send messages to users without the recipient's consent, similar to email spamming. Prior to any Bluetooth communication, the device initiating the connection must provide a name that is displayed on the recipient's screen. Sending anonymous messages over Bluetooth to Bluetooth-enabled devices, via the OBEX(Object Exchange) protocol. (P.2344/2328)

upvoted 3 times

  [cesarai](#) 1 year, 5 months ago

Selected Answer: C

BlueJacking : The art of sending Unsolicited messages CEH mod 16 Page 2328

upvoted 1 times

  [Scryptic](#) 2 years, 2 months ago

Please don't say 'correct', no one knows you

upvoted 4 times

EXAM 312-50 TOPIC 5 QUESTION 8 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 8

Topic #: 5

[\[All 312-50 Questions\]](#)

An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

- A. Timing attack
- B. Replay attack
- C. Memory trade-off attack
- D. Chosen plain-text attack

[Hide Answer](#)

Suggested Answer: D

by  [PennyTester](#) at Oct. 1, 2021, 12:37 p.m.

Comments

  [PennyTester](#) 1 year, 1 month ago

A chosen-plaintext attack (CPA) is a model for cryptanalysis which assumes that the attacker can choose random plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could expose secret information after calculating the secret key.

upvoted 3 times

EXAM 312-50V11 TOPIC 1 QUESTION 396 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 396

Topic #: 1

[All 312-50v11 Questions]

Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner.

What is the type of attack performed on Ben in the above scenario?

- A. Tap 'n ghost attack
- B. Phishing
- C. Advanced SMS phishing Most Voted
- D. Bypass SSL pinning

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  Mimshack at Oct. 1, 2021, 11:16 p.m.

Comments

 **victorfs** 1 year ago

Selected Answer: C

The correct option is C
Advanced SMS phising
upvoted 1 times

 **Daniel8660** 1 year, 7 months ago

Selected Answer: C

Other Techniques for Hacking Android Devices - Advanced SMS Phishing
Advanced SMS phishing attack is a type of phishing scam that occurs due to security flaws in the latest Android-based smartphones. The attack vector mainly depends on a process called Over-the-Air (OTA) provisioning, which is mainly used by network operators. OTA is a mechanism that is used to send provisioning data and updates in a mobile device remotely. (P.2454/2438)
upvoted 3 times

 **Daniel8660** 1 year, 8 months ago

Selected Answer: C

Other Techniques for Hacking Android Devices
Advanced SMS Phishing - The attack vector mainly depends on a process called Over-the-Air (OTA) provisioning, which is mainly used by network operators. Due to its weak authentication methods, OTA is easily vulnerable to phishing attacks. The attacker exploits the mobile device by sending messages that seem to be genuine from the network operator. (P.2454)

upvoted 2 times

 **dinonino** 1 year, 8 months ago

Advanced SMS phishing. As it involves text with PIN.
upvoted 1 times

 **Benoit_G** 1 year, 8 months ago

Selected Answer: C

Module 17 Page 2438
upvoted 3 times

 **MyName7** 1 year, 9 months ago

Selected Answer: C

correct answer is C.

tap and ghost includes the malicious use of NFC technology and RX electrodes - that are used in capacitive smartphone touchscreens
upvoted 4 times

 **Mimshack** 2 years, 8 months ago

Correct. CEH V11 Module 17 Page 2438
upvoted 4 times

 **LoneStarChief** 2 years, 7 months ago

Agreed, as per Module 17 Page 2438 : The attack vector mainly depends on a process called Over-the-Air (OTA) provisioning, which is mainly used by network operators. OTA is a mechanism that is used to send provisioning data and updates in a mobile device remotely. Due to its weak authentication methods, OTA is easily vulnerable to phishing attacks. The attacker exploits the mobile device by sending messages that seem to be genuine from the network operator.

upvoted 3 times

EXAM 312-50V10 TOPIC 1 QUESTION 141 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 141

Topic #: 1

[\[All 312-50v10 Questions\]](#)

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

[Hide Answer](#)

Suggested Answer: A

by  L3PRO at Oct. 17, 2021, 11 p.m.

Comments

  L3PRO 1 year, 1 month ago

It wouldn't be the answer with port 80 b/c it is for http and for insecure traffic. the source would be teh workstations in the network and the destination would be the ban web site.

upvoted 2 times

EXAM 312-50 TOPIC 2 QUESTION 24 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 24

Topic #: 2

[\[All 312-50 Questions\]](#)

Which security control role does encryption meet?

- A. Preventative
- B. Detective
- C. Offensive
- D. Defensive

[Hide Answer](#)

Suggested Answer: A

by  **simron** at Oct. 21, 2021, 3:24 a.m.

Comments

 **blackkofia** 1 year ago

A The data is not in plain text therefore making it hard to read the content
upvoted 1 times

 **simron** 4 years, 1 month ago

Encryption used for preventing eavesdropping data in transit and data at rest.
upvoted 3 times

EXAM 312-50 TOPIC 2 QUESTION 29 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 29

Topic #: 2

[\[All 312-50 Questions\]](#)

What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

- A. Proper testing
- B. Secure coding principles **Most Voted**
- C. Systems security and architecture review
- D. Analysis of interrupts within the software

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

B (100%)

by  simron at Oct. 21, 2021, 3:37 a.m.

Comments

  **asma81** 1 year ago

Selected Answer: B

Secure coding principles are a set of guidelines and best practices that ensure software is developed with security in mind. By following these principles, developers can minimize vulnerabilities such as buffer overflows, SQL injection, and other attacks that could potentially allow the software to tamper with critical data or compromise the system. These principles are designed to prevent the software from unintentionally or maliciously altering or corrupting data.

upvoted 1 times

  **simron** 4 years, 1 month ago

Here focus on last sentence "system is loaded on"

upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 8 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 8

Topic #: 3

[\[All 312-50 Questions\]](#)

Which of the following is a symmetric cryptographic standard?

- A. DSA
- B. PKI
- C. RSA
- D. 3DES

[Hide Answer](#)

Suggested Answer: *D*

by  simron at Oct. 21, 2021, 4:07 a.m.

Comments

  **simron**  1 year, 1 month ago

DSA, RSA algorithms used asymmetric encryption scheme,
PKI use both symmetric and asymmetric encryption scheme
but 3DES uses only asymmetric encryption scheme.

Hence answer is 3DES

upvoted 6 times

EXAM 312-50V11 TOPIC 1 QUESTION 368 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 368

Topic #: 1

[\[All 312-50v11 Questions\]](#)

Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

- A. Bluetooth
- B. WPA2-Enterprise
- C. WPA3-Personal **Most Voted**
- D. ZigBee

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [Osen](#) at Oct. 25, 2021, 6:12 a.m.

Comments

  [Daniel8660](#) 1 year, 1 month ago

Selected Answer: C

WPA3 Encryption

WPA3- Personal: This mode is mainly used to deliver password-based authentication. WPA3 is more rigid to attacks than WPA2 because it uses a modern key establishment protocol called the Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, which replaces the PSK concept used in WPA2- Personal.

Resistance to offline dictionary attacks: It prevents passive password attacks such as brute- forcing. (P.2207/2191)

upvoted 3 times

  [Osen](#) 2 years, 1 month ago

C is correct.

