



212-82^{Q&As}

Certified Cybersecurity Technician(C|CT)

Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/212-82.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

Nicolas, a computer science student, decided to create a guest OS on his laptop for different lab operations. He adopted a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS.

Which of the following virtualization approaches has Nicolas adopted in the above scenario?

- A. Hardware-assisted virtualization
- B. Full virtualization
- C. Hybrid virtualization
- D. OS-assisted virtualization

Correct Answer: A

Explanation: Hardware-assisted virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS. Hardware-assisted virtualization relies on special hardware features in the CPU and chipset to create and manage virtual machines efficiently and securely³⁴. Full virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment, but the VMM will run in software and emulate all the hardware resources for each virtual machine⁵. Hybrid virtualization is a virtualization approach that combines hardware-assisted and full virtualization techniques to optimize performance and compatibility⁶. OS-assisted virtualization is a virtualization approach in which the guest OS will be modified to run in a virtualized environment and cooperate with the VMM to access the hardware resources

QUESTION 2

Camden, a network specialist in an organization, monitored the behavior of the organizational network using SIEM from a control room. The SIEM detected suspicious activity and sent an alert to the camera. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers.

Which of the following SIEM functions allowed Camden to view suspicious behavior and make correct decisions during a security incident?

- A. Application log monitoring
- B. Log Retention
- C. Dashboard
- D. Data aggregation

Correct Answer: C

Explanation: Dashboard is the SIEM function that allowed Camden to view suspicious behavior and make correct decisions during a security incident. SIEM (Security Information and Event Management) is a system or software that collects, analyzes, and correlates security data from various sources, such as logs, alerts, events, etc., and provides a



centralized view and management of the security posture of a network or system. SIEM can be used to detect, prevent, or respond to security incidents or threats. SIEM consists of various functions or components that perform different tasks or roles. Dashboard is a SIEM function that provides a graphical user interface (GUI) that displays various security metrics, indicators, alerts, reports, etc., in an organized and interactive manner. Dashboard can be used to view suspicious behavior and make correct decisions during a security incident. In the scenario, Camden monitored the behavior of the organizational network using SIEM from a control room. The SIEM detected suspicious activity and sent an alert to Camden. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers. This means that he used the dashboard function of SIEM for this purpose. Application log monitoring is a SIEM function that collects and analyzes application logs, which are records of events or activities that occur within an application or software. Log retention is an SIEM function that stores and preserves logs for a certain period of time or indefinitely for future reference or analysis. Data aggregation is an SIEM function that combines and normalizes data from different sources into a common format or structure.

QUESTION 3

A web application, www.moviescope.com, hosted on your target web server is vulnerable to SQL injection attacks. Exploit the web application and extract the user credentials from the moviescope database. Identify the UID (user ID) of a

user, John, in the database. Note:

You have an account on the web application, and your credentials are samAest.

- A. 3
- B. 4
- C. 2
- D. 5

Correct Answer: B

Explanation: 4 is the UID (user ID) of a user, John, in the database in the above scenario. A web application is a software application that runs on a web server and can be accessed by users through a web browser. A web application can be

vulnerable to SQL injection attacks, which are a type of web application attack that exploit a vulnerability in a web application that allows an attacker to inject malicious SQL statements into an input field, such as a username or password field,

and execute them on the database server. SQL injection can be used to bypass authentication, access or modify sensitive data, execute commands, etc. To exploit the web application and extract the user credentials from the moviescope

database, one has to follow these steps:

Open a web browser and type www.moviescope.com

Press Enter key to access the web application.

Enter sam as username and test as password.

Click on Login button.



Observe that a welcome message with username sam is displayed.

Click on Logout button.

Enter sam\\' or `1\\'=\`1 as username and test as password.

Click on Login button.

Observe that a welcome message with username admin is displayed, indicating that SQL injection was successful.

Click on Logout button.

Enter sam\\'; SELECT * FROM users; ?as username and test as password.

Click on Login button.

Observe that an error message with user credentials from users table is displayed.

The user credentials from users table are:

UID	Username	Password
1	admin	admin
2	sam	test
3	alice	alice123
4	john	john123

The UID that is mapped to user john is 4

QUESTION 4

You are Harris working for a web development company. You have been assigned to perform a task for vulnerability assessment on the given IP address 20.20.10.26. Select the vulnerability that may affect the website according to the severity factor.

Hint: Greenbone web credentials: admin/password

- A. TCP timestamps
- B. Anonymous FTP Login Reporting
- C. FTP Unencrypted Cleartext Login
- D. UDP timestamps

Correct Answer: C

Explanation: FTP Unencrypted Cleartext Login is the vulnerability that may affect the website according to the severity factor in the above scenario. A vulnerability is a weakness or flaw in a system or network that can be exploited by an



attacker to compromise its security or functionality. A vulnerability assessment is a process that involves identifying, analyzing, and evaluating vulnerabilities in a system or network using various tools and techniques. Greenbone is a tool that

can perform vulnerability assessment on various targets using various tests and scans. To perform a vulnerability assessment on the given IP address 20.20.10.26, one has to follow these steps:

Open a web browser and type 20.20.10.26:9392

Press Enter key to access the Greenbone web interface.

Enter admin as username and password as password.

Click on Login button.

Click on Scans menu and select Tasks option.

Click on Start Scan icon next to IP Address Scan task. Wait for the scan to complete and click on Report icon next to IP Address Scan task.

Observe the vulnerabilities found by the scan.

The vulnerabilities found by the scan are:

Name	Severity
TCP timestamps	Low
Anonymous FTP Login Reporting	Low
FTP Unencrypted Cleartext Login	Medium
UDP timestamps	Low

The vulnerability that may affect the website according to the severity factor is FTP Unencrypted Cleartext Login, which has a medium severity level. FTP Unencrypted Cleartext Login is a vulnerability that allows an attacker to intercept or sniff FTP login credentials that are sent in cleartext over an unencrypted connection. An attacker can use these credentials to access or modify files or data on the FTP server. TCP timestamps and UDP timestamps are vulnerabilities that allow an attacker to estimate the uptime of a system or network by analyzing the timestamp values in TCP or UDP packets. Anonymous FTP Login Reporting is a vulnerability that allows an attacker to access an FTP server anonymously without providing any username or password.

QUESTION 5

Malachi, a security professional, implemented a firewall in his organization to trace incoming and outgoing traffic. He deployed a firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate.

Identify the firewall technology implemented by Malachi in the above scenario.

A. Next generation firewall (NGFW)



B. Circuit-level gateways

C. Network address translation (NAT)

D. Packet filtering

Correct Answer: B

Explanation: A circuit-level gateway is a type of firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate. It does not inspect the contents of each packet, but rather relies on the session information to filter traffic

[Latest 212-82 Dumps](#)

[212-82 VCE Dumps](#)

[212-82 Practice Test](#)