

EC-COUNCIL.212-89.v2026-10-20.q204

Exam Code:	212-89
Exam Name:	EC Council Certified Incident Handler (ECIH v3)
Certification Provider:	EC-COUNCIL
Free Question Number:	204
Version:	v2026-10-20
# of views:	164
# of Questions views:	2040
https://www.freepdfdumps.com/EC-COUNCIL.212-89.v2026-10-20.q204.html	

NEW QUESTION: 1

During a routine incident response process in a large organization, the incident responder noticed some suspicious activities on the organization's database using ActivTrak. Several databases were accessed late at night, and the main culprit appears to be an internal employee. What should be the incident responder's immediate step in order to prevent further malicious activities?

- A. Disable the network connection for the whole organization until the situation is under control.
- B. Block all access for the suspicious employee, including email, application accounts, physical access cards, and network credentials.
- C. Change the passwords of all systems without notifying the employee.
- D. Inform the senior management about the issue for further action.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 2

Emma, a senior security engineer at a technology firm, discovered during a routine audit that several employees had been granted administrative access to sensitive systems, even though their roles did not require such access rights. One of these employees later accessed restricted financial data and attempted to modify audit logs. Which insider threat eradication measure would have best prevented this incident?

- A. Network segmentation
- B. Enhanced password policy
- C. Principle of least privilege through access controls
- D. User and entity behavior analytics

Answer: C (LEAVE A REPLY)

Applying least privilege ensures users receive only the access required for their job roles. Proper access controls would have prevented employees from having unnecessary

administrative rights, reducing the ability to access restricted financial data or modify audit logs.

NEW QUESTION: 3

James has been appointed as an incident handling and response (IH&R) team lead and he was assigned to build an IH&R plan along with his own team in the company. Identify the IH&R process step James is currently working on.

- A. Eradication
- B. Recovery
- C. Preparation
- D. Notification

Answer: C (LEAVE A REPLY)

In the context of incident handling and response (IH&R), the preparation phase is the initial step where teams and resources are organized to effectively respond to potential security incidents.

This phase involves building the IH&R team, developing incident response plans and policies, setting up communication channels, and ensuring that the team has the necessary tools and authority to act. James, being assigned to build an IH&R plan and organize his team, is engaging in the preparation step of the incident response process. This foundational step is crucial for ensuring a coordinated and efficient response to incidents when they occur.

NEW QUESTION: 4

Which of the following is not a countermeasure to eradicate inappropriate usage incidents?

- A. Avoid VPN and other secure network channels
- B. Register the user activity logs and keep monitoring them regularly
- C. Install firewall and IDS/IPS to block services that violate the organization's policy
- D. Always store the sensitive data in far located servers and restrict its access

Answer: A (LEAVE A REPLY)

Avoiding VPN (Virtual Private Network) and other secure network channels is not a countermeasure to eradicate inappropriate usage incidents. On the contrary, using VPNs and secure network channels is a best practice for enhancing security, as these technologies help protect data in transit, ensuring that it is encrypted and less susceptible to interception or eavesdropping. Countermeasures for inappropriate usage typically involve enhancing security and monitoring, not reducing the security of communications.

NEW QUESTION: 5

A multinational organization recently suffered a massive data breach, resulting in the exposure of sensitive customer information. As an EC-Council Certified Incident Handler (ECIH), you have been tasked with ensuring compliance with incident handling laws and

acts while handling this situation. The company operates in multiple jurisdictions, including Europe and the United States.

What should be your primary legal consideration in this scenario?

- A.** Report the incident to the Internet Crime Complaint Center (IC3) immediately.
- B.** Initiate a customer notification process as guided by the European Data Protection Directive.
- C.** Follow the mandates of the GDPR and the California Consumer Privacy Act (CCPA).
- D.** Conduct an internal audit to identify potential non-compliance areas.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 6

Jason is setting up a computer forensics lab and must perform the following steps:

1. physical location and structural design considerations;
2. planning and budgeting;
3. work area considerations;
4. physical security recommendations;
5. forensic lab licensing;
6. human resource considerations.

Arrange these steps in the order of execution.

- A.** 2 -> 1 -> 3 -> 6 -> 4 -> 5
- B.** 2 -> 3 -> 1 -> 4 -> 6 -> 5
- C.** 5 -> 2 -> 1 -> 3 -> 4 -> 6
- D.** 3 -> 2 -> 1 -> 4 -> 6 -> 5

Answer: A (LEAVE A REPLY)

Setting up a computer forensics lab involves several critical steps that need to be executed in a logical and efficient order. The correct sequence starts with planning and budgeting (2), as it is essential to understand the scope, resources, and financial commitment required for the lab. The next step involves considering the physical location and structural design (1) to ensure the lab meets operational needs and security requirements. Work area considerations (3) follow, focusing on the layout and functionality of the workspace. Human resource considerations (6) are crucial next, to ensure the lab is staffed with qualified personnel. Physical security recommendations (4) are then implemented to protect the lab and its resources. Finally, forensic lab licensing (5) ensures the lab operates within legal and regulatory frameworks.

NEW QUESTION: 7

Aaron, a digital first responder, is dispatched to an R&D lab after a suspected insider data breach involving intellectual property theft. Upon entering the lab, he observes fingerprint smudges on a workstation keyboard, oily residue on a DVD near the printer, and an unplugged USB drive on the desk. He documents the position of each item, uses gloves

and evidence tags, covers surfaces to prevent contamination, and restricts access to the area. Which best practice is Aaron demonstrating?

- A. Preserving trace-level physical indicators for attribution
- B. Isolating system peripherals for digital chain-of-custody
- C. Safeguarding volatile system state for RAM acquisition
- D. Capturing live session activity from open peripherals

Answer: A (LEAVE A REPLY)

This scenario focuses on physical forensic evidence preservation, a key concept in the ECIH First Response module. Trace-level indicators such as fingerprints, residues, and physical media can provide attribution in insider investigations.

Option A is correct because Aaron's actions prevent contamination or destruction of physical trace evidence that may later link the incident to a specific individual. ECIH stresses that digital investigations often involve physical evidence, especially in insider cases.

Options B-D focus on digital evidence, which is not the primary concern described here. Proper preservation of physical trace evidence supports attribution, legal proceedings, and disciplinary action, aligning fully with ECIH forensic readiness principles.

NEW QUESTION: 8

In a Distributed Denial of Service (DDoS) attack where numerous compromised machines are used to flood a single target, what is the term commonly used for these infected devices?

- A. Trojans
- B. Zombies
- C. Spyware
- D. Worms

Answer: B (LEAVE A REPLY)

A Distributed Denial of Service (DDoS) attack is a widespread cyber assault in which multiple compromised systems--often geographically distributed--are manipulated to flood a target (such as a server, website, or network) with massive volumes of traffic. The goal is to exhaust the resources of the target system, rendering it slow, unresponsive, or completely unavailable to legitimate users.

The individual machines used in such an attack are commonly referred to as "zombies" (option B). A zombie is a computer or device that has been silently compromised by malware--typically without the knowledge of its legitimate user. Once infected, the device becomes part of a botnet, a network of zombies controlled remotely by an attacker, also known as a bot herder.

These zombie systems lie dormant until activated, often receiving commands to participate in malicious activities such as:

DDoS attacks

Spam email distribution

Data theft

NEW QUESTION: 9

Drake is an incident handler in Dark CCloud Inc. He is intended to perform log analysis in order to detect traces of malicious activities within the network infrastructure. Which of the following tools Drake must employ in order to view logs in real time and identify malware propagation within the network?

- A. Splunk
- B. HULK
- C. Hydra
- D. LOIC

Answer: ([SHOW ANSWER](#))

Splunk is a powerful tool for log analysis, capable of collecting, analyzing, and visualizing data from various sources in real time. For an incident handler like Drake, intending to detect traces of malicious activities within the network infrastructure, Splunk can efficiently parse large volumes of log data, enabling the identification of patterns and anomalies that may indicate malware propagation or other security incidents. Its real-time analysis capabilities make it an ideal tool for monitoring network activities and responding to incidents promptly.

NEW QUESTION: 10

Clark, a professional hacker, exploited the web application of a target organization by tampering the form and parameter values. He successfully exploited the web application and gained access to the information assets of the organization. Identify the vulnerability in the web application exploited by the attacker.

- A. Broken access control
- B. Security misconfiguration
- C. SQL injection
- D. Sensitive data exposure

Answer: A ([LEAVE A REPLY](#))

The vulnerability exploited by Clark through tampering with form and parameter values to gain unauthorized access to information assets is indicative of Broken Access Control. Broken Access Control vulnerabilities occur when a web application does not properly enforce restrictions on what authenticated users are allowed to do. Attackers can exploit these vulnerabilities to access unauthorized functionality or data, such as accessing other users' accounts, viewing sensitive files, and modifying other users' data.

NEW QUESTION: 11

Sophia, a security analyst, notices that a sensitive folder on a file server was accessed during off- hours by an intern using authorized credentials. The access was not flagged

because the intern's permissions had not been reviewed in months, even after their project ended. What process should have been enforced to avoid this insider threat?

- A. Regular auditing of user access rights
- B. Surveillance camera monitoring
- C. Data classification and encryption
- D. Account lockout policies

Answer: A ([LEAVE A REPLY](#))

Regular access rights audits ensure permissions are reviewed and removed when users no longer need them. This would have identified the intern's outdated folder access after the project ended and reduced the risk of unauthorized insider activity.

NEW QUESTION: 12

Incident handlers at Delta Corp. were alerted about potential unauthorized access to a sensitive server room. Upon reaching the scene, what should be their immediate step to ensure the integrity of potential evidence?

- A. Engage external consultants to determine the extent of the breach.
- B. Turn off all machines to stop further unauthorized access.
- C. Start scanning the network for signs of exfiltration activities.
- D. Document the current state of the room, including positions of devices and opened files.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 13

During a web application security incident, the incident response team discovers that a database containing sensitive customer information has been compromised. What is the first step the incident response team should take during the containment phase?

- A. Schedule the meeting and accounts that were used to access the database
- B. Conduct a forensic investigation of the database server
- C. Shut down the database server to prevent further access
- D. Notify affected customers of the breach

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 14

While handling and responding to a potential web application security incident, you are required to conduct a vulnerability scan of your website. As an EC-Council Certified Incident Handler(ECIH), which of the following steps is NOT part of the process of performing web application vulnerability scanning using Acunetix Web Vulnerability Scanner(WVS)?

- A. Perform a full scan, select OWASP Top 10 2017 from the report, and schedule the scan instantly.
- B. After scanning, view vulnerabilities, analyze their details, and formulate a plan to fix them.

C. Install Acunetix WVS on a Windows 10 virtual machine and log in with the provided credentials.

D. Use the built-in HTTP Editor and HTTP Fuzzer of Acunetix WVS to manually test and validate potential vulnerabilities before scanning.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 15

Which of the following is a type of malicious code or software that appears legitimate but can take control of your computer?

A. Phishing attack

B. DDoS

C. Trojan attack

D. Password attack

Answer: ([SHOW ANSWER](#))

A Trojan attack involves a type of malicious code or software that appears legitimate but can take control of your computer. Trojans often disguise themselves as legitimate software or are hidden within legitimate software that has been tampered with. They differ from viruses and worms because they do not replicate. However, once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. This can include unauthorized actions such as deleting files, monitoring user activities, or installing additional malicious software.

NEW QUESTION: 16

Which of the following encoding techniques replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal?

A. URL encoding

B. Unicode encoding

C. Base64 encoding

D. HTML encoding

Answer: ([SHOW ANSWER](#))

URL encoding, also known as percent-encoding, is a mechanism for encoding information in a Uniform Resource Identifier (URI) under certain circumstances. This technique involves replacing unsafe ASCII characters with a "%" followed by two hexadecimal digits that represent the character's ASCII code. This is necessary for embedding characters that are not allowed in URLs directly, such as spaces and symbols, or characters that have special meanings within URLs, ensuring that the URL is correctly interpreted by web browsers and servers.

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam! Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:
https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 17

As an EC-Council Certified Incident Handler, you have set up a Suricata IDS system on your Ubuntu machine to monitor suspicious ICMP and HTTP traffic in your network. During the configuration process, you have to add a custom rule to the suricata.yaml file and enable the http- log section. After completing the setup, you switch to a Windows 10 machine and ping the Ubuntu machine while also performing some HTTP activity. You then return to the Ubuntu machine and stop the Suricata engine. In the logs, you notice the ICMP traffic, but the HTTP traffic is not captured. What could be the most plausible reason for this issue?

- A. You forgot to save the changes made in the suricata.yaml file after enabling the http-log section.
- B. The Suricata engine didn't start correctly.
- C. The custom rule you added to the suricata.yaml file was not correctly written.
- D. The Ubuntu machine didn't receive the ping from the Windows 10 machine.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 18

Following an internal audit at a mid-sized software development firm, it was discovered that several employees had been sharing system login credentials using personal messaging applications that were not approved by the organization. The audit further revealed that no structured guidance, awareness training, or acceptable usage policies had been provided regarding how and where confidential organizational information should be transmitted. Which of the following preparation steps would have most effectively prevented this situation?

- A. Provide awareness sessions on identifying unauthorized surveillance tools in secure areas.
- B. Schedule recurring data backups to secondary storage locations for disaster recovery.
- C. Establish defined protocols for appropriate digital channels when handling sensitive internal content.
- D. Deploy deception systems that simulate internal resources to lure potential insider threats.

Answer: ([SHOW ANSWER](#)**)**

This scenario represents a failure in the Preparation phase of the Incident Handling and Response (IH&R) lifecycle as defined by the EC-Council ECIH curriculum. Preparation focuses on establishing policies, procedures, standards, and awareness programs that define how systems and data must be used and protected. In this case, employees were sharing credentials via unauthorized channels because the organization failed to provide explicit rules governing acceptable communication practices.

Option C is correct because establishing defined protocols for approved digital channels directly addresses the root cause. ECIH emphasizes that organizations must define acceptable use policies, secure communication standards, and data handling procedures before incidents occur.

These controls reduce the likelihood of human error and insider misuse by setting clear expectations and enforceable boundaries.

Option A relates to physical surveillance risks, which are unrelated to credential sharing.

Option B is a recovery-focused control and does not prevent misuse. Option D is a detection mechanism that cannot compensate for missing governance controls.

By defining approved channels and educating users on their proper use, organizations significantly reduce the probability of credential leakage and insider-driven incidents, fulfilling a core ECIH preparation requirement.

NEW QUESTION: 19

A global bank's IH&R team is investigating an intricate cyber-espionage campaign.

Advanced persistent threat (APT) actors seemingly exfiltrated sensitive financial data over several months using multi-faceted attack vectors. A primary suspicion is that these vectors exploit both software vulnerabilities and human errors. In such a sophisticated scenario, what is the MOST appropriate immediate action for the IH&R team?