The WPA3 standard also replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016 resulting in a more secure initial key exchange in personal mode.

upvoted 3 times

EXAM 312-50V10 TOPIC 1 QUESTION 20 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 20

Topic #: 1

[\[All 312-50v10 Questions\]](#)

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

- A. Cross-site scripting vulnerability
- B. Web site defacement vulnerability
- C. SQL injection vulnerability
- D. Cross-site Request Forgery vulnerability

[Hide Answer](#)

Suggested Answer: A

by  [Holatung](#) at Nov. 12, 2021, 4:30 p.m.

Comments

  [Holatung](#) 1 year ago

Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.
Answer is D

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 320 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 320

Topic #: 1

[All 312-50v11 Questions]

Upon establishing his new startup, Tom hired a cloud service provider (CSP) but was dissatisfied with their service and wanted to move to another CSP.

What part of the contract might prevent him from doing so?

- A. Lock-down
- B. Virtualization
- C. Lock-in Most Voted
- D. Lock-up

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  Khalid_Loudi at Nov. 21, 2021, 9:23 a.m.

Comments

 **Daniel8660** 1 year, 1 month ago

Selected Answer: C

Cloud Computing Threats - Lock-in

Lock-in reflects the inability of the client to migrate from one CSP to another or in-house systems owing to the lack of tools, procedures, standard data formats, applications, and service portability. This threat is related to the inappropriate selection of a CSP, incomplete and non-transparent terms of use, lack of standard mechanisms, etc. (P.2884/2868)

upvoted 4 times

 **Jong1** 1 year, 8 months ago

Selected Answer: C

Lock-in reflects the inability of the client to migrate from one CSP to another or in-house systems owing to the lack of tools, procedures, standard data formats, applications, and service portability. This threat is related to the inappropriate selection of a CSP, incomplete and non-transparent terms of use, lack of standard mechanisms, etc.

upvoted 2 times

 **gokhansah1n** 1 year, 9 months ago

Lock-in: The difficulties experienced by a user when migrating from in-house systems or from one cloud service provider to another due to the lack of tools, procedures, or standard data formats, poses potential threats to data, application, and service portability

CEHv11 Cloud Computing Module Cloud Computing Threats (Page:2860)

upvoted 1 times

 **Khalid_Loudi** 2 years ago

i see this question in my exam in Aug 2021

upvoted 4 times

 **mrhaky** 1 year, 10 months ago

so did u pass that exam ? and are the questions here sufficient

upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 256 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 256

Topic #: 1

[\[All 312-50v10 Questions\]](#)

The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?

- A. Network Sniffer
- B. Vulnerability Scanner
- C. Intrusion Prevention Server
- D. Security Incident and Event Monitoring Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Silascarter](#) at Nov. 23, 2021, 9:03 p.m.

Comments

 [Silascarter](#) 1 year ago

Selected Answer: D

SIEM tools work by gathering event and log data created by host systems, applications and security devices, such as antivirus filters and firewalls, throughout a company's infrastructure and bringing that data together on a centralized platform.

D is Correct

upvoted 1 times

EXAM 312-50 TOPIC 5 QUESTION 26 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 26

Topic #: 5

[All 312-50 Questions]

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

- A. Sender's public key
- B. Receiver's private key
- C. Receiver's public key
- D. Sender's private key

D. Sender's private key **Most Voted**

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (67%)

C (33%)

by  [Ka2021ka](#) at Nov. 25, 2021, 10:52 a.m.

Comments

 [Novmejst](#) 1 year, 1 month ago

Selected Answer: D

D. Sender's private key

In a digital signature, the message digest (a fixed-length representation of the original message) is encrypted with the sender's private key. This process creates a unique digital signature that can only be decrypted by the sender's public key, which is widely available. When the receiver gets the message, they can verify its authenticity by using the sender's public key to decrypt the digital signature and comparing it to the message digest they calculated from the received message. If the two match, the receiver can be reasonably sure that the message came from the claimed sender and has not been altered in transit.

upvoted 3 times

 [salei](#) 1 year, 6 months ago

Selected Answer: D

To prove sender identity, they have to encrypt with its own private key. The receiver can prove that he's who's claim to be by properly decrypting the message with the sender public key

upvoted 1 times

 [Ka2021ka](#) 2 years, 6 months ago

Selected Answer: C

Encrypted by receiver's public key

upvoted 2 times

 [WZ1122](#) 2 years, 2 months ago

Encryption is using receiver's public key and decrypted by receiver's private key.
digital signature is using sender's private key and verified by sender's public key.

upvoted 4 times

 [HeyacedoGomez](#) 1 year, 4 months ago

I think the question stated signing.....and that's done by hashing the data with sender's PRIVATE key.....

upvoted 3 times

 [dorinh](#) 2 years, 6 months ago

Receiver's public key is available also for an attacker, so he can change the message, generate another hash and encrypt the hash with the receiver's public key so the authenticity of the message is not guaranteed. If the hash is encrypted with the sender's private key, anyone can decrypt it with the sender's public key to validate the hash. With this approach, the authenticity of the message is guaranteed, as long as the sender's private key is not compromised.

upvoted 3 times

EXAM 312-50 TOPIC 2 QUESTION 9 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 9

Topic #: 2

[\[All 312-50 Questions\]](#)

Which of the following is a detective control?

- A. Smart card authentication
- B. Security policy
- C. Audit trail
- D. Continuity of operations plan

[Hide Answer](#)

Suggested Answer: C

by  dorinh at Nov. 30, 2021, 3:14 p.m.

Comments

  dorinh 12 months ago

Detective Controls - Detect security violations and record any intrusion attempts
- Examples include motion detectors, alarm systems and sensors, video surveillance, and other methods
upvoted 3 times

EXAM 312-50 TOPIC 3 QUESTION 31 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 31

Topic #: 3

[\[All 312-50 Questions\]](#)

During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local

System account. How can this weakness be exploited to access the system?

- A. Using the Metasploit psexec module setting the SA / Admin credential
- B. Invoking the stored procedure xp_shell to spawn a Windows command shell
- C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
- D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

[Hide Answer](#)

Suggested Answer: D

by  [dorinh](#) at Nov. 30, 2021, 5:03 p.m.

Comments

  [dorinh](#) 12 months ago

xp_cmdshell - Spawns a Windows command shell and passes in a string for execution. Any output is returned as rows of text.
upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 6 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 6

Topic #: 4

[\[All 312-50 Questions\]](#)

Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

- A. They are written in Java.
- B. They send alerts to security monitors.
- C. They use the same packet analysis engine.
- D. They use the same packet capture utility.

[Hide Answer](#)

Suggested Answer: D

by  dorinh at Dec. 1, 2021, 9:44 a.m.

Comments

  dorinh 12 months ago

pcap is an application programming interface (API) for capturing network traffic. While the name is an abbreviation of packet capture, that is not the API's proper name. Unix-like systems implement pcap in the libpcap library; libpcap, WinPcap, and Npcap provide the packet-capture and filtering engines of many open-source and commercial network tools, including protocol analyzers (packet sniffers), network monitors, network intrusion detection systems, traffic-generators and network-testers.

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 10 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 10

Topic #: 4

[\[All 312-50 Questions\]](#)

To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

A. Recipient's private key

B. Recipient's public key

C. Master encryption key

D. Sender's public key

[Hide Answer](#)

Suggested Answer: B

by  dorinh at Dec. 1, 2021, 9:51 a.m.

