Eccouncil 212-82 Practice Questions

Shared by Clayton on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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

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

Question Type: MultipleChoice

You are investigating a data leakage incident where an insider is suspected of using image steganography to send sensitive information to a competitor. You have also recovered a VeraCrypt volume file S3cr3t from the suspect. The VeraCrypt volume file is available In the Pictures folder of the Attacker Machined. Your task Is to mount the VeraCrypt volume, find an image file, and recover the secret code concealed in the file. Enter the code as the answer. Hint: If required, use sniffer@123 as the password to mount the VeraCrypt volume file. (Practical Question)

Options:

A- L76D2E8CBA1K
B- H364F9F4FD3H
C- J782C8C2EH6J
D- G85E2C7AB1R6

Answer:

B

Explanation:

Mounting the VeraCrypt Volume:

Use VeraCrypt to mount the volume file S3cr3t located in the Pictures folder. The provided password sniffer@123 is required to mount the volume.

Locating the Image File:

After mounting the volume, browse through the files to locate the image file that may contain the secret code through steganography.

Extracting the Secret Code:

Use steganography tools to analyze the image file and extract the hidden secret code. Tools such as Stegsolve or Steghide can be used for this purpose.

Recovering the Code:

The extracted secret code from the image file is H364F9F4FD3H.

The recovered secret code from the image file is H364F9F4FD3H.

Question 3

Question Type: MultipleChoice

A renowned research institute with a high-security wireless network recently encountered an advanced cyber attack. The attack was not detected by traditional security measures and resulted in significant data exfiltration. The wireless network was equipped with WPA3 encryption, MAC address filtering, and had disabled SSID broadcasting. Intriguingly. the attack occurred without any noticeable disruption or changes in network performance. After an exhaustive forensic analysis, the cybersecurity team pinpointed the attack method. Which option best wireless network-specific attacks was most likely used?

Options:

A- Jamming Attack, disrupting network communications with interference signals
B- Evil Twin Attack, where a rogue access point mimics a legitimate one to capture network traffic
C- Bluesnarfing. exploiting Bluetooth connections to access network data
D- KRACK (Key Reinstallation Attack), exploiting vulnerabilities in the WPA2 protocol

Answer:

B

Explanation:

Definition of Evil Twin Attack:

An Evil Twin Attack involves setting up a rogue access point that mimics a legitimate Wi-Fi network. Unsuspecting users connect to this rogue AP, allowing the attacker to intercept and capture network traffic.

Bypassing Security Measures:

Even with WPA3 encryption, MAC address filtering, and disabled SSID broadcasting, an Evil Twin can trick users into connecting by mimicking the legitimate network's SSID and signal strength.

Stealth and Detection:

The attack can be performed without noticeable disruption to the network, as the rogue AP simply relays traffic to the legitimate network, making it hard to detect through traditional measures.

Forensic Analysis:

Forensic analysis revealing the method indicates that sophisticated techniques were used to capture and exfiltrate data without triggering security alarms.

Given the described security environment and the nature of the attack, an Evil Twin Attack is the most likely method used.

Question 4

Question Type: MultipleChoice

As a system administrator handling the integration of a recently acquired subsidiary's Linux machines with your company's Windows environment for centralized log management, What is your most significant challenge likely to be?

Options:

A- Dealing with the sheer volume of logs generated by both systems.
B- Navigating the different user interfaces of the built-in log viewers (Event Viewer vs. Syslog).
C- Finding skilled personnel proficient in both Windows and Linux log management tools.
D- Managing the incompatibility of log formats used by Windows and Linux systems.

Answer:

D

Explanation:

Integrating Linux machines with a Windows environment for centralized log management poses significant challenges, primarily due to the incompatibility of log formats:

Log Format Differences:

Windows: Uses Event Viewer to store logs in a proprietary format.

Linux: Uses Syslog to store logs in plain text files with a different structure.

Centralized Management: To achieve effective centralized log management, logs from both systems need to be normalized into a common format.

Solutions:

Log Aggregators: Tools like Logstash or Fluentd can collect, parse, and transform logs from different systems into a unified format.

SIEM Systems: Security Information and Event Management (SIEM) systems like Splunk or ELK

Stack can handle log ingestion from multiple sources, normalizing data for analysis.

SIEM Implementation Guides: Splunk Documentation

Log Management Best Practices: Syslog-ng Documentation

Question 5

Question Type: MultipleChoice

You are the lead cybersecurity analyst for a multinational corporation that handles sensitive financial dat

a. As part of your network security strategy, you have implemented both an Intrusion Detection System (IDS) and an Intrusion Prevention System(IPS) to safeguard against cyber threats. One day, your IDS alerts you to suspicious activity on the network, indicating a potential intrusion attempt from an external source. Meanwhile, your IPS springs into action, swiftly blocking the malicious traffic before it can penetrate deeper into the network. Based on this scenario, what primarily distinguishes the role of the IDS from the IPS In your network security architecture?