A. Conduct an organization-wide cybersecurity awareness training session to mitigate human errors.

B. Publicize the breach to notify potential victims and comply with Incident Handling Laws and Acts.

C. Focus solely on patching known software vulnerabilities in both Linux and Windows environments.

D. Leverage an Incident Response Automation and Orchestration (IRAO) tool to correlate disparate data sources and automate threat-hunting processes.

Answer: D (LEAVE A REPLY)

Advanced persistent threats require coordinated, intelligence-driven response. ECIH emphasizes that APT investigations generate massive volumes of telemetry across endpoints, networks, and cloud platforms.

Option D is correct because Incident Response Automation and Orchestration (IRAO) tools correlate disparate data sources, automate enrichment, and accelerate threat hunting. This enables responders to identify hidden persistence mechanisms and attacker TTPs efficiently.

Options A, B, and C are important but not immediate investigative actions.

ECIH explicitly recommends orchestration platforms for complex, multi-vector incidents such as APTs.

NEW QUESTION: 20

Which of the following information security personnel handles incidents from management and technical point of view?

- A.** Network administrators
- B.** Incident manager (IM)
- C.** Threat researchers
- D.** Forensic investigators

Answer: [\(SHOW ANSWER\)](#)

In the context of information security, the Incident Manager (IM) plays a crucial role in handling incidents from both a management and technical perspective. The Incident Manager is responsible for overseeing the entire incident response process, coordinating with relevant stakeholders, ensuring that incidents are analyzed, contained, and eradicated efficiently, and that recovery processes are initiated promptly. They are pivotal in ensuring communication flows smoothly between technical teams and upper management and that all actions taken are aligned with the organization's broader security policies and objectives. Unlike network administrators, threat researchers, or forensic investigators who may play more specialized roles within the incident response process, the Incident Manager has a broad oversight role that encompasses both technical and managerial aspects to ensure a comprehensive and coordinated response to security incidents.

NEW QUESTION: 21

A self-replicating virus does not alter files but resides in active memory and duplicates itself. It takes advantage of file or information transport features on the system to travel independently.

What is this type of object called?

- A.** Trojan
- B.** Worm
- C.** Spyware
- D.** Adware

Answer: **B** [\(LEAVE A REPLY\)](#)

NEW QUESTION: 22

A financial institution has recently suffered a major security incident. The incident was traced back to a malicious mobile application installed on the personal device of a senior executive, which was used for accessing corporate resources. As a certified incident handler, your immediate task is to mitigate such threats in the future. What step would you prioritize?

- A. Implement strict rules disallowing the use of personal devices to access corporate resources.
- B. Encourage all executives to only use corporate-owned devices for work purposes.
- C. Install an advanced mobile device management solution on all personal devices accessing corporate resources.
- D. Mandate the use of antivirus solutions on all personal devices accessing corporate resources.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 23

Which of the following is a technique used by attackers to make a message difficult to understand through the use of ambiguous language?

- A. Steganography
- B. Spoofing
- C. Encryption
- D. Obfuscation

Answer: D ([LEAVE A REPLY](#))

Obfuscation is a technique used to make data or code difficult to understand. It is often employed by attackers to conceal the true intent of their code or communications, making it harder for security professionals, automated tools, and others to analyze or detect malicious activity.

Obfuscation can involve the use of ambiguous or misleading language, as well as more technical methods such as encoding, encryption, or the use of nonsensical variable names in source code to hide its true functionality.

NEW QUESTION: 24

In which of the following types of fuzz testing strategies the new data will be generated from scratch and the amount of data to be generated are predefined based on the testing model?

- A. Log-based fuzz testing
- B. Generation-based fuzz testing
- C. Mutation-based fuzz testing
- D. Protocol-based fuzz testing

Answer: ([SHOW ANSWER](#))

Generation-based fuzz testing is a strategy where new test data is generated from scratch based on a predefined model that specifies the structure, type, and format of the input data. This approach is systematic and relies on a deep understanding of the format and protocol of the input data to create test cases that are both valid and potentially revealing of vulnerabilities. This contrasts with mutation-based fuzz testing, where existing data samples are modified (mutated) to produce new test cases, and log-based and protocol-

based fuzz testing, which use different approaches to test software robustness and security.

NEW QUESTION: 25

According to NITS, what are the 5 main actors in cloud computing?

- A.** Provider, carrier, auditor, broker, and seller
- B.** Consumer, provider, carrier, auditor, and broker
- C.** Buyer, consumer, carrier, auditor, and broker
- D.** None of these

Answer: B (LEAVE A REPLY)

According to the National Institute of Standards and Technology (NIST), which is a primary source for cloud computing standards and guidelines, the five main actors in cloud computing are Consumer, Provider, Carrier, Auditor, and Broker. These roles are defined as follows:

Consumer: The person or organization that uses cloud computing services.

Provider: The entity that provides the cloud services to consumers.

Carrier: The organization that offers connectivity and transport services to cloud providers and consumers.

Auditor: An independent party that assesses and verifies the cloud services, security controls, and operations.

Broker: An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between cloud providers and consumers.

These actors play critical roles in the ecosystem of cloud computing, ensuring the services are delivered and used securely, efficiently, and effectively.

NEW QUESTION: 26

Elena, a first responder at a multinational firm, receives multiple reports from employees claiming they were asked to update their payroll information through an email that appears to be from HR.

The email includes a URL directing users to a login page identical to the company's intranet but hosted on an unfamiliar domain. Elena immediately informs the IH&R team, preserves the email headers, captures screenshots of the spoofed page, and blocks the domain at the network level.

What type of email security incident is Elena handling?

- A.** DNS cache poisoning
- B.** Mail storm attack
- C.** Email spamming
- D.** Deceptive phishing attack

Answer: D (LEAVE A REPLY)

This scenario is a clear example of a deceptive phishing attack, which is extensively covered in the ECIH Email Security Incident module. Deceptive phishing involves

impersonating a trusted internal entity--such as HR--to trick recipients into disclosing sensitive information like credentials or personal data.

Option D is correct because the email impersonates HR, uses social engineering, and directs users to a visually identical but fraudulent login page hosted on an unfamiliar domain. These characteristics are classic indicators of deceptive phishing.

Option A refers to DNS manipulation and is not evidenced here. Option B involves overwhelming email volume rather than deception. Option C refers to unsolicited bulk email without impersonation.

Elena's actions align with ECIH best practices: preserving headers for forensic validation, capturing screenshots to document fraudulent infrastructure, and blocking malicious domains to prevent further exposure. Correctly categorizing the incident as deceptive phishing ensures appropriate eradication, awareness, and reporting measures.

NEW QUESTION: 27

Which of the following GPG18 and Forensic readiness planning (SPF) principles states that

"organizations should adopt a scenario based Forensic Readiness Planning approach that learns from experience gained within the business"?

- A. Principle 3
- B. Principle 2
- C. Principle 5
- D. Principle 7

Answer: [\(SHOW ANSWER\)](#)

The GPG18 and Forensic readiness planning (SPF) principles outline various guidelines to enhance an organization's readiness for forensic investigation and response. Principle 5, which suggests that organizations should adopt a scenario-based Forensic Readiness Planning approach that learns from experience gained within the business, emphasizes the importance of being prepared for a wide range of potential incidents by leveraging lessons learned from past experiences. This approach helps in continuously improving forensic readiness and response capabilities by adapting to the evolving threat landscape and organizational changes.

NEW QUESTION: 28

A user downloaded what appears to be genuine software. Unknown to her, when she installed the application, it executed code that provided an unauthorized remote attacker access to her computer. What type of malicious threat displays this characteristic?

- A. Backdoor
- B. Trojan
- C. Spyware
- D. Virus

Answer: B [\(LEAVE A REPLY\)](#)

The scenario described is characteristic of a Trojan. A Trojan is a type of malware that disguises itself as legitimate software but performs malicious actions once installed. Unlike viruses, which can replicate themselves, or worms, which can spread across networks on their own, Trojans rely on the guise of legitimacy to trick users into initiating their execution. In this case, the user believed they were downloading and installing genuine software, but the reality was that the application contained a Trojan. The malicious code executed upon installation provided unauthorized remote access to the user's computer, which could be used by an attacker to control the system, steal data, install additional malware, or carry out other malicious activities.

Trojans can come in many forms and can be used to achieve a wide range of malicious objectives, making them a versatile and dangerous type of cyber threat. The deceptive nature of Trojans, exploiting the trust users have in what appears to be legitimate software, is what makes them particularly effective and widespread.

NEW QUESTION: 29

An incident handling team has been alerted about a possible security breach on a Linux system.

As an EC-Council Certified Incident Handler, you decide to perform an incident triage using a tool named buck-security on Linux. After conducting the security check, buck-security returns a warning message indicating a potential issue with the firewall policies.

Considering the above scenario, what should be the immediate next step?

- A.** Analyze and address the vulnerabilities in the firewall policies.
- B.** Install and configure Splunk Universal Forwarder to capture remote system logs.
- C.** Run another security scan with buck-security to validate the issue.
- D.** Configure a Syslog server to review the network devices' logs.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 30

Sophia, a security analyst, notices that a sensitive folder on a file server was accessed during off- hours by an intern using authorized credentials. The access was not flagged because the intern's permissions had not been reviewed in months after their project ended. What process should have been enforced to avoid this insider threat?

- A.** Data classification and encryption
- B.** Account lockout policies
- C.** Regular auditing of user access rights
- D.** Surveillance camera monitoring

Answer: **C** ([LEAVE A REPLY](#))

The EC-Council Incident Handler (ECIH) curriculum stresses that periodic access reviews are essential for preventing insider threats. When user roles change or projects end, permissions must be reviewed and adjusted according to the Principle of Least Privilege (PoLP).

In this case, the intern retained access privileges beyond the project duration due to lack of periodic auditing. Regular auditing of user access rights ensures that permissions remain aligned with job responsibilities and reduces the risk of privilege misuse.

NEW QUESTION: 31

Oscar receives an email from an unknown source containing his domain name oscar.com. Upon checking the link, he found that it contains a malicious URL that redirects to the website evilsite.org.

What type of vulnerability is this?

- A. Malware
- B. Bolen
- C. Unvalidated redirects and forwards
- D. SQL injection

Answer: C (LEAVE A REPLY)

The scenario described, where Oscar receives an email with a link that contains a malicious URL redirecting to evilsite.org, exemplifies a vulnerability related to unvalidated redirects and forwards.

This type of vulnerability occurs when a web application accepts untrusted input that could cause the web application to redirect the request to a URL contained within untrusted input. Attackers can exploit this vulnerability by crafting a malicious URL that leads unsuspecting users to phishing sites or other malicious websites, under the guise of a legitimate domain. This is distinct from malware, which refers to malicious software; SQL injection, which involves inserting malicious SQL queries through input fields to manipulate or exploit databases; and is not a term related to cybersecurity vulnerabilities.

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam!

Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:

https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 32

BetaCorp, a multinational corporation, identified an employee selling company secrets to competitors. BetaCorp wants to prevent such incidents in the future. Which action will be most effective?

- A. Conduct surprise bag checks at office exits.
- B. Implement an Employee Monitoring Tool to track digital activities.
- C. Regularly change office locations of employees.

D. Introduce random polygraph tests for employees.

Answer: B ([LEAVE A REPLY](#))

ECIH identifies insider threats as best mitigated through continuous behavioral and activity monitoring, not physical or invasive measures.

Option B is correct because employee monitoring tools can analyze access patterns, file movements, abnormal data transfers, and deviations from normal behavior. These tools provide early warning of malicious insider activity while remaining compliant with legal and privacy frameworks when properly implemented.

Options A, C, and D are ineffective, intrusive, or legally problematic and are explicitly discouraged by ECIH.

Behavioral monitoring allows organizations to detect insider threats proactively rather than reactively, making Option B the most effective control.

NEW QUESTION: 33

Allan performed a reconnaissance attack on his corporate network as part of a red-team activity.

He scanned the IP range to find live host IP addresses. What type of technique did he use to exploit the network?

- A.** DNS foot printing
- B.** Social engineering
- C.** Port scanning
- D.** Ping sweeping

Answer: D ([LEAVE A REPLY](#))

Ping sweeping is a technique used in network reconnaissance to identify which IP addresses in a range are active or live. By sending ICMP echo requests ("ping") to multiple hosts and observing which ones respond, an attacker or, in this case, a red team member like Allan, can determine which systems are up and potentially vulnerable to further exploration or attack. This method is foundational for mapping the network before deploying more targeted exploits or scans.

NEW QUESTION: 34

Your company has faced a significant SQL injection attack on its web application. As an incident handler using the dotDefender tool, you notice that despite the SQL injection attack, the tool has not registered any events in its log viewer. Which of the following is the most plausible reason for this situation?

- A.** The dotDefender tool was not properly configured to detect SQL injection attacks.
- B.** The dotDefender tool does not register any attacks that are successfully mitigated.
- C.** The dotDefender tool does not have the ability to detect SQL injection attacks.
- D.** The attacker used a zero-day attack technique not recognized by the dotDefender tool.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

Ross is an incident manager (IM) at an organization, and his team provides support to all users in the organization who are affected by threats or attacks. David, who is the organization's internal auditor, is also part of Ross's incident response team. Which of the following is David's responsibility?

- A. Configure information security controls.
- B. Identify and report security loopholes to the management for necessary action.
- C. Coordinate incident containment activities with the information security officer (ISO).
- D. Perform the necessary action to block the network traffic from the suspected intruder.

Answer: B (LEAVE A REPLY)

In the context of an incident response team, the role of an internal auditor like David includes identifying, evaluating, and reporting on information security risks and vulnerabilities within the organization. His responsibility is to ensure that the organization's security controls are effective and to identify any security loopholes that could be exploited by attackers. Once identified, he reports these vulnerabilities to management so that they can take the necessary actions to mitigate the risks. This role is critical in maintaining the organization's overall security posture and ensuring compliance with relevant laws, regulations, and policies.

NEW QUESTION: 36

Rose is an incident-handling person and she is responsible for detecting and eliminating any kind of scanning attempts over the network by any malicious threat actors. Rose uses Wireshark tool to sniff the network and detect any malicious activities going on. Which of the following Wireshark filters can be used by her to detect TCP Xmas scan attempt by the attacker?

- A. `tcp.dstport==7`
- B. `tcp.flags==0X000`
- C. `tcp.flags.reset==1`
- D. `tcp.flags==0X029`

Answer: D (LEAVE A REPLY)

A TCP Xmas scan is a type of network scanning technique used by attackers to identify open ports on a target machine. The name "Xmas" comes from the set of flags that are turned on within the packet, making it 'lit up like a Christmas tree'. Specifically, the FIN, PSH, and URG flags are set, which corresponds to the hexadecimal value 0X029 in the TCP header's flags field.