Comments

  dorinh 12 months ago

PGP Encryption

- o When a user encrypts data with PGP, PGP first compresses the data. Compressing the data reduces patterns in the plaintext that could be exploited by most cryptanalysis techniques to crack the cipher, thereby increasing the resistance to cryptanalysis considerably.
- o PGP then creates a random key that is a one-time-only secret key.
- o PGP uses the random key generated to encrypt the plaintext, resulting in a ciphertext.
- o Once the data are encrypted, a random key is encrypted with the recipient's PUBLIC key.
- o The public-key-encrypted random key is sent along with the ciphertext to the recipient.

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 23 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 23

Topic #: 4

[\[All 312-50 Questions\]](#)

A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

- A. Locate type=ns
- B. Request type=ns
- C. Set type=ns **Most Voted**
- D. Transfer type=ns

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  dorinh at Dec. 1, 2021, 10:33 a.m.

Comments

  dorinh 12 months ago

Selected Answer: C

nslookup set type=<resourcerecordtype>

Specifies a DNS resource record type. The default resource record type is A, but you can use any of the following values:

A: Specifies a computer's IP address.

ANY: Specifies a computer's IP address.

CNAME: Specifies a canonical name for an alias.

GID: Specifies a group identifier of a group name.

HINFO: Specifies a computer's CPU and type of operating system.

MB: Specifies a mailbox domain name.

MG: Specifies a mail group member.

MINFO: Specifies mailbox or mail list information.

MR: Specifies the mail rename domain name.

MX: Specifies the mail exchanger.

NS: Specifies a DNS name server for the named zone.

PTR: Specifies a computer name if the query is an IP address; otherwise, specifies the pointer to other information.

SOA: Specifies the start-of-authority for a DNS zone.

TXT: Specifies the text information.

UID: Specifies the user identifier.

UINFO: Specifies the user information.

WKS: Describes a well-known service.

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup-set-type>

upvoted 3 times

EXAM 312-50 TOPIC 4 QUESTION 28 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 28

Topic #: 4

[\[All 312-50 Questions\]](#)

How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

- A. Defeating the scanner from detecting any code change at the kernel
- B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
- C. Performing common services for the application process and replacing real applications with fake ones
- D. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options

[Hide Answer](#)

Suggested Answer: D

by  dorinh at Dec. 1, 2021, 10:39 a.m.

Comments

  dorinh 12 months ago

By attaching itself to the master boot record in a hard drive and changing the machines boot sequence/options Windows 7 boot record never has the opportunity to determine something is awry.

<https://www.linkedin.com/pulse/how-can-rootkit-bypass-windows-operating-systems-kernel-jameel-nabbo>
upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 30 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 30

Topic #: 4

[\[All 312-50 Questions\]](#)

Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

- A. UDP 123
- B. UDP 541
- C. UDP 514
- D. UDP 415

[Hide Answer](#)

Suggested Answer: C

by  dorinh at Dec. 1, 2021, 10:44 a.m.

Comments

  **blackkofia** 1 year ago

To send log messages to a log analysis tool behind a firewall, you typically use the Syslog protocol.

UDP 514: This is the default port for Syslog over UDP. It's commonly used because it's lightweight, but it does not guarantee message delivery.

upvoted 1 times

EXAM 312-50 TOPIC 4 QUESTION 45 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 45

Topic #: 4

[\[All 312-50 Questions\]](#)

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

- A. 768 bit key
- B. 1025 bit key
- C. 1536 bit key
- D. 2048 bit key

[Hide Answer](#)

Suggested Answer: C

by  [dorinh](#) at Dec. 1, 2021, 11:04 a.m.

Comments

  [dorinh](#) 12 months ago

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/bovpn/manual/diffie_hellman_c.html
upvoted 1 times

  [dorinh](#) 12 months ago

Diffie-Hellman Group 1 (768-bit)
Diffie-Hellman Group 2 (1024-bit)
Diffie-Hellman Group 5 (1536-bit)
Diffie-Hellman Group 14 (2048-bit)
Diffie-Hellman Group 15 (3072-bit)
upvoted 7 times

EXAM 312-50 TOPIC 4 QUESTION 72 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 72

Topic #: 4

[\[All 312-50 Questions\]](#)

A botnet can be managed through which of the following?

- A. IRC
- B. E-Mail
- C. Linkedin and Facebook
- D. A vulnerable FTP server

[Hide Answer](#)

Suggested Answer: A

by  dorinh at Dec. 1, 2021, 12:26 p.m.

Comments

  dorinh 12 months ago

IRC- Internet Relay Chat. A form of real-time internet text messaging often used with chat sessions. Some botnets have used IRC channels to control zombie computers through a command-and-control server.

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 47 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 47

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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 Most Voted
- D. The amount of time it takes to convert biometric data into a template on a smart card

[Hide Answer](#)

Suggested Answer: C

Community vote distribution



by  [Novmejst](#) at Dec. 11, 2021, 4:06 p.m.

Comments

  [Novmejst](#) Highly Voted  2 years, 11 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  1 year, 1 month ago

Selected Answer: C
Answer is C
upvoted 1 times

  [Vincent_Lu](#) 1 year, 2 months 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](#) 1 year, 3 months 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

EXAM 312-50 TOPIC 2 QUESTION 6 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 6

Topic #: 2

[\[All 312-50 Questions\]](#)

What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

- A. Passive
- B. Reflective
- C. Active
- D. Distributive

[Hide Answer](#)

Suggested Answer: C

by  **ligthon7** at Jan. 8, 2022, 8:15 p.m.

Comments

 **ligthon7** 1 year, 4 months ago

Answer is correct:

1. Active fingerprinting

Active fingerprinting is accomplished by sending specially crafted packets to a target machine and then noting down its response and analyzing the gathered information to determine the target OS.

<https://www.zerosuniverse.com/ethical-hacking/what-is-os-fingerprinting/>

upvoted 4 times

EXAM 312-50 TOPIC 2 QUESTION 25 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 25

Topic #: 2

[\[All 312-50 Questions\]](#)

A covert channel is a channel that

- A. transfers information over, within a computer system, or network that is outside of the security policy.
- B. transfers information over, within a computer system, or network that is within the security policy.
- C. transfers information via a communication path within a computer system, or network for transfer of data.
- D. transfers information over, within a computer system, or network that is encrypted.

[Hide Answer](#)

Suggested Answer: A

by  **Sbowo** at Jan. 23, 2022, 10:13 a.m.

Comments

 **Sbowo** 1 year, 4 months ago

A channel that transfers information within a computer system or network in a way that violates the security policy
upvoted 2 times

EXAM 312-50 TOPIC 2 QUESTION 23 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 23

Topic #: 2

[All 312-50 Questions]

Which of the following is considered an acceptable option when managing a risk?

A. Reject the risk.

B. Deny the risk.

C. Mitigate the risk. **Most Voted**

D. Initiate the risk. C

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  Kev at Oct. 24, 2019, 12:30 a.m.