Options:

A- The IDS primarily uses signature-based detection techniques, while the IPS relies primarily on anomaly-based detection methods.
B- The IDS operates solely at the network perimeter, while the IPS can also monitor and protect internal network traffic.
C- The IDS focuses on identifying suspicious activities and generating alerts, while the IPS actively blocks and mitigates potential threats in real-time.
D- The IDS requires manual intervention for threat mitigation, while the IPS can autonomously respond to threats without human intervention.

Answer:

C

Explanation:

The primary distinction between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) lies in their response to detected threats:

Intrusion Detection System (IDS):

Function: Monitors network traffic and system activities for suspicious behavior.

Response: Generates alerts and logs events for analysis.

Role: Passive; does not take action to block or prevent threats. Requires manual intervention to respond to alerts.

Intrusion Prevention System (IPS):

Function: Monitors network traffic and system activities similarly to an IDS but with additional capabilities.

Response: Actively blocks and mitigates threats in real-time.

Role: Proactive; takes automatic actions to prevent or mitigate threats without the need for human intervention.

Scenario Explanation:

In the given scenario, the IDS detected suspicious activity and alerted the security team, allowing them to investigate further.

The IPS, on the other hand, immediately blocked the malicious traffic, preventing the intrusion from succeeding.

EC-Council Certified Network Defender (CND) and Certified Security Analyst (ECSA) materials.

Industry standards on network security and intrusion detection/prevention systems.

Question 6

Question Type: MultipleChoice

Finley, a security professional at an organization, was tasked with monitoring the organizational network behavior through the SIEM dashboard. While monitoring, Finley noticed suspicious activities in the network; thus, he captured and analyzed a single network packet to determine whether the signature included malicious patterns. Identify the attack signature analysis technique employed by Finley in this scenario.

Options:

A- Context-based signature analysis
B- Atomic-signature-based analysis
C- Composite signature-based analysis
D- Content-based signature analysis

Answer:

D

Explanation:

Content-based signature analysis is the attack signature analysis technique employed by Finley in this scenario. Content-based signature analysis is a technique that captures and analyzes a single network packet to determine whether the signature included malicious patterns. Content-based signature analysis can be used to detect known attacks, such as buffer overflows, SQL injections, or cross-site scripting2.

Question 7

Question Type: MultipleChoice

Calvin spotted blazing flames originating from a physical file storage location in his organization because of a Short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large are

a. Which of the following firefighting systems did Calvin use in this scenario?

Options:

A- Fire detection system
B- Sprinkler system
C- Smoke detectors
D- Fire extinguisher

Answer:

D

Explanation:

Fire extinguisher is the firefighting system that Calvin used in this scenario. A firefighting system is a system that detects and suppresses fire in a physical location or environment. A firefighting system can consist of various components, such as sensors, alarms, sprinklers, extinguishers, etc. A firefighting system can use various agents or substances to suppress fire, such as water, foam, gas, powder, etc. A fire extinguisher is a portable device that contains an agent or substance that can be sprayed or discharged onto a fire to extinguish it . A fire

extinguisher can be used to curb fire in the initial stage and prevent it from spreading over a large area . In the scenario, Calvin spotted blazing flames originating from a physical file storage location in his organization because of a short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large area. This means that he used a fire extinguisher for this purpose. A fire detection system is a system that detects the presence of fire by sensing its characteristics, such as smoke, heat, flame, etc., and alerts the occupants or authorities about it . A sprinkler system is a system that consists of pipes and sprinkler heads that release water onto a fire when activated by heat or smoke. A smoke detector is a device that senses smoke and emits an audible or visual signal to warn about fire.

Question 8

Question Type: MultipleChoice

You work in a Multinational Company named Vector Inc. on Hypervisors and Virtualization Software. You are using the Operating System (OS) Virtualization and you have to handle the Security risks associated with the OS virtualization. How can you mitigate these security risks?

Options:

A- Isolate the affected cloud servers and redirect traffic to backup servers, ensuring continuous service while initiating a deep-dive analysis of the suspicious activities using cloud-native security tools.
B- Implement least privilege access control for users managing VMs.
C- Regularly patch and update the hypervisor software for security fixes.
D- Disable security features on virtual machines to improve performance.

Answer:

A

Explanation:

Mitigating security risks associated with OS virtualization involves a comprehensive approach. Here's a breakdown of the steps:

Implement Least Privilege Access Control for Users Managing VMs:

Limit access to only those users who need it.

Ensure that users have only the permissions necessary to perform their tasks.

Regularly Patch and Update the Hypervisor Software for Security Fixes:

Keep the hypervisor and virtualization software up-to-date to protect against known vulnerabilities.

Regular patching minimizes the risk of exploitation.

Disable Security Features on Virtual Machines to Improve Performance:

Note: This is actually a security risk. The correct approach is to enable and configure security features to protect VMs, despite the potential minor impact on performance.

Comprehensive Approach:

A holistic security strategy includes enforcing least privilege, maintaining updated systems, and enabling security features on VMs to protect against a wide range of threats.

EC-Council Certified Ethical Hacker (CEH) materials.

Best practices for virtualization security from NIST and other cybersecurity frameworks.