Wireshark, a popular network protocol analyzer, allows users to create custom filters to detect specific types of network traffic, including malicious scanning attempts. By using the filter `tcp.flags==0X029`, Rose can detect packets that have these specific flags set, indicating a potential TCP Xmas scan attempt.

NEW QUESTION: 37

A company has migrated its infrastructure and services to the cloud to leverage its scalability and flexibility. However, they are facing challenges in effectively handling and responding to security incidents in the cloud environment. What is one of the key challenges in cloud incident handling and response?

- A. Difficulty in conducting forensic investigations in a shared cloud environment.
- B. Inadequate incident response team training and skills.
- C. Limited availability of cloud service provider's security tools and features.
- D. Lack of visibility and control over cloud infrastructure and data.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 38

Shally, an incident handler, is working for a company named Texas Pvt. Ltd. based in Florida.

She was asked to work on an incident response plan. As part of the plan, she decided to enhance and improve the security infrastructure of the enterprise. She has incorporated a security strategy that allows security professionals to use several protection layers throughout their information system. Due to multiple layer protection, this security strategy assists in preventing direct attacks against the organization's information system as a break in one layer only leads the attacker to the next layer.

Identify the security strategy Shally has incorporated in the incident response plan.

- A. Defense-in-depth
- B. Three-way handshake
- C. Covert channels
- D. Exponential backoff algorithm

Answer: ([SHOW ANSWER](#))

Shally has incorporated the Defense-in-depth strategy into the incident response plan for Texas Pvt. Ltd. Defense-in-depth is a layered security approach that involves implementing multiple security measures and controls throughout an information system. This strategy is designed to provide several defensive barriers to protect against threats and attacks, ensuring that if one layer is compromised, others still provide protection. The goal is to create a multi-faceted defense that addresses potential vulnerabilities in various areas, including physical security, network security, application security, and user education.

NEW QUESTION: 39

SafeGuard Inc., a cloud storage company, identified attackers exploiting a Server-Side Request Forgery (SSRF) vulnerability, leading to internal network reconnaissance. Which measure should SafeGuard Inc. prioritize to mitigate this vulnerability?

- A. Disable unused application features and services.
- B. Implement a Content Security Policy (CSP).
- C. Increase monitoring and logging of application activities.
- D. Restrict outbound traffic from the application server.

Answer: D (LEAVE A REPLY)

SSRF vulnerabilities allow attackers to coerce a server into making unauthorized internal or external requests. The ECIH Web Application Security module states that controlling outbound traffic is the most effective mitigation against SSRF.

Option D is correct because restricting outbound traffic ensures that even if an SSRF flaw exists, the server cannot access internal resources or attacker-controlled endpoints. ECIH emphasizes network-level egress filtering as a primary defensive control for SSRF.

Option A reduces attack surface but does not stop exploitation. Option B addresses client-side risks, not server-side requests. Option C improves detection but does not prevent exploitation.

Thus, outbound traffic restriction is the priority mitigation measure.

NEW QUESTION: 40

Aarav, an IT support specialist, identifies that multiple employees have engaged with an email promoting free shopping vouchers, which appears suspicious. To minimize the potential threat, he instructs staff to report the message, classify it as junk, and remove it from their inboxes. He further advises them not to interact with similar messages in the future, even if they seem to come from internal contacts. Which best practice is Aarav reinforcing?

- A. Sort emails by priority
- B. Digitally sign email attachments
- C. Disable preview pane in the inbox
- D. Avoid replying to or forwarding suspicious emails

Answer: D (LEAVE A REPLY)

This scenario focuses on user-driven mitigation of phishing threats, a key element of the ECIH Email Security Incident Handling module. Aarav's guidance directly reinforces one of the most important user best practices: never engage with suspicious emails.

Option D is correct because avoiding replies or forwarding suspicious emails prevents attackers from validating active accounts, spreading malware, or escalating social engineering attacks.

ECIH emphasizes that user interaction often determines the success of phishing campaigns, making awareness and behavior critical controls.

Option A is unrelated to security. Option B is a sender-side control, not a user response. Option C may reduce accidental clicks but does not address the broader behavioral risk. By instructing users to report, delete, and avoid engagement, Aarav strengthens the organization's human firewall, which ECIH recognizes as essential in reducing phishing impact.

NEW QUESTION: 41

John is a professional hacker who is performing an attack on the target organization where he tries to redirect the connection between the IP address and its target server such that

when the users type in the Internet address, it redirects them to a rogue website that resembles the original website. He tries this attack using cache poisoning technique. Identify the type of attack John is performing on the target organization.

- A. War driving
- B. Pharming
- C. Skimming
- D. Pretexting

Answer: B (LEAVE A REPLY)

Pharming is a cyber attack intended to redirect a website's traffic to another, bogus website. By poisoning a DNS server's cache, attackers can redirect users from the site they intended to visit to one that is malicious, without the user's knowledge or any action on their part, such as clicking a deceptive link. This technique is particularly insidious because it can affect well-intentioned users who type the correct URL into their browsers but are still redirected. War driving involves searching for wireless networks from a moving vehicle, skimming refers to stealing credit card information using a device placed on ATMs or point-of-sale terminals, and pretexting is a form of social engineering where the attacker lies to obtain privileged data.

NEW QUESTION: 42

EcoEarth Inc. detects abnormal archival data access from dormant employee profiles, modification of critical datasets, and suspicious encrypted packet transmissions. Given the risk, what is the first responder's primary action?

- A. Decrypt the suspicious packets to understand the breach.
- B. Notify global ecological partners to review shared data.
- C. Initiate a rollback to a previous safe state using real-time backups.
- D. Isolate and shut down sections of the server showing abnormal activity.

Answer: D (LEAVE A REPLY)

First responders prioritize containment and preservation: stop ongoing harm while protecting evidence. The scenario suggests active misuse (dormant accounts modifying data) and possible exfiltration (encrypted transmissions). The quickest way to prevent further manipulation/leakage is isolating affected services/segments--reducing attacker access paths and limiting spread. This also prevents additional data corruption while investigators capture logs, account activity, and network traces.

(A) decrypting traffic is not a first responder priority; it may be impossible (TLS/unknown keys) and consumes time while damage continues. (B) external notification can be necessary later, but premature partner notification can create panic and doesn't stop the incident. (C) rollback is a recovery step and can destroy forensic context or reintroduce compromised states if you haven't validated backup integrity; it also doesn't address how access happened or stop current attacker sessions unless paired with containment. Therefore, (D) best matches initial response doctrine: contain first, preserve evidence, then analyze and recover.

NEW QUESTION: 43

Sarah, an employee at a company, feels frustrated and resentful due to a hostile work environment and perceived unfair treatment. She decides to attack the organization's systems as a means of retaliation. What is the driving force behind Sarah's insider attack?

- A. Work-Related Grievance
- B. Challenge
- C. Corporate Espionage
- D. Hacktivism

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 44

What command does a Digital Forensic Examiner use to display the list of all open ports and the associated IP addresses on a victim computer to identify the established connections on it:

- A. "arp" command
- B. "dd" command
- C. "ifconfig" command
- D. "netstat -an" command

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 45

A computer forensic investigator must perform a proper investigation to protect digital evidence.

During the investigation, an investigator needs to process large amounts of data using a combination of automated and manual methods.

Identify the computer forensic process involved:

- A. Analysis
- B. Examination
- C. Collection
- D. Preparation

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 46

Which of the following email security tools can be used by an incident handler to prevent the organization against evolving email threats?

- A. Email Header Analyzer
- B. G Suite Toolbox
- C. MxToolbox
- D. Gpg4win

Answer: ([SHOW ANSWER](#))

MxToolbox is an online tool that provides various network diagnostics and email security checks, including looking up DNS and MX records, SPF records, and more. It can be used by incident handlers to prevent the organization against evolving email threats by analyzing domain health, checking blacklists, verifying email delivery issues, and more. While Email Header Analyzer is useful for analyzing specific emails for traces of phishing or spoofing, G Suite Toolbox might be specific to Google's services, and Gpg4win is more focused on email encryption. MxToolbox provides a broader set of functionalities for monitoring and troubleshooting email delivery issues and security threats, making it a versatile tool for incident handlers.

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam! Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:
https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 47

A multinational corporation with a diverse computing environment experiences a sophisticated malware attack targeting its endpoint devices. The malware is designed to evade traditional antivirus solutions and establish a persistent backdoor for data exfiltration. This incident underscores the complex landscape of endpoint security and the evolving threat vectors. In this context, what is the most critical reason for establishing a robust endpoint security incident handling and response capability?

- A. To facilitate real-time threat intelligence sharing across the industry.
- B. To ensure compliance with international data protection regulations.
- C. To mitigate financial losses associated with data breaches and system downtime.
- D. To enable rapid containment and eradication of threats to maintain business continuity.

Answer: D (LEAVE A REPLY)

The primary objective of endpoint incident handling, as outlined in the ECIH curriculum, is rapid containment and eradication of threats to preserve business operations. Advanced malware that bypasses traditional defenses requires coordinated response capabilities to prevent widespread compromise.

Option D is correct because endpoint IH&R enables organizations to quickly isolate infected systems, remove malicious components, and restore trusted states, thereby maintaining operational continuity. ECIH emphasizes speed and coordination as critical success factors in endpoint response.

Option A is secondary. Option B is a compliance outcome, not a response objective.

Option C is a consequence, not the primary driver.

Therefore, the most critical reason is to ensure rapid containment and eradication, making Option D correct.

NEW QUESTION: 48

A company's HR department receives a tip that an employee is planning to steal confidential information and sell it to a competitor. What is the best course of action for the company's incident response team to mitigate the risk of an insider threat in this scenario?

- A.** Select the employee's network threats and communications to detect any suspicious behavior
- B.** Conduct a thorough investigation of the employee and their potential motives
- C.** Immediately terminate the employee's employment to prevent any further risk
- D.** Restrict the employee's access to confidential information and systems

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 49

Which of the following is defined as the identification of the boundaries of an IT system along with the resources and information that constitute the system?

- A.** System characterization
- B.** Vulnerability identification
- C.** Threat identification
- D.** Control analysis

Answer: A ([LEAVE A REPLY](#))

System characterization is the process of defining the boundaries of an IT system, which includes identifying the resources, information, and functionality that constitute the system. This process is crucial for understanding the scope of the system, the data it processes, and the technology it employs. By characterizing a system, incident handlers can better understand the system's normal operations and behaviors, which is essential for identifying anomalies that may indicate a security incident. System characterization involves documenting the hardware, software, network configuration, data flows, and other critical elements of the IT environment. This foundational knowledge supports effective incident handling by providing a baseline against which suspicious activities can be compared.

NEW QUESTION: 50

During routine checks, EduSoft, an educational software provider, identified malware within their digital examination tools. This malware not only provided answers to students but mined personal data. With a digital forensic tool and an encryption protocol tool, what's the ideal primary action?

- A.** Disable the examination tool until further notice.
- B.** Alert educational institutions about the compromised software.
- C.** Use the forensic tool to ascertain the malware's source and method of operation.
- D.** Deploy the encryption tool to safeguard students' data.

Answer: C (LEAVE A REPLY)

Once malware is identified, ECIH guidance requires responders to analyze before eradication to understand scope, infection vectors, persistence mechanisms, and data impact. This ensures effective removal and prevents reinfection.

Option C is correct because forensic analysis allows investigators to determine how the malware entered the system, what data was accessed, and whether additional components are compromised. Without this understanding, containment and recovery efforts may be incomplete or ineffective.

Option A is a containment step but does not address root cause. Option B is a notification step that must be supported by verified facts. Option D protects future data but does not address the active malware.

Therefore, forensic analysis is the ideal primary action following detection, as emphasized in the ECIH malware handling process.

NEW QUESTION: 51

In a situation where an insider threat has been detected in your organization using the ActivTtak Employee Monitoring Solution, what would be the most appropriate step to handle this situation while ensuring minimal damage to the organizational resources?

- A.** Confront the suspicious employee directly and ask them about their unusual activities.
- B.** Immediately block all access to suspicious employees, including email, application accounts, physical access cards, and network credentials.
- C.** Inform all employees about the detected threat and ask them to be more cautious in the future.
- D.** Ignore the threat if it seems non-serious and continue monitoring employee activities.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 52

During a web application security incident, the incident response team discovers that the attacker has compromised a web server and is using it to launch further attacks against other systems on the network. What is the best course of action for the incident response team during the containment phase?

- A.** Allow the attacker to continue the attacks to gather more information about their methods
- B.** Isolate the compromised web server from the rest of the network to prevent further attacks
- C.** Install additional security measures on the compromised web server to prevent further attacks
- D.** Shut down the compromised web server to prevent further attacks

Answer: B (LEAVE A REPLY)

NEW QUESTION: 53

Which of the following tools helps incident handlers to view the file system, retrieve deleted data, perform timeline analysis, web artifacts, etc., during an incident response process?

- A. Autopsy
- B. netstat
- C. Process Explorer
- D. nbtstat

Answer: A ([LEAVE A REPLY](#))

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. Autopsy enables incident handlers to view the file system, retrieve deleted data, perform timeline analysis, and analyze web artifacts, among other functionalities. This tool is particularly useful during the incident response process for conducting in-depth investigations into the nature of a security incident, identifying the methods used by attackers, and recovering lost or compromised data.

NEW QUESTION: 54

Following a security alert, the incident response team at a legal consulting firm suspects that an employee used a USB storage device to exfiltrate confidential client data. The employee had physical access to critical systems during off-hours. To proceed with the investigation, the team needs to confirm which USB device was connected and gather related evidence such as timestamps and device identifiers. Which method is most effective for detecting and verifying the specific USB device used in this insider incident?

- A. Check Windows registry entries under Enum\USB to trace USB device history.
- B. Scan network logs to check for USB file upload patterns.
- C. Review recent entries in the Windows SetupAPI.dev.log file for USB installation events.
- D. Use WHOIS lookup to trace the origin of USB activity via external IPs.

Answer: ([SHOW ANSWER](#))

ECIH forensic readiness guidance identifies the Windows Registry as a primary source for USB device artifacts. The Enum\USB registry key stores vendor IDs, product IDs, serial numbers, and connection history.

Option A is correct because it provides direct evidence of which USB devices were connected, when they were installed, and on which system--critical for insider investigations.

Option B cannot reliably identify physical USB usage. Option C contains driver installation data but is less comprehensive. Option D is irrelevant.

Registry analysis is a foundational forensic technique in ECIH, making Option A correct.

NEW QUESTION: 55

ABC Corp., in the wake of frequent malware attacks, decided to conduct a forensic investigation on a suspected machine in their network. The incident response team used CurrPorts to monitor TCP/IP connections and identified a suspicious process. They also

leveraged Regshot for registry entry monitoring. While analyzing the registry changes before and after the execution of a suspicious process, they noticed some entries in the startup section of the registry. Given this scenario, which of the following is the most likely reason for malware creating entries in the startup section of the registry?