Comments

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

The answer is C. Mitigating risks is always a prudent way to approach risk management.

upvoted 7 times

 **greeklover84** **Most Recent** 11 months, 3 weeks ago

Selected Answer: C

no doubt !! C

upvoted 1 times

 **igodomigododevcenter** 1 year ago

Selected Answer: C

C make most sense

upvoted 1 times

 **igodomigododevcenter** 1 year, 1 month ago

C when there is a risk that exceed your level of tolerance, you must mitigate the risk

upvoted 1 times

 **kodji** 1 year, 8 months ago

Selected Answer: C

Mitigate the risk.

upvoted 1 times

 **isaackitonij** 2 years, 2 months ago

I think risk mitigation is the right choice since it entails reducing the impact of potential risks by developing a plan to manage, eliminate, or limit setbacks as much as possible.

upvoted 1 times

 **shahid0q** 2 years, 7 months ago

Selected Answer: C

MITIGATE

upvoted 1 times

 **Blade832** 2 years, 9 months ago

Selected Answer: C

Mitigating the Risk

upvoted 1 times

✉️  **CybeXRay** 2 years, 9 months ago

Selected Answer: C

Mitigating the Risk

upvoted 1 times

✉️  **zahidchaudhary** 3 years, 4 months ago

Selected Answer: C

Mitigate the risk.

upvoted 1 times

✉️  **vnandha** 3 years, 4 months ago

Selected Answer: C

Mitigating the risk

upvoted 1 times

✉️  **jagodziasz** 3 years, 4 months ago

Selected Answer: C

C, rest of answers are wrong

upvoted 1 times

✉️  **Grezavi** 3 years, 11 months ago

C Mitigate the risk

upvoted 2 times

✉️  **simplimarvelous** 4 years, 10 months ago

Mitigating

upvoted 2 times

✉️  **Kev** 5 years, 7 months ago

The answer is in the wrong spot.

upvoted 3 times

EXAM 312-50 TOPIC 3 QUESTION 16 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 16

Topic #: 3

[All 312-50 Questions]

A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

- A. Forensic attack
- B. ARP spoofing attack **Most Voted**
- C. Social engineering attack
- D. Scanning attack

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

B (100%)

by  Yuzuki at Feb. 9, 2022, 5:16 a.m.

Comments

 **bic3p** 1 year, 3 months ago

they are trying to trick us, for arp spoofing attack we need to secure the network devices like router and set up firewall. So the answer is definately C
upvoted 1 times

 **gtantse** 3 years, 8 months ago

Answer is definitely C! Why will you need to secure your email gateway for ARP. But in C the email gateway will monitor the email. And if a malicious email got through the antivirus will catch the malicious software
upvoted 4 times

 **WZ1122** 3 years, 8 months ago

Should be C.
An email gateway is a type of email server that protects an organizations or users internal email servers. This server acts as a gateway through which every incoming and outgoing email passes through. A Secure Email Gateway (SEG) is a device or software used for email monitoring that are being sent and received. Email gateway protection is designed to prevent unwanted email and deliver good email. Messages that are unwanted include spam, phishing attacks, malware or fraudulent content. Outgoing messages can be analyzed to prevent sensitive data from leaving the organization or to automatically encrypt emails that contain sensitive information.
upvoted 3 times

 **Khza** 3 years, 8 months ago

Me too is B
upvoted 1 times

 **Qudaz** 3 years, 9 months ago

Selected Answer: B
Answer is definitely not C, I would go with B.
upvoted 1 times

 **Yuzuki** 3 years, 9 months ago

Ans should be B.
upvoted 1 times

EXAM 312-50 TOPIC 5 QUESTION 6 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 6

Topic #: 5

[\[All 312-50 Questions\]](#)

A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

- A. Public key
- B. Private key**
- C. Modulus length
- D. Email server certificate

[Hide Answer](#)

Suggested Answer: *B*

by  [WZ1122](#) at March 20, 2022, 7:10 a.m.

Comments

  [WZ1122](#) 3 years, 8 months ago

why not D?

upvoted 2 times

  [a4687eb](#) 1 year, 4 months ago

This is a tricky question. When you send an e-mail, to ensure integrity you generate hash value from your message. Then you should sign the message and hash by private key. Technically hash provides you with integrity. Private key provides something like non-repudiation. There is not possible to choose Hash here so the private key is the best option.

upvoted 1 times

EXAM 312-50V10 TOPIC 1 QUESTION 123 DISCUSSION

Actual exam question from ECCouncil's 312-50v10

Question #: 123

Topic #: 1

[\[All 312-50v10 Questions\]](#)

During the process of encryption and decryption, what keys are shared?

- A. Private keys
- B. User passwords
- C. Public keys
- D. Public and private keys

[Hide Answer](#)

Suggested Answer: C

by [deleted] at April 2, 2022, 8:38 p.m.

Comments

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

EXAM 312-50 TOPIC 2 QUESTION 1 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 1

Topic #: 2

[\[All 312-50 Questions\]](#)

Passive reconnaissance involves collecting information through which of the following?

- A. Social engineering
- B. Network traffic sniffing
- C. Man in the middle attacks
- D. Publicly accessible sources Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  U_Rock at April 7, 2022, 8:42 p.m.

Comments

  Null_Pointer_Exception 1 year, 5 months ago

Selected Answer: D

Passive reconnaissance is one that's performed without direct interactions with systems we're investigating. This makes me think that sniffing would also suffice, since we just hijack data that's already sent into ether, but option D seems the safest.
upvoted 2 times

  AmalUB 2 years, 3 months ago

Answer D

upvoted 2 times

  U_Rock 3 years, 1 month ago

Selected Answer: D

I agree.

upvoted 2 times

EXAM 312-50 TOPIC 5 QUESTION 1 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 1

Topic #: 5

[\[All 312-50 Questions\]](#)

Which of the following is optimized for confidential communications, such as bidirectional voice and video?

A. RC4 **Most Voted**

B. RC5

C. MD4

D. MD5

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  **ESPNCCH** at June 28, 2022, 12:30 a.m.

Comments

 **a4687eb** 1 year, 4 months ago

Selected Answer: A

RC4 is stream encryption and therefore is good for listed purposes
upvoted 1 times

 **ESPNCCH** 3 years, 5 months ago

RC4, RC5 & RC6 are the algorithms of a symmetric encryption.
upvoted 1 times

 EXAM 312-50V11 TOPIC 1 QUESTION 292 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 292

