Eccouncil 212-89 Practice Questions

Shared by Beasley on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following processes is referred to as an approach to respond to the security incidents that occurred in an organization and enables the response team by ensuring that they know exactly what process to follow in case of security incidents?

Options:

A- Risk assessment
B- Incident response orchestration
C- Vulnerability management
D- Threat assessment

Answer:

B

Explanation:

Incident response orchestration refers to the process and technologies used to coordinate and streamline the response to security incidents. This approach ensures that incident response teams have clear procedures and workflows to follow, enabling them to act swiftly and effectively when dealing with security incidents. By orchestrating the response, organizations can minimize the impact of incidents, ensure consistent and thorough investigation and remediation activities, and improve their overall security posture. Incident response orchestration involves integrating various security tools, automating response actions where possible, and providing a centralized platform for managing incidents.

Question 2

Question Type: MultipleChoice

Meera, part of the Incident Handling & Response (IH&R) team, identifies an ongoing phishing campaign targeting internal employees. She immediately circulates an organization-wide alert, warning staff not to engage with the suspicious email. Along with the alert, she provides visual cues and instructions on how to recognize similar phishing threats in the future. Her goal is to prevent further damage and strengthen employee awareness. What additional action would best align with Meera's eradication efforts?

Options:

A- Installing anti-DDoS tools
B- Sharing threat details with security forums
C- Issuing server restart commands
D- Deleting user accounts
Comprehensive and Detailed Explanation (ECIH-aligned):
In the ECIH email incident response framework, eradication extends beyond internal cleanup and includes threat intelligence sharing. Option B is correct because sharing phishing indicators with trusted security communities helps disrupt attacker infrastructure and prevents reuse of the same campaign against other organizations.
Option A is unrelated. Option C is ineffective against phishing. Option D is overly destructive and unnecessary.
ECIH promotes collaborative defense as part of post-detection eradication and prevention.

Answer:

B

Question 3

Question Type: MultipleChoice

Malicious Micky has moved from the delivery stage to the exploitation stage of the kill chain. This malware wants to find and report to the command center any useful services on the system. Which option best recon attacks is the MOST LIKELY to provide this information?

Options:

A- IP range sweep
B- Packet sniffing
C- Session hijack
D- Port scan
When malware moves from the delivery stage to the exploitation stage in the cyber kill chain, its objective often shifts to identifying exploitable vulnerabilities within the targeted system. A port scan is a technique used to discover services that are listening on ports within a system. By scanning the system's ports, the malware can identify open ports and the services running on them, providing valuable information about potential entry points for further exploitation. This type of reconnaissance attack is aimed at gathering intelligence on the target system's network services, which can then be reported back to a command and control center for further malicious activity planning.
Port scanning is more relevant than IP range sweeps, packet sniffing, or session hijacking for identifying useful services on a system because it directly targets the discovery of accessible network services and their corresponding ports. While the other methods can also be part of the

reconnaissance phase, they serve different purposes: IP range sweeps aim to identify active IP addresses, packet sniffing intercepts data packets to gather information, and session hijacking involves taking over a valid user session. In contrast, port scanning is specifically designed to enumerate services that could be exploited.

Answer:

D

Question 4

Question Type: MultipleChoice

Zoe, a security analyst, deploys a high-interaction honeypot in the DMZ that mimics critical systems and monitors logs for scans, exploit attempts, and lateral movement techniques. What is the main purpose of Zoe's activity?

Options:

A- Deceiving attackers to study their behavior.
B- Preventing malware execution using sandboxing.
C- Blocking DDoS traffic through ACL rules.
D- Testing the organization's backup and recovery systems.
Explanation (aligned to threat intelligence & detection):
A high-interaction honeypot is designed to attract and engage adversaries, providing realistic services so defenders can observe tactics, techniques, and procedures (TTPs) with higher fidelity than a low-interaction decoy. The goal is not to ''stop'' attacks directly, but to detect and learn: identify scanning patterns, credential stuffing attempts, exploit chains, payload delivery methods, and post-exploitation behaviors such as enumeration and lateral movement. That intelligence is then used to improve controls---signatures, detections, segmentation, and hardening priorities.
Sandboxing (B) is typically about detonating suspicious files/URLs to observe behavior in a controlled environment; it's not what a DMZ honeypot primarily does. ACL rules and DDoS blocking (C) are traffic filtering measures, not deception telemetry. Backup/recovery testing (D) is resilience planning, unrelated to studying attacker behavior in real-time.
In incident handling terms, honeypots support the ''preparation'' and ''detection'' posture---expanding visibility, generating early warning, and enriching threat intelligence. They can also reduce risk by luring opportunistic attackers away from production assets, but their primary value is behavioral observation and evidence collection.