- A. To encrypt and hold data ransom for money.
- B. To log the keystrokes and send the user credentials over the network to the attacker.
- C. To ensure that the malicious process runs whenever the system boots.
- D. To propagate the malware across the connected devices in the network.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 56

John, a system administrator, has been with the company for several years and has access to sensitive company data. However, he has recently become disgruntled due to a denied promotion. He decides to seek revenge on the company by compromising its resources. Which type of insider threat does John represent?

- A. Accident-Prone Employee
- B. Privileged User
- C. Disgruntled Employee
- D. Terminated Employee

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 57

Finn is working in the eradication phase, wherein he is eliminating the root cause of an incident that occurred in the Windows operating system installed in a system. He ran a tool that can detect missing security patches and install the latest patches on the system and networks. Which of the following tools did he use to detect the missing security patches?

- A. Microsoft Cloud App Security
- B. Office360 Advanced Threat Protection
- C. Microsoft Advanced Threat Analytics
- D. Microsoft Baseline Security Analyzer

Answer: D ([LEAVE A REPLY](#))

The Microsoft Baseline Security Analyzer (MBSA) is a tool designed to assess a computer or network's security state by checking for missing security updates and common security misconfigurations. In the scenario with Finn, who is working in the eradication phase of an incident response process, the use of MBSA makes sense. The tool's ability to detect missing security patches and recommend the installation of the latest patches is crucial for eliminating vulnerabilities in the Windows operating system that could be the root cause of the incident.

MBSA scans the system for missing security updates, misconfigurations, and other vulnerabilities and provides detailed reports and recommendations for remediation. This step is vital in the eradication phase, where the goal is to remove the root causes of the

incident and secure the system against future attacks. By ensuring that all necessary patches are applied, Finn is addressing any security gaps that could be exploited by attackers.

NEW QUESTION: 58

After a series of email-based attacks, FinServCo, a financial services provider, wanted to establish robust defenses against potential email security incidents. While discussing preventive measures, which action emerged as a top priority to guard against email threats?

- A.** Prohibit employees from accessing personal emails on corporate devices.
- B.** Ensure that all email traffic is encrypted, both in transit and at rest.
- C.** Employ an email sandboxing solution to analyze email attachments in a secure environment.
- D.** Move all email services to a reputable cloud provider for better management.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 59

A global manufacturing company detected unauthorized privilege escalation on one of its OT workstations connected to critical production systems. The IH&R team must respond without alerting the attacker or risking deletion of forensic artifacts. The attacker's persistence mechanisms and data exfiltration activity are not yet fully identified. The CISO instructs the team to implement a strategy that limits the threat's lateral movement without tipping off the adversary.

Which of the following containment actions best aligns with this objective?

- A.** Disable select services and maintain a low profile using passive monitoring.
- B.** Initiate system-wide shutdown to prevent any further compromise.
- C.** Restore the system using the latest verified backup image.
- D.** Notify all employees immediately to change their credentials across the domain.

Answer: A ([LEAVE A REPLY](#))

This scenario requires stealthy containment, a technique emphasized in ECIH when dealing with advanced threats, particularly in OT environments.

Option A is correct because disabling selective services while maintaining passive monitoring restricts attacker movement without tipping them off. ECIH stresses that premature disruption can cause attackers to destroy evidence or accelerate damage. Options B, C, and D are noisy actions that alert the adversary and risk operational disruption.

ECIH recommends low-profile containment for advanced and persistent threats, especially in critical infrastructure, making Option A the correct response.

NEW QUESTION: 60

In the aftermath of a cybersecurity incident at TechGuard Ltd., the response team identified a USB drive suspected of containing malicious code. To preserve its integrity for forensic analysis, what should the team do?

- A. Connect it to a sandboxed environment to check its contents.
- B. Copy the contents to a secure server for backup.
- C. Format the USB drive to remove any malware.
- D. Store it in an anti-static bag, ensuring it's well-labeled and sealed.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 61

Which of the following risk management processes identifies the risks, estimates the impact, and determines sources to recommend proper mitigation measures?

- A. Risk assessment
- B. Risk assumption
- C. Risk mitigation
- D. Risk avoidance

Answer: A (LEAVE A REPLY)

Risk assessment is the risk management process that involves identifying risks, estimating their impact on the organization, and determining the sources of those risks to recommend appropriate mitigation measures. The goal of a risk assessment is to understand the nature of potential threats, vulnerabilities, and the consequences of those risks materializing, allowing an organization to make informed decisions about how to address them effectively. Risk assumption involves accepting the potential impact of a risk, risk mitigation focuses on reducing the likelihood or impact of risks, and risk avoidance involves taking actions to avoid the risk entirely.

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam! Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:

https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 62

You are talking to a colleague who is deciding what information they should include in their organization's logs to help with security auditing. Which of the following items should you tell them to NOT log?

- A. Timestamp
- B. Session ID

C. Source IP address

D. userid

Answer: D (LEAVE A REPLY)

Logging User IDs (D) can pose privacy concerns and may conflict with regulations such as the General Data Protection Regulation (GDPR), which emphasizes the protection of personal data and privacy. Therefore, while logging details such as Timestamps, Session IDs, and Source IP addresses are essential for security auditing to track when events occur, who is initiating sessions, and from where, care must be taken with User IDs. The handling of personally identifiable information (PII) must comply with privacy laws and organizational policies to safeguard individual privacy rights.

NEW QUESTION: 63

After a recent email attack, Harry is analyzing the incident to obtain important information related to the incident. While investigating the incident, he is trying to extract information such as sender identity, mail server, sender's IP address, location, and so on. Which of the following tools Harry must use to perform this task?

A. Clamwin

B. Loggly

C. Yesware

D. Sharp

Answer: C (LEAVE A REPLY)

Yesware is a tool primarily known for its email tracking capabilities, which can be useful for sales, marketing, and customer relationship management. However, in the context of investigating email attacks and analyzing incidents to extract details such as sender identity, mail server, sender's IP address, and location, a more appropriate tool would be one that specializes in analyzing and extracting detailed header information from emails, providing insights into the path an email took across the internet. While Yesware can provide data related to email interactions, it might not offer the depth of forensic analysis required for incident investigation. Tools like email header analyzers, which are designed specifically for dissecting and interpreting email headers, would be more fitting. In the absence of a direct match from the given options, the description might imply a broader interpretation of tools like Yesware in context but traditionally, tools specifically designed for email forensics would be sought after for this task.

NEW QUESTION: 64

A multinational firm recently encountered a severe cloud-based data breach where confidential data was accessed by unauthorized users. Keen to bolster its capacity to respond to such events in the future, the company must decide on the most suitable action to adopt. What should it do?

A. Set up a specialized cloud-focused incident response team and develop a corresponding plan.

- B.** Activate full-disk encryption on all cloud servers to safeguard data at rest.
- C.** Set up an IP-based access control list to limit access to cloud resources.
- D.** Transition to a private cloud model to maintain full control over data.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 65

Liam, a network engineer, configures firewalls to prevent outbound file transfers over unauthorized FTP and HTTP channels. Despite this, an insider used encrypted traffic via HTTPS to exfiltrate data. A review revealed that no deep packet inspection was in place. Which insider threat eradication control could have helped prevent this?

- A.** Mandatory biometric authentication
- B.** Implementing data loss prevention (DLP) tools
- C.** Enforcing secure coding practices
- D.** Using USB blocking software

Answer: B ([LEAVE A REPLY](#))

The EC-Council Incident Handler (ECIH) curriculum explains that insider data exfiltration frequently occurs through legitimate channels such as HTTPS to bypass traditional firewall rules.

When encrypted traffic is not inspected, sensitive data can be transmitted without detection.

Data Loss Prevention (DLP) tools monitor, detect, and block unauthorized transmission of sensitive information across endpoints, networks, and cloud services. DLP solutions can inspect encrypted traffic (when integrated with SSL/TLS inspection mechanisms) and enforce policies that prevent confidential data from leaving the organization.

The absence of deep packet inspection allowed encrypted HTTPS traffic to evade detection.

Implementing DLP would provide content-aware monitoring and policy-based enforcement, reducing insider exfiltration risk.

NEW QUESTION: 66

During the process of detecting and containing malicious emails, incident responders should examine the originating IP address of the emails. The steps to examine the originating IP address are as follow:

1. Search for the IP in the WHOIS database
2. Open the email to trace and find its header
3. Collect the IP address of the sender from the header of the received mail
4. Look for the geographic address of the sender in the WHOIS database

Identify the correct sequence of steps to be performed by the incident responders to examine originating IP address of the emails.

- A.** 4-->1-->2-->3
- B.** 2-->1-->4-->3

C. 1-->3-->2-->4

D. 2-->3-->1-->4

Answer: D ([LEAVE A REPLY](#))

The correct sequence to examine the originating IP address of emails involves first accessing the email's header to locate the IP address, then using external resources to investigate that address further. The steps are as follows:

Step 2: Open the email to trace and find its header. This is the initial step because the header contains valuable information about the email's journey across the internet, including the originating IP address.

Step 3: Collect the IP address of the sender from the header of the received mail. This detail is crucial for the next steps in the investigation.

Step 1: Search for the IP in the WHOIS database. This database can provide information about the owner of the IP address, including the ISP and sometimes the geographic location.

Step 4: Look for the geographic address of the sender in the WHOIS database. With the IP address information obtained from the WHOIS search, the geographic location or the originating country of the email can often be deduced, contributing to the analysis of the email's legitimacy.

NEW QUESTION: 67

After unearthing malware within their AI-based prediction systems, Future Tech Corp realized that their business projections were skewed. This malware was not just altering data but was equipped with machine learning capabilities, evolving its methods. With access to a dedicated AI security module and a database restoration tool, what's the primary step?

A. Restore the database to a point before malware infiltration.

B. Deploy the AI-security module to counteract and remove the evolved malware.

C. Disable the AI prediction system and rely on manual predictions temporarily.

D. Inform business partners about potentially skewed projections.

Answer: ([SHOW ANSWER](#))

This incident involves adaptive malware embedded within an AI system, actively evolving its behavior. The ECIH malware incident handling methodology prioritizes containment and eradication of the threat before recovery actions. Restoring data without removing the malware risks immediate reinfection and continued manipulation.

Option B is correct because deploying the AI-security module directly targets the malware's adaptive mechanisms, allowing responders to detect, contain, and eradicate the malicious logic within the AI environment. ECIH emphasizes using appropriate, context-aware security controls that match the technology stack involved in the incident. For AI-driven environments, specialized tools are necessary to counter threats that traditional controls may not detect.

Option A is premature and unsafe prior to eradication. Option C disrupts business operations without resolving the threat. Option D is a communication step that should follow containment and validation.

Therefore, neutralizing the evolved malware using the AI-security module is the correct primary step.

NEW QUESTION: 68

An organization named Sam Morison Inc. decided to use cloud-based services to reduce the cost of maintenance. The organization identified various risks and threats associated with cloud service adoption and migrating business-critical data to thirdparty systems. Hence, the organization decided to deploy cloud-based security tools to prevent upcoming threats.

Which of the following tools help the organization to secure the cloud resources and services?

- A. Nmap
- B. Burp Suite
- C. Wireshark
- D. Alert Logic

Answer: D (LEAVE A REPLY)

Alert Logic is a cloud-based security tool that provides Security-as-a-Service solutions including threat management, vulnerability assessment, and improved security outcomes. It is designed specifically to secure cloud resources and services, making it an ideal choice for organizations like Sam Morison Inc. that are moving their operations to the cloud and are concerned about the security of their data. Tools like Nmap, Burp Suite, and Wireshark, while valuable in certain contexts, do not offer the same cloud-focused security capabilities as Alert Logic.

NEW QUESTION: 69

During a routine investigation, Daniel, a threat analyst, notices repetitive failed login attempts in server logs with HTTP POST requests and status code 200 across several entries. At log entry

117, a 302 redirect status is recorded for the same user account. What type of attack is this indicative of?

- A. Dictionary attack
- B. Session hijacking
- C. SQL injection
- D. CSRF attack

Answer: A (LEAVE A REPLY)

The EC-Council Incident Handler (ECIH) curriculum explains that dictionary attacks are a form of brute-force authentication attack where an attacker systematically attempts multiple username- password combinations until valid credentials are found.

In web server logs, repeated HTTP POST requests targeting login endpoints with consistent status codes indicate automated credential attempts. The repeated failed attempts followed by a 302 redirect (commonly used after successful authentication to redirect users to a dashboard or landing page) strongly suggests that valid credentials were eventually discovered.

NEW QUESTION: 70

Johnson an incident handler is working on a recent web application attack faced by the organization. As part of this process, he performed data preprocessing in order to analyzing and detecting the watering hole attack. He preprocessed the outbound network traffic data collected from firewalls and proxy servers and started analyzing the user activities within a certain time period to create time-ordered domain sequences to perform further analysis on sequential patterns.

Identify the data-preprocessing step performed by Johnson.

- A. Filtering invalid host names
- B. Identifying unpopular domains
- C. Host name normalization
- D. User-specific sessionization

Answer: D (LEAVE A REPLY)

The data preprocessing step performed by Johnson, where he analyzes user activities within a certain time period to create time-ordered domain sequences for further analysis on sequential patterns, is known as user-specific sessionization. This process involves aggregating all user activities and requests into discrete sessions based on the individual user, allowing for a coherent analysis of user behavior over time. This is critical for identifying patterns that may indicate a watering hole attack, where attackers compromise a site frequently visited by the target group to distribute malware. User-specific sessionization helps in isolating and examining sequences of actions taken by users, making it easier to detect anomalies or patterns indicative of such an attack.

NEW QUESTION: 71

Which of the following is considered a best practice during the containment phase of incident handling?

- A. Shutting down the affected system immediately to stop the attack
- B. Notifying law enforcement before conducting internal analysis
- C. Isolating compromised systems from the network to prevent spread
- D. Publicly disclosing the breach before any investigation is completed

Answer: C (LEAVE A REPLY)

The containment phase of the incident handling process is all about limiting the scope and impact of a confirmed security incident. Once an incident is verified in the identification

phase, it is crucial to act swiftly and carefully to prevent it from spreading to other systems, damaging more data, or affecting critical operations.

NEW QUESTION: 72

James is a professional hacker and is employed by an organization to exploit their cloud services.

In order to achieve this, James created anonymous access to the cloud services to carry out various attacks such as password and key cracking, hosting malicious data, and DDoS attacks.

Which of the following threats is he posing to the cloud platform?