Topic #: 1

[All 312-50v11 Questions]

```
ping-* 6 192.168.0.101
```

Output:

```
Pinging 192.168.0.101 with 32 bytes of data:  
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128  
Reply from 192.168.0.101:  
Ping statistics for 192.168.0.101  
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss).  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

What does the option * indicate?

- A. t
- B. s
- C. a

D. n Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  MyName7 at Aug. 31, 2022, 12:44 p.m.

Comments

 **Daniel8660** Highly Voted 1 year, 7 months ago

Selected Answer: D

ping www.certifiedhacker.com -i 2 -n 1

Note: -n specifies the number of echo requests to be sent to the target. (P.3479/LAB P.50)

upvoted 5 times

 **victorfs** Most Recent 1 year ago

Selected Answer: D

The correcto option is D.

n

upvoted 1 times

 **MyName7** 1 year, 9 months ago

Selected Answer: D

You can see how many replies are sent back (6) and make an analogy that "n" is the correct response.

upvoted 4 times

EXAM 312-50V11 TOPIC 1 QUESTION 46 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 46

Topic #: 1

[All 312-50v11 Questions]

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. **Most Voted**
- C. The host is likely a router.
- D. The host is likely a Windows machine.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [TroyMcLure](#) at Sept. 3, 2022, 8:19 p.m.

Comments

 [TroyMcLure](#) **Highly Voted** 1 year, 9 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** 1 year, 2 months ago

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

upvoted 1 times

 [MGRavindra](#) 1 year, 2 months ago

ipp is open. So obviously printer

upvoted 1 times

 [Daniel8660](#) 1 year, 7 months ago

Selected Answer: B

TCP 631, Internet Printing Protocol (IPP)

TCP 9100, Printer

upvoted 4 times

 [damienronce](#) 1 year, 8 months ago

B is the correct awswer :

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

upvoted 2 times

 [Ranjanarajshree](#) 1 year, 8 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

EXAM 312-50V11 TOPIC 1 QUESTION 289 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 289

Topic #: 1

[All 312-50v11 Questions]

From the following table, identify the wrong answer in terms of Range (ft).

Standard	Range (ft)
802.11a	150-150
802.11b	150-150
802.11g	150-150
802.16 (WiMax)	30 miles

A. 802.16 (WiMax) Most Voted

B. 802.11g

C. 802.11b

D. 802.11a

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (62%)

D (38%)

by  [Jacs](#) at Sept. 6, 2022, 4:24 p.m.

Comments

 [Acidscars](#) Highly Voted  1 year, 11 months ago

Selected Answer: A

The real answer is likely D which truly is 95 feet. The bs EC Council answer is probably A based on out dated and incorrect material. Another example of a terrible question written by incompetent people.

upvoted 6 times

 [sringan](#) Most Recent  1 year ago

Selected Answer: A

802.11a --> 35-100, 5000 m
802.11b --> 35-140 m
802.11g --> 38-140m
802.16(WiMAX) --> 1609.34 - 9656.06 m (1-6 miles)
Reference: CEH v12 Ebook Pg no: 2371

upvoted 1 times

 [DataTraveler](#) 1 year ago

Selected Answer: D

The correct answer is D. See P. 2186/2170
upvoted 1 times

 [Attila777](#) 1 year, 1 month ago

the answer is definetly D.

802.16 provides up to 50 km (31 miles) of linear service area range and allows users connectivity without a direct line of sight to a base station. The technology also provides shared data rates up to 75 Mbit/s

upvoted 1 times

 [victorfs](#) 1 year, 6 months ago

Selected Answer: D

The correct "incorrect" option is D.
802.11a is ft: 95 indoor and 300 outdoor.

upvoted 2 times

✉ **mdmdmd** 1 year, 10 months ago

Selected Answer: D

802.11a is approximately 95ft...

Option A seems correct but at specifications for the 2 to 11 GHz range which is less than 30miles

upvoted 1 times

✉ **CandidKing** 1 year, 11 months ago

Selected Answer: D

The maximum range of each standard varies, depending on environmental factors such as obstructions and interference from other sources of radio frequency signals. The maximum range of 802.11a wireless was approximately 95 feet with throughput of up to 54 megabits per second, while 802.11b was capable of transmitting up to 150 feet at 11 Mbps. The 802.11g standard extended that range to 170 feet at the same speed as 802.11a; 802.11n extended the maximum range to 230 feet and throughput to a maximum of 600 Mbps. 802.11ac routers provide similar range but increase throughput to a theoretical maximum of 1.33 gigabits per second.

WiMAX operates in between 10 and 66 GHz Line of Sight (LOS) at a range up to 50 km (30 miles) and 2 to 11GHz non Line-of-Sight (NLOS) typically up to 6 - 10 km (4 - 6 miles) for fixed customer premises equipment (CPE).

upvoted 1 times

✉ **josevirtual** 1 year, 11 months ago

Selected Answer: A

According to the course material, the range are like Daniel8660 says:

802.11a Range 35- 100 meters

802.11b Range 35- 140 meters

802.11g Range 38- 140 meters

802.16 (WiMAX) Range 1- 6 miles

150 feet are about 50 meters, so I'd say that all the answers are confusing, but the clearly wrong option is 802.16 (WiMAX), so I go with A.

upvoted 3 times

✉ **Daniel8660** 2 years, 1 month ago

Selected Answer: A

802.11a Range 35- 100 meters

802.11b Range 35- 140 meters

802.11g Range 38- 140 meters

802.16 (WiMAX) Range 1- 6 miles

upvoted 4 times

✉ **ErryErry** 2 years, 1 month ago

Selected Answer: D

The correct Answer is D

WiMAX can have a max range of 30 miles

802.11a about 95ft

upvoted 3 times

✉ **sergiет** 2 years, 1 month ago

Selected Answer: D

I think the D is the correct one:

The maximum range of 802.11a wireless was approximately 95 feet with throughput of up to 54 megabits per second, while 802.11b was capable of transmitting up to 150 feet at 11 Mbps.

WiMAX operates in between 10 and 66 GHz Line of Sight (LOS) at a range up to 50 km (30 miles) and 2 to 11GHz non Line-of-Sight (NLOS) typically up to 6 - 10 km (4 - 6 miles) for fixed customer premises equipment (CPE).

upvoted 2 times

✉ **AbusedLink** 2 years, 2 months ago

Selected Answer: A

WiMAX is only 1-6 miles according to the course materials.

upvoted 2 times

✉ **Jacs** 2 years, 2 months ago

wifi max is only 18 miles

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 117 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 117

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [TroyMcLure](#) at Sept. 7, 2022, 7:50 p.m.

Comments

  [Daniel8660](#) Highly Voted 1 year, 1 month ago

Selected Answer: D

Intrusion Detection Tools: Snort , open-sources (P.1518/1502)
upvoted 5 times

  [TroyMcLure](#) Most Recent 1 year, 2 months ago

Selected Answer: D

This is a typical snort rule. Snort is a kind of IDS.
upvoted 2 times

 EXAM 312-50V11 TOPIC 1 QUESTION 124 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 124

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [TroyMcLure](#) at Sept. 7, 2022, 8:21 p.m.

Comments

  [TroyMcLure](#) Highly Voted 1 year, 8 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, 7 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 1 year ago

Selected Answer: D

The correcto opción is D.
Email spoofing
upvoted 1 times

  [josevirtual](#) 1 year, 5 months ago

Selected Answer: D

Are not A and D essentially the same answer?
upvoted 1 times

EXAM 312-50 TOPIC 7 QUESTION 1 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 1

Topic #: 7

[\[All 312-50 Questions\]](#)

An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?

- A. Start by foot printing the network and mapping out a plan of attack.
- B. Ask the employer for authorization to perform the work outside the company.
- C. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.
- D. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.

[Hide Answer](#)

Suggested Answer: *B*

by  **Fekki** at Sept. 8, 2022, 8:04 a.m.

Comments

 **Raym0523** 1 year, 3 months ago

Keyword: 'Before starting work on this job'

upvoted 1 times

 **Fekki** 2 years, 8 months ago

Wrong, the friend is the owner, and he asked him to do the test

upvoted 1 times

 **Sutokuto** 2 years, 3 months ago

They're talking about the company he currently works for, not the friends company

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 275 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 275

Topic #: 1

[\[All 312-50v11 Questions\]](#)

You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