Answer:

A

Question 5

Question Type: MultipleChoice

OmegaTech Corp identified unauthorized remote access to its primary server and data exfiltration tunnels. Simultaneously, IoT device firmware corruption was reported. As the first responder, what should Olivia prioritize?

Options:

A- Start reinstalling IoT firmware
B- Begin isolating the primary server and cutting off remote access
C- Alert all divisions to initiate a system-wide shutdown
D- Engage the AI-driven security system to trace unauthorized access
Comprehensive and Detailed Explanation (ECIH-aligned):
ECIH prioritizes containment of the most critical threat vector. The primary server actively exfiltrating data represents the highest risk.
Option B is correct because isolating the primary server immediately stops data loss and attacker control. IoT remediation can follow once core assets are secured.
Options A and D delay containment. Option C causes unnecessary disruption.
ECIH stresses that responders must address the most damaging threat first, making Option B correct.

Answer:

B

Question 6

Question Type: MultipleChoice

Malicious downloads that result from malicious office documents being manipulated are caused by which of the following?

Options:

A- Clickjacking
B- Impersonation
C- Registry key manipulation
D- Macro abuse
Malicious downloads initiated through manipulated office documents typically involve macro abuse. Macros are scripts that can automate tasks within documents and are embedded within Office documents like Word, Excel, and PowerPoint files. While macros can be used for

legitimate purposes, they can also be abused by attackers to execute malicious code. When an office document with a malicious macro is opened, and macros are enabled, the macro can run arbitrary code that leads to malicious downloads, installing malware or performing other unauthorized actions on the victim's system.
Macro abuse has become a common vector for cyber attacks, as it exploits the functionality of widely used office applications. Attackers often craft phishing emails with attachments or links to documents that contain malicious macros, tricking users into enabling macros to execute the malicious code. This method is effective for bypassing some security measures since it relies on user interaction and exploitation of legitimate features.

Answer:

D

Question 7

Question Type: MultipleChoice

GlobalCorp, a leading software development company, recently launched a cloud-based CRM application. However, within a week, customers reported unauthorized access incidents. On investigation, it was discovered that the vulnerability was due to improper session management, allowing session fixation attacks. How should GlobalCorp address this vulnerability?

Options:

A- Implement CAPTCHA on all login pages.
B- Rotate session tokens after successful login.
C- Increase the complexity of user passwords.
D- Store session IDs in encrypted cookies.
Comprehensive and Detailed Explanation (ECIH-aligned):
This scenario involves a session fixation vulnerability, a well-known web application attack where an attacker forces or predicts a session identifier and then tricks a user into authenticating with that session. According to the ECIH web application security module, proper session management is essential to prevent such attacks.
Option B is correct because rotating or regenerating session tokens immediately after successful authentication ensures that any session identifier known to an attacker becomes invalid. This breaks the attack chain inherent in session fixation attacks. ECIH explicitly identifies session regeneration as a primary mitigation control.
Option A helps against automated abuse but does not address session reuse. Option C strengthens authentication but does not prevent session hijacking. Option D improves confidentiality but does not prevent fixation if the same session ID remains valid.
ECIH stresses that authentication and session management must be treated as distinct security controls. Even strong passwords cannot protect against flawed session handling. Therefore, regenerating session tokens post-login is the correct and most effective remediation.

Answer:

B

Question 8

Question Type: MultipleChoice

Robert is an incident handler working for Xsecurity Inc. One day, his organization faced a massive cyberattack and all the websites related to the organization went offline. Robert was on duty during the incident and he was responsible to handle the incident and maintain business continuity. He immediately restored the web application service with the help of the existing backups.

According to the scenario, which of the following stages of incident handling and response (IH&R) process does Robert performed?

Options:

A- Evidence gathering and forensics analysis
B- Eradication
C- Notification
D- Recovery

Restoring web application services with the help of existing backups, as performed by Robert, falls under the Recovery stage of the Incident Handling and Response (IH&R) process. The Recovery stage involves actions taken to return the organization to normal operations after an incident, which includes restoring systems to their operational state using backups, patching vulnerabilities, and ensuring that all systems are clean and secure before being brought back online. This step is crucial for resuming business operations and mitigating the impact of the incident.

Answer:

D

Question 9

Question Type: MultipleChoice

SWA Cloud Services added PKI as one of their cloud security controls. What does PKI stand for?

Options:

A- Private key infrastructure
B- Private key in for ma lion
C- Public key information
D- Public key infrastructure

Public Key Infrastructure (PKI) is a framework used to manage digital certificates and public-key encryption. It enables secure electronic transfer of information for a range of network activities such as e-commerce, internet banking, and confidential email. PKI is fundamental to the management of encryption keys and digital certificates, ensuring the secure exchange of data over networks and verification of identity.

Answer:

D

To Get Premium Files for 212-89 Visit

https://www.p2pexams.com/products/212-89

For More Free Questions Visit

https://www.p2pexams.com/eccouncil/pdf/212-89