- A.** Insecure interface and APIs
- B.** Data breach/loss
- C.** Insufficient duo diligence
- D.** Abuse end nefarious use of cloud services

Answer: D (LEAVE A REPLY)

James's activities, including creating anonymous access to cloud services to carry out attacks such as password and key cracking, hosting malicious data, and conducting DDoS attacks, exemplify the abuse and nefarious use of cloud services. This threat involves exploiting cloud computing resources to conduct malicious activities, which can impact the cloud service provider as well as other users of the cloud services. This abuse ranges from using the cloud platform's resources for computationally intensive tasks like cracking passwords or encryption keys to conducting DDoS attacks that can disrupt services for legitimate users.

NEW QUESTION: 73

An international insurance provider observed a sharp rise in endpoint infections across geographically dispersed offices. The IR team correlated the infections with recent access to a series of trusted informational websites visited during routine research activities. After cross-referencing network telemetry and endpoint logs, analysts uncovered that these sites had been covertly altered by threat actors to include obfuscated scripts that launched on page render. Upon visiting the tampered content, a series of exploit chains were executed, targeting unpatched vulnerabilities in rendering engines of commonly used client applications. The malicious code was injected directly into volatile memory, allowing the payload to operate stealthily without initiating file creation events or prompting user interaction. Security tools failed to detect the compromise in real time due to the absence of conventional indicators such as user-triggered executions or external file transfers. Which web-based malware delivery technique is MOST consistent with the described attack?

- A.** Spam email propagation using malicious file attachments disguised as legitimate documents
- B.** Search engine poisoning using black hat search engine optimization

C. Drive-by download attacks that exploit vulnerabilities

D. Malvertising via poisoned ad banners embedded in third-party ad-serving platforms

Answer: C (LEAVE A REPLY)

The EC-Council Incident Handler (ECIH) curriculum defines drive-by download attacks as web-based attacks where malicious code is automatically executed when a user visits a compromised website. These attacks often exploit browser or rendering engine vulnerabilities without requiring user interaction or explicit file downloads.

In this scenario, trusted informational websites were covertly modified to include obfuscated scripts that executed upon page rendering. The exploit chains targeted unpatched vulnerabilities and injected payloads directly into memory, avoiding file creation and traditional detection mechanisms. This behavior is characteristic of drive-by download attacks leveraging exploit kits.

NEW QUESTION: 74

EduTech University noticed unauthorized access to student records, including academic and financial details. As the semester's examinations approached, there were concerns about potential leaks or manipulations of question papers. In this complex digital scenario, what is the optimal step for the first responder?

A. Capture logs from the academic servers, focusing on recent access and modifications.

B. Collaborate with faculty to develop alternative exam papers as a backup.

C. Isolate the academic systems, ensuring the integrity of upcoming examinations.

D. Notify students and staff, urging them to change their university portal passwords.

Answer: C (LEAVE A REPLY)

The ECIH Incident Handling lifecycle prioritizes containment during first response when active compromise threatens data integrity and operational continuity. In this scenario, the risk extends beyond data theft to potential manipulation of examination materials.

Option C is correct because isolating the affected academic systems immediately prevents further unauthorized access and preserves the integrity of examination content.

Containment ensures that attackers cannot alter or leak sensitive academic materials while investigations proceed.

Option A supports investigation but does not stop ongoing risk. Option B is a contingency plan, not a response action. Option D is premature and does not address system compromise.

According to ECIH, first responders must act decisively to prevent further damage before moving into analysis and recovery, making Option C correct.

NEW QUESTION: 75

Jason, a cybersecurity analyst in the incident response team, begins investigating several complaints from employees who received emails urgently requesting wire transfers to an overseas account. The emails appeared to come from the company's CEO, using a tone of authority and pressure to bypass standard procedures. Upon closer inspection, Jason

identifies that the sender's email address includes a minor alteration in the domain name--a form of domain spoofing. He examines the email headers, confirms the falsified sender identity, and cross-checks with the actual CEO's activity logs to ensure there was no internal compromise. Immediately, Jason blocks the sender's IP address at the firewall level, alerts the finance department to prevent any unauthorized transactions, and issues a company-wide advisory about the impersonation attempt. What type of phishing is Jason handling?

- A. Whaling
- B. Mail bombing
- C. Credential stuffing
- D. Spimming

Answer: A (LEAVE A REPLY)

This incident is a textbook example of whaling, a specialized form of phishing that targets senior executives or impersonates them to exploit authority and trust. According to the ECIH Email Security module, whaling attacks often focus on financial fraud, such as wire transfer requests or invoice manipulation, and are designed to bypass normal controls through urgency and executive impersonation.

Option A is correct because the attacker impersonated the CEO and targeted employees responsible for financial actions. The minor domain alteration and authoritative language are classic whaling indicators.

Option B refers to overwhelming inboxes with large volumes of mail. Option C involves automated credential testing. Option D targets mobile messaging platforms.

Jason's response--header analysis, identity verification, firewall blocking, financial alerting, and organization-wide notification--aligns with ECIH best practices for handling executive impersonation attacks. Recognizing the attack type correctly is critical for appropriate escalation and mitigation, making Option A the correct answer.

NEW QUESTION: 76

A company's mobile device management (MDM) solution alerts the incident response team to a malware infection on an employee's smartphone. What is the best course of action for the incident response team in this scenario?

- A. Collect and analyze logs from the MDM solution to identify the source of the infection
- B. Notify the affected employee and ask them to uninstall the malware
- C. Conduct a full system scan on the infected smartphone to identify the extent of the infection
- D. Block access to the company network and quarantine the infected smartphone

Answer: D (LEAVE A REPLY)

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam! Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:
https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 77

Which of the following is not a best practice to eliminate the possibility of insider attacks?

- A.** Disable the users from installing unauthorized software or accessing malicious websites using the corporate network
- B.** Monitor employee behaviors and the computer systems used by employees
- C.** Implement secure backup and disaster recovery processes for business continuity
- D.** Always leave business details over voicemail or email broadcast message

Answer: D (LEAVE A REPLY)

Leaving sensitive business details over voicemail or sending them out through email broadcast messages is not a best practice for security. This approach significantly increases the risk of information leakage and unauthorized access to critical business information. Such practices can be exploited by insiders to conduct malicious activities, including data theft, fraud, or sabotage.

The best practices for mitigating insider threats involve implementing strict access controls, monitoring and auditing employee actions, securing communications, and ensuring that sensitive information is only shared through secure and authorized channels. Encouraging or allowing the practice of leaving sensitive business details in such insecure manners contradicts the principles of information security and increases the vulnerability to insider attacks.

NEW QUESTION: 78

Clark is investigating a cybercrime at TechSoft Solutions. While investigating the case, he needs to collect volatile information such as running services, their process IDs, startmode, state, and status.

Which of the following commands will help Clark to collect such information from running services?

- A.** Openfiles
- B.** netstat -ab
- C.** wmic
- D.** net file

Answer: C (LEAVE A REPLY)

WMIC (Windows Management Instrumentation Command-line) is a command-line tool that provides a unified interface for Windows management tasks, including the collection of

system information. It allows administrators and forensic investigators to query the live system for information about running services, their process IDs, start modes, states, and statuses, among other data. The use of WMIC is particularly valuable in incident response scenarios for gathering volatile information from a system without having to install additional software, which might alter the state of the system being investigated. By executing specific WMIC commands, Clark can extract detailed information about the services running on a system at the time of the investigation, making it an essential tool for collecting volatile data in a forensically sound manner.

NEW QUESTION: 79

James is working as an incident responder at CyberSol Inc. The management instructed James to investigate a cybersecurity incident that recently happened in the company. As a part of the investigation process, James started collecting volatile information from a system running on Windows operating system. Which of the following commands helps James in determining all the executable files for running processes?

- A. date /t & time /t
- B. netstat -ab
- C. top
- D. doskey/history

Answer: B (LEAVE A REPLY)

The netstat -ab command is useful in Windows operating systems for displaying all connections and listening ports, along with the executable involved in creating each connection or listening port. This can be particularly valuable for an incident responder like James when attempting to determine which processes are running on a system and how they are communicating over the network. This information can help identify malicious processes, unauthorized connections, or other signs of compromise on the system. While netstat -ab does not exclusively list executable files for running processes, it ties processes to network activity, which is a critical part of collecting volatile information during a cybersecurity incident investigation.

NEW QUESTION: 80

NanoCorp, a nano-technology firm, experienced a ransomware attack originating from a malicious email link. Post-containment, the IT team debated the best eradication strategy. Which action ensures the thorough removal of any remnants of the ransomware?

- A. Restore affected systems from a known good backup.
- B. Conduct a company-wide password reset and two-factor authentication setup.
- C. Increase email scanning frequency and tighten security policies.
- D. Apply patches and updates to all company software and systems.

Answer: (SHOW ANSWER)

NEW QUESTION: 81

Which of the following is a common tool used to help detect malicious internal or compromised actors?

- A. User behavior analytics
- B. SOC2 compliance report
- C. Log forwarding
- D. Syslog configuration

Answer: A (LEAVE A REPLY)

User Behavior Analytics (UBA) is a cybersecurity process or tool that utilizes machine learning, algorithms, and statistical analyses to detect potentially harmful activities within an organization's network by comparing them against established patterns of users' behavior. It is particularly effective in identifying malicious internal actors or compromised users who may be conducting activities that deviate from their normal behavior patterns, such as accessing unauthorized data or systems, excessive file downloads, or unusual login times. UBA tools can flag these activities for further investigation, often before traditional security tools detect a breach. In contrast, SOC2 compliance reports, log forwarding, and syslog configuration are important for maintaining and auditing security standards and for infrastructure monitoring, but they are not primarily focused on detecting malicious behavior based on deviations from established user behavior patterns.

NEW QUESTION: 82

An attacker traced out and found the kind of websites a target company/individual is frequently surfing and tested those particular websites to identify any possible vulnerabilities. When the attacker detected vulnerabilities in the website, the attacker started injecting malicious script/code into the web application that can redirect the webpage and download the malware onto the victim's machine. After infecting the vulnerable web application, the attacker waited for the victim to access the infected web application.

Identify the type of attack performed by the attacker.

- A. Watering hole
- B. Obfuscation application
- C. Directory traversal
- D. Cookie/Session poisoning

Answer: A (LEAVE A REPLY)

The described attack is a "Watering hole" attack. This type of attack targets specific groups of users by infecting websites they are known to frequently visit. The attacker first identifies websites that are popular with the target group, then finds vulnerabilities in those websites to inject malicious code. When the victims visit the compromised site, the code redirects them to other sites or automatically downloads malware onto their machines. This attack leverages the trust users have in regularly visited sites to distribute malware. Unlike obfuscation application, directory traversal, or cookie/session poisoning attacks, watering

hole attacks specifically aim to compromise a commonly used and trusted website to target its users.

NEW QUESTION: 83

Following a spear-phishing campaign targeting executive-level employees, a mid-sized financial firm experienced unauthorized access to internal systems, leading to widespread disruption of customer-facing applications. Although the technical issues were resolved within days, the breach triggered legal scrutiny and negative press coverage. Several major customers expressed concern about the firm's risk posture and began transitioning to competitors. Investor confidence was impacted as the stock value dipped, and senior leadership initiated a damage control campaign. Which of the following best categorizes the broader consequences experienced by the organization?

- A. Tangible operational costs including the deployment of response infrastructure.
- B. Recovery complications caused by delayed asset inventory synchronization.
- C. Intangible business effects involving stakeholder defection and public image decline.
- D. Measurable loss from hardware failure and direct asset compromise.

Answer: (SHOW ANSWER)

The scenario describes consequences extending beyond technical remediation into reputational, financial, and stakeholder trust impacts. According to ECIH risk assessment and post-incident analysis guidance, these outcomes are classified as intangible business effects.

Option C is correct because customer loss, investor confidence decline, and reputational damage cannot be easily quantified yet often exceed direct incident response costs. ECIH emphasizes that post-incident reviews must consider both tangible and intangible impacts to accurately assess business risk.

Options A, B, and D describe operational or technical impacts, which were resolved quickly in this scenario. The lasting damage occurred at the business and market perception level. Understanding intangible impacts is critical for executive reporting, risk management, and long-term resilience planning, making Option C correct.

NEW QUESTION: 84

AlphaTech, a technology firm, recently discovered signs of an advanced persistent threat (APT) in its infrastructure. The incident response team is trying to gather more information about the threat to form a comprehensive response strategy. While leveraging threat intelligence platforms, which of the following approaches would be most effective in gathering detailed and actionable insights about the APT to improve the firm's defense against such threats?

- A. Searching for IOCs (Indicators of Compromise) related to known APT campaigns and comparing them with the observed patterns.
- B. Collaborating with industry peers to understand similar threats they have faced and the tactics, techniques, and procedures (TTPs) observed.

C. Obtaining historical data on common cyber threats and using it to predict future APT movements.

D. Gathering information about APTs from open-source forums and integrating this with their internal threat database.

Answer: B (LEAVE A REPLY)

ECIH emphasizes that advanced persistent threats require intelligence beyond static indicators.

While IOCs are useful, they often change quickly and provide limited context.

Option B is correct because collaboration with industry peers enables sharing of tactics, techniques, and procedures (TTPs), which are more stable and actionable than IOCs.

ECIH strongly promotes information sharing communities, ISACs, and trusted peer collaboration to improve situational awareness against APTs.

Options A, C, and D provide partial or outdated insights and lack operational depth.

Therefore, peer collaboration focused on attacker behavior is the most effective approach.

NEW QUESTION: 85

A cloud service provider detected anomalous activities pointing to a potential compromise of their infrastructure. The IH&R team is confronted with vast amounts of data from various cloud-native logging mechanisms. To ensure swift and effective incident triage, what should be their primary course of action?

A. Exclusively focus on cloud-native logging mechanisms, ignoring any third-party logging tools that might be integrated.

B. Send a notification to all clients, advising them to back up their data and prepare for potential service disruptions.

C. Implement an Incident Response Automation and Orchestration (IRAO) tool specifically designed for cloud environments to correlate logs and prioritize alerts.

D. Immediately isolate all affected cloud instances, regardless of the impact on customer operations.

Answer: C (LEAVE A REPLY)

With large volumes of cloud-native logs, automation and orchestration tools are essential to correlate events, prioritize alerts, and accelerate triage, enabling efficient identification of true incidents and faster response.

NEW QUESTION: 86

An organization named Sam Morison Inc. decided to use cloud-based services to reduce the cost of their maintenance. They first identified various risks and threats associated with cloud ..

adoption and migrating critical business data to third-party systems. Hence, the organization decided to deploy cloud-based security tools to prevent upcoming threats.

Which of the following tools would help the organization to secure cloud resources and services?

- A. Burp Suite
- B. Alert Logic
- C. Wireshark
- D. Nmap

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 87

WebDynamics experienced altered webpage content due to stored Cross-Site Scripting (XSS) attacks caused by lack of output encoding. What should be the main focus to prevent this?

- A. Implement proper output encoding for displayed content.
- B. Establish a Web Application Firewall (WAF).
- C. Regularly update the CMS and plugins.
- D. Introduce mandatory two-factor authentication.