```
invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP
fingerprinting (for OS scan) xxxxxxxx xxxxxx xxxxxxxxx. QUITTING!
```

What seems to be wrong?

- A. The nmap syntax is wrong.
- B. This is a common behavior for a corrupted nmap application.
- C. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
- D. OS Scan requires root privileges. Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [king777](#) at Sept. 11, 2022, 4:09 p.m.

Comments

  [jucuar](#) 1 year ago

En la imagen se ve en una sola linea:
nmap -T4 -O 10.10.0.0/24 TCP/IP
Por lo cual pareciera que la sintaxis es incorrecta
upvoted 2 times

  [Daniel8660](#) 1 year, 1 month ago

Selected Answer: D
In Nmap, the - O option is used to perform OS discovery, providing OS details of the target machine.
upvoted 3 times

  [king777](#) 1 year, 2 months ago

Selected Answer: D
Yes, the given answer is correct, I try it yourself in your home lab.
upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 73 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 73

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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. Most Voted
- B. This is a scam because Bob does not know Scott.
- C. Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.
- D. This is probably a legitimate message as it comes from a respectable organization.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  baybay at Sept. 12, 2022, 8:53 p.m.

Comments

  **ostorgaf** 1 year, 3 months 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** 2 years, 2 months ago

Selected Answer: A

A. is the only plausible answer.
upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 190 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 190

Topic #: 1

[All 312-50v11 Questions]

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 Most Voted
- D. Null byte

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [TroyMcLure](#) at Sept. 13, 2022, 6:09 p.m.

Comments

 [Daniel8660](#) Highly Voted 2 years, 1 month 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](#) Most Recent 1 year, 3 months ago

CORRECT ANS IS C

upvoted 1 times

 [victorf5](#) 1 year, 6 months ago

Selected Answer: C

The correct option is C

upvoted 1 times

 [TroyMcLure](#) 2 years, 2 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

EXAM 312-50V11 TOPIC 1 QUESTION 298 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 298

Topic #: 1

[\[All 312-50v11 Questions\]](#)

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag:"b0aac0542e25c31:89d"
Content-Length: 7369
```

Which of the following is an example of what the engineer performed?

- A. Banner grabbing **Most Voted**
- B. SQL injection
- C. Whois database query
- D. Cross-site scripting

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [dinonino](#) at Sept. 18, 2022, 6:25 p.m.

Comments

  [Daniel8660](#) 1 year, 1 month ago

Selected Answer: A

Web Server Footprinting/Banner Grabbing

An attacker can gather valuable system-level data such as account details, OSs, software versions, server names, and database schema details. Web Server Footprinting Tools: Netcat, Uniscan, Nmap. (P.1652/1636)

upvoted 4 times

EXAM 312-50V11 TOPIC 1 QUESTION 267 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 267

Topic #: 1

[\[All 312-50v11 Questions\]](#)

The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

- A. The ACL 104 needs to be first because is UDP
- B. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router Most Voted
- C. The ACL for FTP must be before the ACL 110
- D. The ACL 110 needs to be changed to port 80

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [TroyMcLure](#) at Sept. 20, 2022, 4:26 p.m.

Comments

  [TroyMcLure](#) Highly Voted 1 year, 8 months ago

Selected Answer: B

ACLs are read by the device and followed in order.
102 is the statement denying TCP ANY ANY
This means that every TCP traffic will be denied by the statement.
upvoted 5 times

  [boog](#) Most Recent 11 months, 3 weeks ago

None of the above
102 is denying tcp only. 104 should permit as it's udp
upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 270 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 270

Topic #: 1

[\[All 312-50v11 Questions\]](#)

An attacker scans a host with the below command. Which three flags are set?

```
# nmap -sX host.domain.com
```

A. This is SYN scan. SYN flag is set.

B. This is Xmas scan. URG, PUSH and FIN are set. Most Voted

C. This is ACK scan. ACK flag is set.

D. This is Xmas scan. SYN and ACK flags are set.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [TroyMcLure](#) at Sept. 20, 2022, 4:51 p.m.

Comments

  [TroyMcLure](#) Highly Voted  1 year, 2 months ago

Selected Answer: B

Xmas scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.
upvoted 5 times

  [Daniel8660](#) Highly Voted  1 year, 1 month ago

Selected Answer: B

Inverse TCP flag scan

Using the Xmas scan, attackers send a TCP frame to a remote device with FIN, URG, and PUSH flags set.

Nmap -sX -v <target IP address> (P.307/291)

upvoted 5 times

EXAM 312-50 TOPIC 8 QUESTION 214 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 214

Topic #: 8

[\[All 312-50 Questions\]](#)

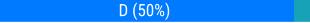
Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?

- A. NET FILE
- B. NET USE
- C. NET CONFIG
- D. NET VIEW Most Voted

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

 D (50%)  B (50%)

by  [salei](#) at Oct. 1, 2022, 3:25 p.m.

Comments

  [guspukydo](#) 1 year, 3 months ago
D

The "NET VIEW" command is a built-in command in Windows that can be used to display a list of shared resources (including folders and printers) on a specific computer. By default, the command will display all shares on the local computer, but it can also be used to list shares on remote computers.

upvoted 1 times

  [jasonkym](#) 1 year, 3 months ago
Selected Answer: B

Net use : The command used to show the shared drives you've mapped and allow you to manage those mapped drives.

Net view : Is used to show a list of computers and network devices on the network.

So B is the correct answer.
upvoted 1 times

  [salei](#) 1 year, 8 months ago
Selected Answer: D

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh875576\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh875576(v=ws.11))
upvoted 1 times

  [jasonkym](#) 1 year, 3 months ago
It is B.
Net use : The command used to show the shared drives you've mapped and allow you to manage those mapped drives.

Net view : Is used to show a list of computers and network devices on the network.

<https://www.google.com/amp/s/www.linuxhelp.com/amp/questions/what-is-the-difference-between-the-net-user-net-use-and-net-view-commands-in-windows-cmd>
upvoted 1 times

EXAM 312-50 TOPIC 8 QUESTION 274 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 274

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following Nmap commands would be used to perform a stack fingerprinting?

- A. Nmap -O -p80 <host(s.>
- B. Nmap -hU -Q<host(s.>
- C. Nmap -sT -p <host(s.>
- D. Nmap -u -o -w2 <host>
- E. Nmap -sS -Op targe

[Hide Answer](#)

Suggested Answer: *B*

by  [AlexT](#) at Nov. 17, 2019, 6:37 p.m.

Comments

  [devag](#) 1 year ago

definitely A
upvoted 2 times

  [styx](#) 1 year, 8 months ago

Answer is indeed A
upvoted 2 times

  [AlexT](#) 2 years ago

Nmap -O -p80 <host(s.>
Explanation: This option activates remote host identification via TCP/IP fingerprinting.
In other words, it uses a bunch of techniques to detect subtlety in the underlying operating system network stack of the computers you are scanning. It uses this information to create a "fingerprint" which it compares with its database of known OS fingerprints (the nmap-os-fingerprints file. to decide what type of system you are scanning.
upvoted 3 times

EXAM 312-50 TOPIC 8 QUESTION 271 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 271

Topic #: 8

[\[All 312-50 Questions\]](#)

What are two things that are possible when scanning UDP ports? (Choose two.)

- A. A reset will be returned
- B. An ICMP message will be returned
- C. The four-way handshake will not be completed
- D. An RFC 1294 message will be returned
- E. Nothing

[Hide Answer](#)

Suggested Answer: BE

by  salei at Oct. 2, 2022, 3:22 p.m.

Comments

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

EXAM 312-50 TOPIC 3 QUESTION 34 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 34

Topic #: 3

[\[All 312-50 Questions\]](#)

Which of the following types of firewall inspects only header information in network traffic?

A. Packet filter Most Voted

B. Stateful inspection

C. Circuit-level gateway

D. Application-level gateway

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [salei](#) at Oct. 10, 2022, 12:40 p.m.

Comments

 [salei](#) 1 year, 1 month ago

Selected Answer: A

<https://techgenix.com/types-of-firewalls/#:~:text=1.-,Packet%2DFiltering%20Firewalls,only%20inspects%20a%20packet's%20header.>
upvoted 1 times

EXAM 312-50 TOPIC 3 QUESTION 39 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 39

Topic #: 3

[\[All 312-50 Questions\]](#)

Which of the following cryptography attack methods is usually performed without the use of a computer?

A. Ciphertext-only attack

B. Chosen key attack

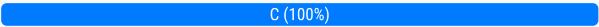
C. Rubber hose attack Most Voted

D. Rainbow table attack

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

 C (100%)

by  [salei](#) at Oct. 10, 2022, 1:40 p.m.

Comments

  [salei](#) 1 year, 1 month ago

Selected Answer: C

The rubber hose attack is extracting secrets from people by use of torture or coercion. Other means is governmental and corporate influence over other sub-entities. The best method of defense is for people to know nothing or as little secrets as possible.

upvoted 3 times

EXAM 312-50 TOPIC 8 QUESTION 43 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 43

Topic #: 8

[\[All 312-50 Questions\]](#)

You've 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 tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts?

A. CHNTPW Most Voted

B. Cain & Abel

C. SET

D. John the Ripper

[Hide Answer](#)

Suggested Answer: A

chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.

References: <https://en.wikipedia.org/wiki/Chntpw>

Community vote distribution

A (100%)

by  salei at Oct. 13, 2022, 11:33 a.m.

Comments

  salei 1 year, 1 month ago

Selected Answer: A

<https://opensource.com/article/18/3/how-reset-windows-password-linux>

upvoted 1 times

EXAM 312-50V11 TOPIC 1 QUESTION 155 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 155

Topic #: 1

[\[All 312-50v11 Questions\]](#)

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 Most Voted
- C. CSRF
- D. XSS

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Daniel8660](#) at Oct. 16, 2022, 5:52 a.m.

Comments

  [Daniel8660](#) Highly Voted 1 year, 1 month ago

Selected Answer: B

Simple Buffer Overflow in C

EX: int buffer(char str[]) (P.637/621)

upvoted 5 times

EXAM 312-50V11 TOPIC 1 QUESTION 183 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 183

Topic #: 1

[All 312-50v11 Questions]

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('.  
upvoted 1 times

## EXAM 312-50 TOPIC 8 QUESTION 340 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 340

Topic #: 8

[\[All 312-50 Questions\]](#)

Which of the following is the primary objective of a rootkit?

- A. It opens a port to provide an unauthorized service
- B. It creates a buffer overflow
- C. It replaces legitimate programs
- D. It provides an undocumented opening in a program

[Hide Answer](#)

**Suggested Answer:** C

by  [salei](#) at Nov. 22, 2022, 7:10 a.m.

### Comments

 [salei](#) 1 year ago

The main purpose of rootkits is to mask malware payloads effectively and preserve their privileged existence on the system. For that reason, a rootkit will conceal files, malware processes, injected modules, registry keys, user accounts or even system registries running on system boot.  
upvoted 1 times

## EXAM 312-50 TOPIC 2 QUESTION 8 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 8

Topic #: 2

[\[All 312-50 Questions\]](#)

---

A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

- A. white box
- B. grey box
- C. red box
- D. black box

[Hide Answer](#)

**Suggested Answer:** D

---

by  [DjoCh](#) at Nov. 23, 2022, 7:14 p.m.

### Comments

  [kodji](#) 1 year, 2 months ago

In a black-box testing assignment, the penetration tester is placed in the role of the average hacker, with no internal knowledge of the target system. Testers are not provided with any architecture diagrams or source code that is not publicly available. A black-box penetration test determines the vulnerabilities in a system that are exploitable from outside the network.

upvoted 1 times

  [karthik\\_2003](#) 1 year, 5 months ago

Black box scanning is a method of software security testing in which the security controls, defenses and design of an application are tested from the outside-in, with little or no prior knowledge of the application's internal workings. It is typically used to test web applications and web services.

upvoted 2 times

  [DjoCh](#) 2 years ago

i confirm D  
the black box scan shoud be done without credential

upvoted 2 times

## EXAM 312-50V11 TOPIC 1 QUESTION 278 DISCUSSION

Actual exam question from ECCouncil's 312-50v11

Question #: 278

Topic #: 1

[All 312-50v11 Questions]

```
#!/usr/bin/python import socket buffer=[““A””] counter=50 while len(buffer)<=100:
buffer.append (““A””*counter) counter=counter+50 commands= [““HELP””,““STATS .””,
““RTIME .””,““LTIME .””,““SRUN .””,““TRUN .””,““GMON .””,““GDOG .””,““KSTET .””,
““GTER .””,““HTER .””, ““LTER .””,““KSTAN .””] for command in commands: for
buffstring in buffer: print ““Exploiting”” +command +““:””+str(len(buffstring))
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM) s.connect((‘127.0.0.1’, 9999))
s.recv(50) s.send(command+buffstring) s.close()
```

What is the code written for?

- A. Denial-of-service (DOS)
- B. Buffer Overflow **Most Voted**
- C. Bruteforce
- D. Encryption

[Hide Answer](#)

**Suggested Answer: B**

*Community vote distribution*

B (100%)

by  [josevirtual](#) at Dec. 14, 2022, 6:12 p.m.

### Comments

 **mdmdmd** 1 year, 4 months ago

so obvious with the lines  
upvoted 2 times

 **josevirtual** 1 year, 5 months ago

**Selected Answer: B**  
Seems obvious  
upvoted 1 times

## EXAM 312-50 TOPIC 8 QUESTION 229 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 229

Topic #: 8

[\[All 312-50 Questions\]](#)

While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?

- A. The port will send an ACK
- B. The port will send a SYN
- C. The port will ignore the packets Most Voted
- D. The port will send an RST

[Hide Answer](#)

**Suggested Answer: C**

Reference: <https://nmap.org/book/man-port-scanning-techniques.html>

*Community vote distribution*

 C (100%)

by  salei at Dec. 21, 2022, 2:26 p.m.

### Comments

  salei 1 year, 5 months ago

Selected Answer: C

Xmas scan is a type of inverse TCP scanning technique with the FIN, URG, and PUSH flags set to send a TCP frame to a remote device. If the target has opened the port, then you will receive no response from the remote system. If the target has closed the port, then you will receive a remote system reply with an RST.

upvoted 1 times

## EXAM 312-50 TOPIC 8 QUESTION 293 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 293

Topic #: 8

[\[All 312-50 Questions\]](#)

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible? (Choose two.)

- A. It used TCP as the underlying protocol.
- B. It uses community string that is transmitted in clear text. Most Voted
- C. It is susceptible to sniffing. Most Voted
- D. It is used by all network devices on the market.

[Hide Answer](#)

**Suggested Answer: BD**

*Community vote distribution*

BC (100%)

by  salei at Dec. 28, 2022, 6:10 p.m.

### Comments

  salei 1 year, 5 months ago

Selected Answer: BC

We cannot say that D is true. Not all network devices use SNMP. However, it's susceptible to sniffing, especially in its version 1 and 2  
upvoted 2 times

## EXAM 312-50 TOPIC 3 QUESTION 24 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 24

Topic #: 3

[\[All 312-50 Questions\]](#)

What is the main reason the use of a stored biometric is vulnerable to an attack?

- A. The digital representation of the biometric might not be unique, even if the physical characteristic is unique.
- B. Authentication using a stored biometric compares a copy to a copy instead of the original to a copy.
- C. A stored biometric is no longer "something you are" and instead becomes "something you have".
- D. A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric. Most Voted

[Hide Answer](#)

**Suggested Answer: D**

*Community vote distribution*

D (100%)

by  [Hemanshu87](#) at Dec. 31, 2022, 5:38 p.m.