Answer: ([SHOW ANSWER](#))

Stored XSS vulnerabilities arise when untrusted input is rendered without proper output encoding.

The ECIH Web Application module clearly states that output encoding is the primary defense against XSS.

Option A is correct because encoding ensures that user-supplied input is treated as data rather than executable script. This directly prevents malicious script execution in users' browsers.

Options B and C provide additional protection but do not fix the root cause. Option D is unrelated to XSS prevention.

ECIH emphasizes fixing vulnerabilities at the application logic level, making output encoding the correct focus.

NEW QUESTION: 88

During a web application security incident, the incident response team discovers that a hacker has gained access to a server hosting a critical web application. The hacker has also installed malware that has enabled them to steal sensitive data from the server. What is the best course of action for the incident response team during the containment phase?

- A. Leave the server connected to the network to gather more information about the attack
- B. Back up the compromised server to preserve evidence
- C. Disconnect the server from the network to prevent further access
- D. Notify the affected customers of the breach

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 89

Alexis works as an incident responder at XYZ organization. She was asked to identify and attribute the actors behind an attack that occurred recently. For this purpose, she is

performing a type of threat attribution that deals with the identification of a specific person, society, or country sponsoring a well-planned and executed intrusion or attack on its target. Which of the following types of threat attributions is Alexis performing?

- A. Campaign attribution
- B. True attribution
- C. Nation-state attribution
- D. Intrusion set attribution

Answer: C (LEAVE A REPLY)

Nation-state attribution involves identifying a specific country or government as the sponsor behind a cyber-attack or intrusion. This type of threat attribution is focused on determining the involvement of state actors in cyber operations against specific targets, which often involves sophisticated, well-planned, and executed cyber campaigns. Alexis's efforts to identify and attribute the actors behind the attack to a specific nation-state fall under this category, as she seeks to uncover the geopolitical motives and the extent of state sponsorship behind the incident.

Nation-state attribution requires analyzing a variety of indicators, including technical evidence, tactics, techniques, and procedures (TTPs), and contextual intelligence. This is distinct from campaign attribution, which focuses on linking attacks to a specific campaign or operation, true attribution, which aims at identifying the actual individuals behind an attack, and intrusion set attribution, which involves attributing a set of malicious activities to a particular threat actor or group.

NEW QUESTION: 90

Your company sells SaaS, and your company itself is hosted in the cloud (using it as a PaaS). In case of a malware incident in your customer's database, who is responsible for eradicating the malicious software?

- A. Your company
- B. Building management
- C. The PaaS provider
- D. The customer

Answer: A (LEAVE A REPLY)

In the scenario where your company sells Software as a Service (SaaS) and is hosted on the cloud using it as a Platform as a Service (PaaS), your company is responsible for eradicating malware in your customer's database. This is because, as the SaaS provider, your company manages the software and is responsible for its security and maintenance, including the databases that store customer data. While the PaaS provider is responsible for the underlying infrastructure, platform, and possibly some middleware security aspects, the application layer security, including data and application management, falls to the SaaS provider. Building management would not be involved in digital security matters, and while customers are responsible for their data, the actual software maintenance and security in a SaaS model are the provider's responsibility.

NEW QUESTION: 91

Jake, a senior incident responder in a financial institution's SOC, receives a high-severity alert from the intrusion detection system (IDS). The alert indicates a flood of SYN packets targeting the internal web server, which has now become sluggish and unresponsive to legitimate client requests. The sudden surge in half-open connections is causing resource exhaustion on the server. Suspecting a SYN flood attack--a type of denial-of-service (DoS) attack--Jake needs to verify the source and nature of the traffic to determine the appropriate containment and mitigation strategy while preserving system integrity and uptime. What step should Jake take first in response to this suspected DoS incident?

- A. Notify HR to instruct employees on mandatory password resets
- B. Disconnect all users from the network to isolate the server
- C. Inspect network traffic to confirm the attack pattern and verify source behavior
- D. Reboot the affected server to restore availability

Answer: C (LEAVE A REPLY)

The EC-Council Incident Handler (ECIH) curriculum states that during the detection and analysis phase, responders must validate the incident before taking disruptive containment actions. In suspected DoS attacks, traffic analysis is critical to confirm attack patterns such as SYN floods characterized by numerous half-open TCP connections.

Inspecting network traffic using packet captures, firewall logs, and IDS telemetry allows responders to confirm the nature of the attack, identify source IP behavior, and determine whether IP spoofing or distributed sources are involved. This ensures appropriate mitigation such as SYN cookies, rate limiting, or upstream filtering.

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam!

Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:

https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 92

Rinni is an incident handler and she is performing memory dump analysis. Which of following tools she can use in order to perform memory dump analysis?

- A. OllyDbg and IDA Pro
- B. Scylla and OllyDumpEx
- C. Procmon and ProcessExplorer
- D. iNetSim

Answer: B (LEAVE A REPLY)

For memory dump analysis, tools like Scylla and OllyDumpEx are more suited. These tools are designed to analyze and extract information from memory dumps, which can be crucial for understanding the state of a system at the time of an incident. Scylla is used for reconstructing imports in dumped binaries, while OllyDumpEx is an OllyDbg plugin used for dumping process memory. Both tools are valuable for incident handlers like Rinni who are performing memory dump analysis to uncover evidence or understand the behavior of malicious software.

NEW QUESTION: 93

You are an EC-Council Certified Incident Handler for a financial institution. A sudden network spike has been detected in one of your data centers late at night. The company might be dealing with a distributed denial of service attack. As the one on the front line, what is the top priority action you'd need to jump on right away?

- A. Switch off the servers to stop further data transmission.
- B. Initiate a complete system backup to preserve current data.
- C. Isolate affected systems to prevent the spread of the attack.
- D. Notify all customers about the potential breach.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 94

The following steps describe the key activities in forensic readiness planning:

1. Train the staff to handle the incident and preserve the evidence
2. Create a special process for documenting the procedure
3. Identify the potential evidence required for an incident
4. Determine the source of the evidence
5. Establish a legal advisory board to guide the investigation process
6. Identify if the incident requires full or formal investigation
7. Establish a policy for securely handling and storing the collected evidence
8. Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption

Identify the correct sequence of steps involved in forensic readiness planning.

- A. 2-->3-->1-->4-->6-->5-->7-->8
- B. 3-->4-->8-->7-->6-->1-->2-->5
- C. 3-->1-->4-->5-->8-->2-->6-->7
- D. 1-->2-->3-->4-->5-->6-->7-->8

Answer: ([SHOW ANSWER](#))

The correct sequence of steps involved in forensic readiness planning, based on the activities described, is as follows:

Identify the potential evidence required for an incident.

Determine the source of the evidence.

Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption.

Establish a policy for securely handling and storing the collected evidence.

Identify if the incident requires full or formal investigation.

Train the staff to handle the incident and preserve the evidence.

Create a special process for documenting the procedure.

Establish a legal advisory board to guide the investigation process.

This sequence ensures that an organization is prepared to handle incidents efficiently, with a focus on identifying relevant evidence and the legal context of its collection, followed by staff training and the establishment of guiding policies and advisory boards.

NEW QUESTION: 95

As the new CISO for a mid-sized healthcare organization, you've been tasked with fortifying the company's cyber defenses. Your predecessor mainly focused on network security, but you believe that endpoint security incident handling and response are equally vital. What is the most compelling reason to justify the additional investment to the board of directors?

- A.** Endpoint security is a current trend in the cybersecurity industry.
- B.** The company's competitors have invested heavily in endpoint security.
- C.** Regulatory bodies demand a greater focus on endpoint security.
- D.** Increasing the number of remote workers makes the network perimeter less defined.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 96

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?

- A.** Installing anti-DDoS tools
- B.** Sharing threat details with security forums
- C.** Issuing server restart commands
- D.** Deleting user accounts

Answer: ([SHOW ANSWER](#))

In the ECIRH 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.

NEW QUESTION: 97

Maria, a network security analyst working in a multinational corporation, is monitoring real-time logs from the organization's firewall and intrusion detection system (IDS). During her routine analysis, she observes a sharp increase in failed login attempts on the internal web server, all coming from various IP addresses within a short time frame. Moments later, the outbound traffic from that same server spikes unusually, transmitting large volumes of data to an unfamiliar external IP address. Based on this behavior, Maria suspects a successful brute-force attack on a weak administrator password, followed by data exfiltration by the attacker. She acts quickly by isolating the compromised server from the network, preserving the logs, and alerting the incident handling and response (IH&R) team for further investigation and containment. What type of network security incident is this?

- A. Wireless network incident
- B. Unauthorized access incident
- C. Inappropriate usage incident
- D. Denial-of-service incident

Answer: B (LEAVE A REPLY)

According to the EC-Council Incident Handler (ECIH) curriculum, an unauthorized access incident occurs when an attacker gains access to a system without proper authorization, often through credential compromise, brute-force attacks, or exploitation of weak authentication controls.

The scenario describes repeated failed login attempts followed by successful access and subsequent data exfiltration. This sequence--brute-force attempts leading to compromise and data transmission--clearly indicates unauthorized system access. The large outbound traffic spike to an unfamiliar IP further confirms potential data exfiltration following successful authentication bypass.

NEW QUESTION: 98

Sam, an employee of a multinational company, sends emails to third-party organizations with a spoofed email address of his organization. How can you categorize this type of incident?

- A. Network intrusion incident
- B. Inappropriate usage incident
- C. Unauthorized access incident.
- D. Denial-of-service incident

Answer: B (LEAVE A REPLY)

An inappropriate usage incident involves misuse of the organization's resources or violations of its acceptable use policies. Sam's actions, where he sends emails to third-party organizations with a spoofed email address of his employer, constitute misuse of the organization's email system and misrepresentation of the organization. This behavior can

harm the organization's reputation, violate policy, and potentially lead to legal consequences. Inappropriate usage incidents can range from unauthorized use of systems for personal gain to the dissemination of unapproved content.

NEW QUESTION: 99

You are the cloud security incident response manager for a large organization. Your team has identified a potential security incident in the cloud environment. Upon investigation, you find that an unauthorized individual gained access to a critical database containing sensitive customer information. What is the MOST appropriate immediate action to take?

- A.** Collect evidence and preserve logs for forensic analysis.
- B.** Shut down the compromised database server to prevent further unauthorized access.
- C.** Notify affected customers and guide them on protecting their personal information.
- D.** Engage the organization's legal team to assess potential liability and regulatory obligations.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 100

Lina, a threat responder, uses the Nuix Adaptive Security tool to analyze alerts of suspicious file uploads. She identifies that an insider used Outlook to send attachments to unknown email addresses during off-hours. The tool captures screenshots, file metadata, and keystroke logs.

What type of evidence is Lina primarily relying on?

- A.** User behavior analytics and endpoint monitoring
- B.** SIEM event correlation
- C.** Network forensics logs
- D.** Host-based intrusion prevention logs

Answer: A ([LEAVE A REPLY](#))

The EC-Council Incident Handler (ECIH) curriculum explains that insider threat investigations frequently depend on endpoint monitoring and user behavior analytics (UBA/UEBA). In this case, the Nuix Adaptive Security tool captured screenshots, file metadata, and keystroke logs--forms of host-level monitoring that directly observe user activity on the endpoint.

User behavior analytics focuses on detecting deviations from normal patterns, such as sending attachments to unknown external addresses during non-business hours. ECIH identifies this as anomalous insider behavior indicative of potential data exfiltration.

Endpoint monitoring tools provide detailed artifacts including screen captures, application usage logs, keystroke records, and file transfer metadata, which are critical for forensic analysis and evidence preservation.

NEW QUESTION: 101

Lara, a SOC analyst, investigates multiple alerts generated by an IDS showing repeated login failures from a specific workstation to an internal application. When reviewing Windows Event Viewer logs, she discovers a user repeatedly attempting logins outside of working hours. Further checks reveal the user had installed an unauthorized remote desktop tool. Which of the following best describes this situation?

- A. Policy-enforced remote work attempt
- B. Unauthorized access incident from a third party
- C. Inappropriate usage due to policy violation and software installation
- D. DoS attack against an internal application

Answer: C (LEAVE A REPLY)

The EC-Council Incident Handler (ECIH) curriculum categorizes incidents such as unauthorized software installation and policy violations under inappropriate usage incidents. In this scenario, the activity originated from a legitimate internal workstation and user account, not an external third party.

The repeated login failures outside business hours combined with installation of an unauthorized remote desktop tool indicate a breach of acceptable use policy and potentially malicious intent.

However, the key factor is that the actions were performed by an internal user using valid access credentials, making this an insider-related policy violation rather than an external unauthorized access attack.

NEW QUESTION: 102

Eric works as a system administrator at ABC organization and previously granted several users with access privileges to the organizations systems with unlimited permissions. These privileged users could prospectively misuse their rights unintentionally, maliciously, or could be deceived by attackers that could trick them to perform malicious activities. Which of the following guidelines would help incident handlers eradicate insider attacks by privileged users?

- A. Do not allow administrators to use unique accounts during the installation process
- B. Do not enable default administrative accounts to ensure accountability
- C. Do not control the access to administrator and privileged users
- D. Do not use encryption methods to prevent, administrators and privileged users from accessing backup tapes and sensitive information

Answer: B (LEAVE A REPLY)

Not enabling default administrative accounts is crucial to ensuring accountability and minimizing the risk of insider attacks by privileged users. By disabling or renaming default accounts, organizations can better track the actions performed by individual administrators, reducing the risk of unauthorized or malicious activities going unnoticed. This practice is part of a broader approach to privilege management that includes limiting permissions to the minimum necessary and monitoring the use of administrative privileges.

NEW QUESTION: 103

What is the primary goal of the identification phase in the incident handling process?

- A. Eliminating the threat actor's access to the network
- B. Restoring affected systems to normal operation
- C. Determining whether an event qualifies as a security incident
- D. Deploying security patches to vulnerable systems

Answer: C ([LEAVE A REPLY](#))

In the identification phase of the incident handling lifecycle, the primary objective is to determine whether an observed anomaly qualifies as a security incident. This is a critical first step in incident response because not every unusual activity signifies a true threat. Some anomalies may be harmless system errors, false positives, or performance-related issues rather than attacks.

The process typically begins when security monitoring tools, such as intrusion detection systems (IDS), security information and event management (SIEM) systems, or antivirus software, generate alerts. Security teams then investigate these alerts to assess the scope, impact, and authenticity of the event.

NEW QUESTION: 104

A ransomware attack recently disrupted operations at a manufacturing facility, specifically targeting its IoT-integrated conveyor system. While attempting to recover from the incident, the incident response team discovered that the available backups were incomplete--several critical sensor logs and control commands were missing, which caused delays in restoring device functions and syncing with other systems. The team concludes that relying on traditional backup routines alone is insufficient for restoring full IoT functionality after an attack. Which strategy would best prevent such issues in future recovery efforts?