### Comments

  [Hemanshu87](#) 1 year, 5 months ago

[Selected Answer: D](#)

Vulnerable to manually prompting users, e.g. touch ID scams that targeted Apple devices  
upvoted 1 times

## EXAM 312-50 TOPIC 3 QUESTION 25 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 25

Topic #: 3

[\[All 312-50 Questions\]](#)

During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

- A. The tester must capture the WPA2 authentication handshake and then crack it. **Most Voted**
- B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
- C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
- D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

[Hide Answer](#)

**Suggested Answer: A**

*Community vote distribution*

A (100%)

by  [Hemanshu87](#) at Dec. 31, 2022, 5:51 p.m.

### Comments

  [Hemanshu87](#) 1 year, 5 months ago

**Selected Answer: A**

Sniffing 4-way handshake

- 4-way handshake is the ceremony between AP and the device
- Vulnerability in WPA and WPA-Personal (WPA-PSK, pre-shared key)
- During WPA handshake, password is shared in encrypted form (called PMK (pairwise master key))

upvoted 1 times

## EXAM 312-50 TOPIC 1 QUESTION 3 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 3

Topic #: 1

[\[All 312-50 Questions\]](#)

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 corporate network. What tool should the analyst use to perform a Blackjacking attack?

A. Paros Proxy

B. BBProxy

C. BBCrack

D. Blooover

[Hide Answer](#)

### **Suggested Answer: B**

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>

by  **AmalUB** at Feb. 4, 2023, 4:32 a.m.

## Comments

 **Erpan1143** 2 years, 2 months ago

Answer B

upvoted 1 times

 **Ramaz\_Azam** 2 years, 3 months ago

b:BBPROXY

upvoted 1 times

 **AmalUB** 2 years, 9 months ago

B

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 1 times

## EXAM 312-50 TOPIC 1 QUESTION 4 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 4

Topic #: 1

[\[All 312-50 Questions\]](#)

Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

- A. Restore a random file.
- B. Perform a full restore.
- C. Read the first 512 bytes of the tape.
- D. Read the last 512 bytes of the tape.

[Hide Answer](#)

**Suggested Answer: B**

A full restore is required.

by  **AmalUB** at Feb. 4, 2023, 4:35 a.m.

### Comments

  **Ramaz\_Azam** 2 years, 3 months ago

B: A full restore is required.

upvoted 2 times

  **AmalUB** 2 years, 9 months ago

Answer B

A full restore is required.

upvoted 2 times

## EXAM 312-50 TOPIC 1 QUESTION 9 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 9

Topic #: 1

[\[All 312-50 Questions\]](#)

---

In order to show improvement of security over time, what must be developed?

- A. Reports
- B. Testing tools
- C. Metrics
- D. Taxonomy of vulnerabilities

[Hide Answer](#)

**Suggested Answer: C**

Today, management demands metrics to get a clearer view of security.

Metrics that measure participation, effectiveness, and window of exposure, however, offer information the organization can use to make plans and improve programs.

References: <http://www.infoworld.com/article/2974642/security/4-security-metrics-that-matter.html>

---

by  **AmalUB** at Feb. 4, 2023, 4:41 a.m.

### Comments

 **AmalUB** 1 year, 3 months ago

Answer C

Today, management demands metrics to get a clearer view of security.

Metrics that measure participation, effectiveness, and window of exposure, however, offer information the organization can use to make plans and improve programs

upvoted 2 times

## EXAM 312-50 TOPIC 2 QUESTION 2 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 2

Topic #: 2

[\[All 312-50 Questions\]](#)

---

How can rainbow tables be defeated?

- A. Password salting
- B. Use of non-dictionary words
- C. All uppercase character passwords
- D. Lockout accounts under brute force password cracking attempts

[Hide Answer](#)

**Suggested Answer:** A

---

by  **AmalUB** at Feb. 4, 2023, 4:43 a.m.

### Comments

 **AmalUB** 1 year, 3 months ago

Answer A

upvoted 2 times

## EXAM 312-50 TOPIC 2 QUESTION 3 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 3

Topic #: 2

[\[All 312-50 Questions\]](#)

The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

```
[ATTEMPT] target 192.168.1.106 - login "root" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20
```

What is most likely taking place?

- A. Ping sweep of the 192.168.1.106 network
- B. Remote service brute force attempt**
- C. Port scan of 192.168.1.106
- D. Denial of service attack on 192.168.1.106

[Hide Answer](#)

**Suggested Answer: B**

*Community vote distribution*

C (100%)

by  [AmalUB](#) at Feb. 4, 2023, 4:44 a.m.

### Comments

 **Booict** 10 months, 3 weeks ago

**Selected Answer: C**

C - A port scan involves probing a target machine to identify open ports and services running on those ports  
upvoted 1 times

 **AmalUB** 1 year, 3 months ago

Answer B  
upvoted 3 times

## EXAM 312-50 TOPIC 2 QUESTION 4 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 4

Topic #: 2

[\[All 312-50 Questions\]](#)

An NMAP scan of a server shows port 25 is open. What risk could this pose?

- A. Open printer sharing
- B. Web portal data leak
- C. Clear text authentication
- D. Active mail relay

[Hide Answer](#)

**Suggested Answer:** D

by  **AmalUB** at Feb. 4, 2023, 4:44 a.m.

### Comments

 **DzbuJ** 1 year, 1 month ago

D is correct

upvoted 2 times

 **MacDee31** 1 year, 2 months ago

Answer is D because port 25 is a SMTP port.

upvoted 2 times

 **AmalUB** 1 year, 9 months ago

Answer D

upvoted 2 times

## EXAM 312-50 TOPIC 3 QUESTION 50 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 50

Topic #: 3

[\[All 312-50 Questions\]](#)

WPA2 uses AES for wireless data encryption at which of the following encryption levels?

- A. 64 bit and CCMP
- B. 128 bit and CRC
- C. 128 bit and CCMP**
- D. 128 bit and TKIP

[Hide Answer](#)

**Suggested Answer: C**

by  **Had20ck** at Feb. 6, 2023, 10:15 a.m.

### Comments

 **Novmejst** 1 year, 1 month ago

WPA CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is an encryption protocol that is used to secure Wi-Fi networks.

upvoted 1 times

 **Had20ck** 1 year, 3 months ago

<https://www.controleng.com/articles/wireless-security-ieee-802-11-and-ccmp-aes/>

upvoted 1 times

## EXAM 312-50 TOPIC 3 QUESTION 55 DISCUSSION

Actual exam question from ECCouncil's 312-50

Question #: 55

Topic #: 3

[\[All 312-50 Questions\]](#)

---

The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

- A. An attacker, working slowly enough, can evade detection by the IDS. Most Voted
- B. Network packets are dropped if the volume exceeds the threshold.
- C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.
- D. The IDS will not distinguish among packets originating from different sources.

[Hide Answer](#)

**Suggested Answer: A**

*Community vote distribution*

A (100%)

---

by  [Had20ck](#) at Feb. 6, 2023, 10:52 a.m.

### Comments

  [greeklover84](#) 1 year, 5 months ago

Selected Answer: A

Agree A

upvoted 1 times

  [Had20ck](#) 2 years, 9 months ago

[https://en.wikipedia.org/wiki/Intrusion\\_detection\\_system\\_evasion\\_techniques#:~:text=An%20IDS%20can%20be%20evaded,host%20without%20alerting%20the%20IDS.](https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#:~:text=An%20IDS%20can%20be%20evaded,host%20without%20alerting%20the%20IDS.)

upvoted 1 times