- A. Use long-term tape archival for all IoT firmware images.
- B. Store historical sensor logs in compressed ZIP archives on shared drives.
- C. Schedule periodic external hard drive backups for operator terminals.
- D. Maintain synchronized cloud replicas of critical IoT resources.

Answer: (SHOW ANSWER)

This scenario highlights recovery challenges specific to IoT environments, which are addressed in the ECIH Endpoint and IoT Incident Handling modules. IoT systems generate continuous streams of operational data, configuration states, and control commands that are essential for accurate recovery after disruption.

Option D is correct because maintaining synchronized cloud replicas of critical IoT resources ensures near-real-time availability of sensor data, device configurations, and control logic. ECIH emphasizes that traditional periodic backups are often insufficient for IoT and OT systems due to their dynamic and state-dependent nature. Cloud replication supports faster, more complete restoration and reduces data gaps.

Options A, B, and C rely on static or delayed backup mechanisms that cannot capture the operational state required to restore IoT systems accurately. Tape archives and external drives introduce latency and risk data loss, while ZIP archives lack synchronization. ECIH recovery guidance stresses resilience and continuity, particularly for operational technology. Continuous replication is therefore the most effective strategy.

NEW QUESTION: 105

Posta debilitating malware attack on RetailHub, a chain of e-commerce platforms, the top brass decided to bolster their defenses. They acknowledged human error as a significant vulnerability.

As part of their renewed strategy, which preventive guideline would be most impactful against malware introduction?

- A.** Outsourcing their IT infrastructure to a third-party vendor for better management.
- B.** Mandating biannual security audits.
- C.** Conducting regular employee training on phishing and social engineering threats.
- D.** Restricting administrative privileges to a select few.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 106

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?

- 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.

Answer: B ([LEAVE A REPLY](#))

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.

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam! Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:
https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 107

Which of the following is not the responsibility of first responders?

- A. Protecting the crime scene
- B. Identifying the crime scene
- C. Packaging and transporting the electronic evidence
- D. Preserving temporary and fragile evidence and then shut down or reboot the victim's computer

Answer: D (LEAVE A REPLY)

The responsibility of first responders does not include shutting down or rebooting the victim's computer as a measure to preserve temporary and fragile evidence. In fact, such actions can potentially alter or destroy volatile data that could be crucial for the investigation. The primary responsibilities of first responders include protecting and identifying the crime scene, and ensuring the preservation of evidence in its original state as much as possible, which may involve isolating affected systems from the network but not necessarily shutting them down or rebooting them without proper forensic readiness and consideration.

NEW QUESTION: 108

Michael is a part of the computer incident response team of a company. One of his responsibilities is to handle email incidents. The company receives an email from an unknown source, and one of the steps that he needs to take is to check the validity of the email. Which of the following tools should he use?

- A. Zendio
- B. Email Dossier
- C. Yesware
- D. G Suite Toolbox

Answer: B (LEAVE A REPLY)

Email Dossier is a tool designed to assist in the investigation of email incidents by analyzing and validating email headers and providing detailed information about the origin, routing, and authenticity of an email. When Michael is tasked with handling an email incident and needs to check the validity of an email received from an unknown source, Email Dossier can be utilized to trace the email's path, assess its credibility, and identify potential red flags associated with phishing or other malicious email-based attacks.

NEW QUESTION: 109

Alex is an incident handler in QWERTY Company. He identified that an attacker created a backdoor inside the company's network by installing a fake AP inside a firewall. Which of the following attack types did the attacker use?

- A. AP misconfiguration
- B. Wardriving
- C. Rogue access point
- D. Ad hoc associations

Answer: C (LEAVE A REPLY)

When an attacker installs a fake AP (Access Point) within a company's network, especially behind a firewall, this constitutes the deployment of a Rogue Access Point. Rogue APs are unauthorized wireless access points installed within a network without the network administrator's knowledge or consent. They pose a significant security risk because they can be used to intercept sensitive information, bypass network security configurations, and provide a gateway for attackers to enter the network undetected. This type of attack circumvents the security measures put in place by a company, including firewalls, by creating an illicit entry point into the network that is under the control of the attacker.

NEW QUESTION: 110

ZYX company experienced a DoS/DDoS attack on their network. Upon investigating the incident, they concluded that the attack is an application-layer attack. Which of the following attacks did the attacker use?

- A. Slowloris attack
- B. UDP flood attack
- C. SYN flood attack
- D. Ping of death

Answer: A (LEAVE A REPLY)

The Slowloris attack is a type of application-layer attack that targets the web server by establishing and maintaining many simultaneous HTTP connections to the target server. Unlike traditional network-layer DoS/DDoS attacks such as UDP flood or SYN flood, Slowloris is designed to hold as many connections to the target web server open for as long as possible. It does so by sending partial requests, which are never completed, and periodically sending subsequent HTTP headers to keep the connections open. This consumes the server's resources, leading to denial of service as legitimate users cannot

establish connections. The Slowloris attack is effective even against servers with a high bandwidth because it targets the server's connection pool, not its network bandwidth.

NEW QUESTION: 111

Rachel, a digital forensics investigator, arrives at the scene of a suspected data breach. She photographs all electronic devices, labels and packages each item in static-resistant bags, and ensures each item is documented with time, location, and device details. What activity best describes Rachel's task?

- A.** Packaging and transporting electronic evidence
- B.** Reviewing the organization's access policies
- C.** Analyzing system logs to find vulnerabilities
- D.** Collecting testimonial evidence from witnesses

Answer: (SHOW ANSWER)

According to the EC-Council Incident Handler (ECIH) curriculum, proper handling of digital evidence is a critical responsibility of first responders. This includes photographing the scene, labeling devices, packaging them in anti-static or static-resistant bags, and documenting detailed information such as time, location, and device identifiers.

These steps are part of evidence preservation and packaging procedures designed to prevent contamination, electrostatic damage, or loss of evidentiary integrity. ECIH emphasizes maintaining a clear chain of custody and ensuring that all digital evidence is properly documented before transportation to a forensic laboratory.

NEW QUESTION: 112

David, an incident responder, investigates an email-based breach where the CFO's email account was compromised and used to send invoice modification requests to vendors. Logs reveal the attacker accessed the account using valid credentials after the CFO clicked on a fake Microsoft 365 login prompt sent via email. Which technique did the attacker most likely use?

- A.** Mail bombing
- B.** Pharming
- C.** Spimming
- D.** Spear phishing

Answer: (SHOW ANSWER)

This incident is a classic spear phishing attack, where a targeted individual is deceived into entering credentials on a fraudulent login page. The ECIH Email Security module describes spear phishing as highly targeted and often tailored to specific roles, such as executives.

Option D is correct because the CFO was targeted with a convincing fake Microsoft 365 login prompt, leading to credential theft. The use of valid credentials afterward confirms successful social engineering rather than technical exploitation.

Option A involves email flooding. Option B redirects traffic via DNS manipulation. Option C targets mobile messaging platforms.

Recognizing spear phishing is critical because it informs remediation steps such as credential resets, MFA enforcement, and executive awareness training, all emphasized in ECIH guidance.

NEW QUESTION: 113

During a routine security assessment at SoftTech, a major software development company, a series of suspicious email transmissions were flagged from a senior executive's account to an external domain. Preliminary investigations suggest that the emails contained critical IP details.

To identify the cause and extent of this compromise, what should be the primary action?

- A.** Enforce immediate password resets for all senior executive accounts.
- B.** Conduct a forensic examination of the affected email account's recent activities.
- C.** Coordinate with the external domain to retrieve the sent emails.
- D.** Send an alert to all staff members about potential phishing threats.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 114

ThetaTec, a global fintech giant, identified that an employee was siphoning off funds using a sophisticated method undetectable by traditional monitoring tools. The firm decided to employ advanced techniques to detect such hidden insider threats. What should be its primary focus?

- A.** Install hidden microphones in the office to capture conversations.
- B.** Use behavioral analytics to identify potential risks based on employee actions and patterns.
- C.** Mandate all employees to provide access to their personal bank statements.
- D.** Conduct polygraph tests on all employees quarterly.

Answer: ([SHOW ANSWER](#))

Insider threats are among the most difficult risks to detect because insiders often operate within legitimate access boundaries. The ECIH Insider Threat module emphasizes that behavioral analytics is the most effective approach for identifying sophisticated, low-and-slow insider activity.

Option B is correct because behavioral analytics correlates user actions over time to detect anomalies such as unusual transaction patterns, abnormal access times, or deviations from job role norms. This allows detection of malicious behavior that traditional rule-based monitoring may miss.

Options A, C, and D are invasive, unethical, and often illegal, and they contradict ECIH guidance on lawful, proportional monitoring.

ECIH stresses that insider threat programs must balance security, privacy, and legality while providing meaningful detection. Behavioral analytics meets these requirements and provides actionable insights, making Option B the correct answer.

NEW QUESTION: 115

EnviroTech, a global environmental research institute, faced anomalies in six months of satellite weather data. Unauthorized data modification entries were found in logs, occurring in microbursts with minimal traces. While the intent was unclear, the implications were significant. What's the optimal response?

- A.** Immediately release a public statement highlighting discrepancies, urging other institutions to cross-check their data.
- B.** Approach international cybersecurity agencies, speculating a nation-state actor attempting to manipulate climate data.
- C.** Isolate the affected systems, initiate a thorough forensic examination, and revert to the most recent unaltered backup.
- D.** Collaborate with other global institutes, sharing data to identify the point of discrepancy without revealing the potential breach.

Answer: (SHOW ANSWER)

This scenario requires decisive action across containment, analysis, and recovery, as defined in the ECIH incident handling lifecycle.

Option C is correct because isolating affected systems prevents further manipulation, forensic examination identifies scope and method, and restoring from a verified clean backup ensures data integrity. ECIH emphasizes verified restoration only after investigation begins.

Options A, B, and D are premature or speculative and risk misinformation.

NEW QUESTION: 116

Otis is an incident handler working in an organization called Delmont. Recently, the organization faced several setbacks in business, whereby its revenues are decreasing. Otis was asked to take charge and look into the matter. While auditing the enterprise security, he found traces of an attack through which proprietary information was stolen from the enterprise network and passed onto their competitors. Which of the following information security incidents did Delmont face?

- A.** Network and resource abuses
- B.** Espionage
- C.** Email-based abuse
- D.** Unauthorized access

Answer: (SHOW ANSWER)

Espionage, in the context of information security incidents, refers to the unauthorized access and theft of proprietary information for competitive advantage. In the scenario described, where proprietary information was stolen from Delmont's enterprise network

and passed onto their competitors, this directly aligns with the definition of espionage. The incident involves deliberate targeting and extraction of sensitive business information, which is then used by competitors to gain a market advantage. Such actions not only compromise the confidentiality of business-critical information but can also significantly impact the financial stability and competitive positioning of the victim organization.

NEW QUESTION: 117

For analyzing the system, the browser data can be used to access various credentials. Which of the following tools is used to analyze the history data files in Microsoft Edge browser?

- A.** ChromeHistoryView
- B.** BrowsingHistoryView
- C.** MZCacheView
- D.** MZHistoryView

Answer: B (LEAVE A REPLY)

BrowsingHistoryView is a tool designed to collect and analyze history data from various web browsers, including Microsoft Edge. It allows users to view the browsing history stored by their browsers in one unified interface. This includes URLs visited, page titles, visit times, and the number of visits to each page. While ChromeHistoryView is specific to Google Chrome, BrowsingHistoryView supports multiple browsers, making it versatile for analyzing history data across different platforms. MZCacheView and MZHistoryView do not exist as tools recognized for this purpose in the context of Microsoft Edge or other browser history analysis.

NEW QUESTION: 118

In which of the following types of insider threats an insider who is uneducated on potential security threats or simply bypasses general security procedures to meet workplace efficiency?

- A.** Compromised insider
- B.** Negligent insider
- C.** Professional insider
- D.** Malicious insider

Answer: B (LEAVE A REPLY)

A negligent insider is an individual within an organization who, due to a lack of knowledge on security threats or in an attempt to increase workplace efficiency, inadvertently bypasses security procedures or makes errors that compromise security. This type of insider threat is not malicious in intent; rather, it stems from carelessness, oversight, or a lack of proper security training. Such insiders might click on phishing links, mishandle sensitive information, or use unsecured networks for work-related tasks, thereby exposing the organization to potential security breaches. This contrasts with compromised insiders

(who are manipulated by external parties), professional insiders (who misuse their access for personal gain), and malicious insiders (who intentionally aim to harm the organization).

NEW QUESTION: 119

During the eradication phase of a web application security incident, the incident response team discovers that the web application was compromised due to a known vulnerability that had not been patched. What is the best course of action for the incident response team?

- A.** Monitor the web application for any further signs of compromise
- B.** Conduct a penetration test to identify any other vulnerabilities
- C.** Conduct a root cause analysis to identify why the vulnerability was not patched
- D.** Patch the vulnerability and restore the web application to its previous state

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 120

Elizabeth, who works for OBC organization as an incident responder, is assessing the risks to the organizational security. As part of the assessment process, she is calculating the probability of a threat source exploiting an existing system vulnerability. Which of the following risk assessment steps is Elizabeth currently in?

- A.** Vulnerability identification
- B.** Impact analysis
- C.** Likelihood analysis
- D.** System characterization

Answer: **C** ([LEAVE A REPLY](#))

In the risk assessment process, calculating the probability that a threat source will exploit an existing system vulnerability is known as likelihood analysis. This step involves evaluating how probable it is that the organization's vulnerabilities can be exploited by potential threats, considering various factors such as the nature of the vulnerability, the presence and capability of threat actors, and the effectiveness of current controls.

Elizabeth's task of assessing the probability of exploitation is crucial for understanding the risk level associated with different vulnerabilities and for prioritizing risk mitigation efforts based on the likelihood of occurrence.

NEW QUESTION: 121

A network administrator reviews firewall and IDS/IPS configurations to ensure logging is properly set, updates logging to centralize alerts from all network devices, and confirms that all response team members know their responsibilities. Which preparatory activity is he performing?

- A.** Hardening backup systems.
- B.** Coordinating external law enforcement.
- C.** Conducting vulnerability scanning.

D. Ensuring network monitoring readiness.

Answer: (SHOW ANSWER)

This is classic preparation work aimed at improving detection and response speed. Valid incident handling begins before incidents occur: ensuring telemetry exists, logs are collected centrally, alerts are actionable, and roles are defined so handoffs and escalation happen quickly.

Reviewing firewall and IDS/IPS logging, centralizing alerts, and aligning the response team on responsibilities directly supports monitoring readiness and operational coordination.

(A) backup hardening is about recovery resilience and integrity of backups; nothing in the scenario references backup configurations or restore testing. (B) law enforcement coordination is a procedural/legal readiness task, not what is described. (C) vulnerability scanning is proactive identification of weaknesses; again, the actions here are about log visibility and alerting, not scanning.

Network monitoring readiness (D) best fits because it includes: ensuring the right data sources are logging, time synchronization, centralized collection (SIEM/log platform), and defined responsibilities for triage and escalation. This aligns with playbook-style preparation models that emphasize roles and monitoring visibility before incidents occur .

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam! Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:

https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 122

Identify the network security incident where intended or authorized users are prevented from using system, network, or applications by flooding the network with a high volume of traffic that consumes all existing network resources.

- A. XSS attack
- B. Denial-of-service
- C. URL manipulation
- D. SQL injection

Answer: B (LEAVE A REPLY)

A Denial-of-Service (DoS) attack is characterized by flooding the network with a high volume of traffic to consume all available network resources, preventing intended or authorized users from accessing system, network, or applications. This type of attack aims to overwhelm the target's capacity to handle incoming requests, causing a denial of access to legitimate users. Unlike XSS (Cross-Site Scripting) attacks, URL manipulation, or SQL

injection, which exploit vulnerabilities in web applications for unauthorized data access or manipulation, a DoS attack specifically targets the availability of services.

NEW QUESTION: 123

Chandler is a professional hacker who is targeting Technote organization. He wants to obtain important organizational information that is being transmitted between different hierarchies. In the process, he is sniffing the data packets transmitted through the network and then analyzing them to gather packet details such as network, ports, protocols, devices, issues in network transmission, and other network specifications. Which of the following tools Chandler must employ to perform packet analysis?

- A.** shARP
- B.** IDAPro
- C.** Omnippeek
- D.** BeEf

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 124

Which of the following best describes an email issued as an attack medium, in which several messages are sent to a mailbox to cause overflow?

- A.** Email-bombing
- B.** Masquerading
- C.** Spoofing
- D.** Smurf attack

Answer: A ([LEAVE A REPLY](#))

Email-bombing refers to the attack where the attacker sends a massive volume of emails to a specific email address or mail server in order to overflow the mailbox or overwhelm the server, potentially causing it to fail or deny service to legitimate users. This attack can disrupt communications and, in some cases, lead to the targeted email account being disabled.

Masquerading involves pretending to be another legitimate user, spoofing is the creation of emails (or other communications) with a forged sender address, and a smurf attack is a specific type of Distributed Denial of Service (DDoS) attack that exploits Internet Protocol (IP) and Internet Control Message Protocol (ICMP) to flood a target with traffic. Email-bombing specifically targets email services with the goal of causing disruption by overflowing inboxes.

NEW QUESTION: 125

Following a ransomware attack, CyberTech Inc. initiated a full-scale risk assessment. They found multiple potential vulnerabilities and realized the need to prioritize them for remediation. Which criteria should CyberTech primarily use to prioritize these vulnerabilities?

- A. Popularity of the vulnerability in the hacker community.
- B. The potential business impact of a successful exploitation of the vulnerability.
- C. Time since the vulnerability was discovered.
- D. The cost associated with the mitigation of each vulnerability.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 126

Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system.

EVIDENCE PROTECTION is also required to meet legal compliance issues.

Which of the following documents helps in protecting evidence from physical or logical damage?

- A. Chain-of-Custody
- B. Chain-of-Precedence
- C. Network and host log records
- D. Forensic analysis report

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 127

The EC-Council Certified Incident Handler (ECIH) at an organization suspects an employee to be an insider threat due to unusual network activities. The handler is currently using the ActivTrak Employee Monitoring Solution for insider threat detection. Which of the following actions is the most appropriate first step for the incident handler to perform in this scenario?

- A. Immediately report the suspicious activity to senior management to seek further advice.
- B. Analyzing the screenshots captured by ActivTrak and the resources involved in the suspected activities.
- C. Contact law enforcement agencies and legal authorities for a thorough investigation.
- D. Blocking all access for the suspected employee, including email, application accounts, physical access cards, and network credentials.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 128

Your manager hands you several items of digital evidence and asks you to investigate them in the order of volatility. Which of the following is the MOST volatile?

- A. Cache
- B. Disk
- C. Emails
- D. Temp files

Answer: A ([LEAVE A REPLY](#))

In the context of digital evidence investigation, volatility refers to how quickly data can change or be lost when power is removed or systems are altered. Among the options provided, cache is the most volatile because it is temporary storage that is designed to speed up access to data and is frequently overwritten. Cache data resides in RAM and includes things like memory buffers, system and network information, and process execution data, which are lost upon reboot or power loss. This contrasts with disks, emails, and temp files, which are considered less volatile because they are stored on permanent or semi-permanent media and are less likely to be immediately lost or overwritten.

NEW QUESTION: 129

During the eradication phase of a web application security incident at a major online retail platform, the incident response team discovers that the application was compromised through a previously unknown zero-day vulnerability. This vulnerability allowed the attacker to access user credit card information. The incident has severe financial and reputational implications. In this highly sensitive scenario, what is the best course of action for the incident response team?

- A.** Conceal the incident to protect the company's reputation
- B.** Immediately go public with the details of the zero-day vulnerability
- C.** Focus solely on tracking the attacker without addressing the vulnerability
- D.** Patch the vulnerability, remove all traces of the attacker, inform affected users, and coordinate with relevant authorities

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 130

Patrick is doing a cyber forensic investigation. He is in the process of collecting physical evidence at the crime scene.

Which of the following elements he must consider while collecting physical evidence?

- A.** Open ports, services, and operating system (OS) vulnerabilities
- B.** DNS information including domain and subdomains
- C.** Published name servers and web application source code
- D.** Removable media, cable, and publications

Answer: ([SHOW ANSWER](#))

In the context of collecting physical evidence during a cyber forensic investigation, Patrick must consider items like removable media, cables, and publications. These items can contain crucial information related to the crime, such as data storage devices (USB drives, external hard drives), cables connected to potentially relevant devices, and any printed materials that might have information or clues about the incident. Open ports, services, and OS vulnerabilities, DNS information, and published name servers and web application source code, while important in digital forensics, do not constitute physical evidence in the traditional sense.

NEW QUESTION: 131

If the browser does not expire the session when the user fails to logout properly, which of the following OWASP Top 10 web vulnerabilities is caused?

- A. A7: Cross-site scripting
- B. A3: Sensitive- data exposure
- C. A2: Broken authentication
- D. A5: Broken access control

Answer: C (LEAVE A REPLY)

When a browser does not expire a session after the user fails to logout properly, it is indicative of a vulnerability related to broken authentication. Broken authentication is a security issue where attackers can exploit flaws in the authentication mechanism to impersonate other users or take over their sessions. Failure to properly manage session lifetimes, such as not expiring sessions on logout, can allow an attacker to reuse old sessions or session IDs, potentially gaining unauthorized access to user accounts. This vulnerability is classified under A2: Broken Authentication in the OWASP Top 10, which lists the most critical web application security risks.

The OWASP Top 10 serves as a guideline for developers and web application providers to understand and mitigate common security risks.

NEW QUESTION: 132

Sofia, an incident handler, notices unusual requests in the web server logs, such as GET /documents/../../wp-config.php. She confirms that the attacker tried to access configuration files by bypassing the web root restrictions using encoded strings like %2e%2e%2f. What type of attack has occurred here?

- A. XSS attack
- B. LFI attack
- C. Directory traversal
- D. SQL injection

Answer: C (LEAVE A REPLY)

The request uses path traversal sequences to move outside the intended web directory and access restricted configuration files. Encoded traversal strings are commonly used to bypass filtering and web root restrictions.

NEW QUESTION: 133

An incident handler is analyzing email headers to find out suspicious emails. Which of the following tools he/she must use in order to accomplish the task?

- A. Barracuda Email Security Gateway
- B. Gophish
- C. SPAMfighter

Answer: A (LEAVE A REPLY)

The Barracuda Email Security Gateway is designed to manage and filter inbound and outbound email traffic to protect organizations from email-borne threats and data leaks. As an incident handler analyzing email headers to find out suspicious emails, using a tool like the Barracuda Email Security Gateway would be appropriate. This tool can help identify and block spam, phishing, malware, and other malicious email threats, making it easier to focus on analyzing potentially harmful emails more closely.

NEW QUESTION: 134

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

- A. Clickjacking
- B. Impersonation
- C. Registry key manipulation
- D. Macro abuse

Answer: D (LEAVE A REPLY)

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.

NEW QUESTION: 135

Which of the following plans is an essential component of a comprehensive business continuity strategy that ensures recovery after a major disruption?

- A. Forensic Investigation Plan
- B. Business Recovery Plan
- C. Marketing Strategy Plan
- D. New Product Development Plan

Answer: B (LEAVE A REPLY)

A Business Continuity Plan (BCP) is a strategic framework organizations use to ensure that essential functions can continue during and after a significant disruption such as a natural disaster, cyberattack, or system failure. One of the foundational elements of a BCP

is the Business Recovery Plan, which focuses on restoring critical operations and services in a structured and timely manner.

The Business Recovery Plan outlines detailed procedures for resuming business activities after a crisis. This includes recovering IT systems, restoring data from backups, and re-establishing communication lines. Its purpose is to minimize downtime, reduce revenue loss, and ensure a smooth transition back to normal operations. By prioritizing business-critical services, the recovery plan enables the organization to maintain operational resilience in challenging situations.

NEW QUESTION: 136

The security team at a multinational company has noticed a few unusual activities on their web applications and suspects potential SQL injection and XSS attacks. The incident handler is tasked with identifying and analyzing these incidents. Which of the following options would best enable the incident handler to detect and analyze the suspected attacks in this scenario?

- A.** Use of a network-based intrusion detection system (IDS) to detect any anomalies in network traffic.
- B.** Manual review of IIS server logs for SQL injection and XSS attack patterns.
- C.** Running a vulnerability scan on the web application to detect any potential weak points that could be exploited by an attacker.
- D.** Deployment of a Web Application Firewall (WAF) such as dotDefender to detect, block, and log SQL injection and XSS attacks.

Answer: ([SHOW ANSWER](#))

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam! Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:
https://www.actual4test.com/212-89_examcollection.html (**359** Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 137

John, a professional hacker, is attacking an organization, where he is trying to destroy the connectivity between an AP and client to make the target unavailable to other wireless devices.

Which of the following attacks is John performing in this case?

- A.** Routing attack
- B.** EAP failure
- C.** Disassociation attack

D. Denial-of-service

Answer: C ([LEAVE A REPLY](#))

In a disassociation attack, the attacker sends disassociation frames to a wireless access point (AP) using a spoofed MAC address of a client or to the client pretending to be the AP. This forces the target to disconnect and often reconnect, causing a disruption in the wireless connectivity.

Such attacks can be used to create a denial-of-service condition for the client, making the network resource unavailable. The primary objective of this attack is not to eavesdrop but to disrupt the normal operation of the wireless connection between the client and the AP.

NEW QUESTION: 138

XYZ Inc. was affected by a malware attack and James, being the incident handling and response (IH&R) team personnel handling the incident, found out that the root cause of the incident is a backdoor that has bypassed the security perimeter due to an existing vulnerability in the deployed firewall. James had contained the spread of the infection and removed the malware completely.

Now the organization asked him to perform incident impact assessment to identify the impact of the incident over the organization and he was also asked to prepare a detailed report of the incident. Which of the following stages in IH&R process is James working on?

- A. Notification
- B. Evidence gathering and forensics analysis
- C. Post-incident activities
- D. Eradication

Answer: ([SHOW ANSWER](#))

James is working on the post-incident activities stage of the Incident Handling and Response (IH&R) process. After containing the spread of the infection and removing the malware, the focus shifts to assessing the impact of the incident on the organization and preparing a detailed report.

This phase involves analyzing the extent of the damage, determining the cost of the attack, evaluating how well the incident was managed, and identifying lessons learned to improve future response efforts. The objective is to restore systems to normal operation, ensure no remnants of the threat remain, and implement measures to prevent recurrence.

NEW QUESTION: 139

Which of the following methods help incident responders to reduce the false-positive alert rates and further provide benefits of focusing on topmost priority issues reducing potential risk and corporate liabilities?

- A. Threat profiling
- B. Threat contextualization
- C. Threat correlation
- D. Threat attribution

Answer: ([SHOW ANSWER](#))

Threat correlation is a method used by incident responders to analyze and associate various indicators of compromise (IoCs) and alerts to identify genuine threats. By correlating data from multiple sources and applying intelligence to distinguish between unrelated events and coordinated attack patterns, responders can significantly reduce the rate of false-positive alerts.

This enables teams to prioritize their efforts on the most critical and likely threats, thereby reducing potential risks and corporate liabilities. Effective threat correlation involves the use of sophisticated security information and event management (SIEM) systems, threat intelligence platforms, and analytical techniques to identify relationships between seemingly disparate security events and alerts.

NEW QUESTION: 140

Who is mainly responsible for providing proper network services and handling network-related incidents in all the cloud service models?

- A. Cloud consumer
- B. Cloud auditor
- C. Cloud brokers
- D. Cloud service provide

Answer: ([SHOW ANSWER](#))

In cloud computing environments, the responsibility for providing and managing network services, as well as handling incidents related to these services, primarily falls on the cloud service provider. This includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models. The cloud service provider is tasked with ensuring the availability, integrity, and security of the network services they offer. This responsibility includes managing and responding to incidents that may affect these services, ranging from security breaches to performance issues. The cloud service provider employs a variety of tools and techniques to monitor the network, identify potential threats, and implement corrective actions to mitigate any impact on the services and their users.

NEW QUESTION: 141

As an incident handler, you are responsible for managing unauthorized access incidents. After a series of reconnaissance attacks on your network, you have employed tools such as Wireshark and Nmap to detect the incidents. During one such scenario, you notice an IP address,

10.10.10.9, has been repeatedly conducting ICMP echo requests and TCP SYN scans.

What would be your immediate course of action to mitigate the situation?

- A. Ignore the IP address 10.10.10.9. as it is not causing harm to the network.
- B. Report the IP address 10.10.10.9 to local law enforcement.
- C. Launch a counter-attack against IP address 10.10.10.9.

D. Block the IP address 10.10.10.9 at the firewall level.

Answer: (SHOW ANSWER)

NEW QUESTION: 142

FinServ, a financial services firm, experienced a significant malware attack. Once the immediate threat was contained, a massive cleanup ensued. A board meeting was convened to determine the final steps to ensure system integrity. Among the proposed solutions, which ensures a thorough eradication of malware?

- A. Reinstalling the OS on affected machines and restoring data from trusted backups.
- B. Relying on a combination of multiple antivirus solutions for enhanced detection.
- C. Consulting with external cybersecurity firms for an in-depth system analysis.
- D. Implementing stricter firewall policies and access controls.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 143

A company utilizing multiple cloud services aims to enhance its posture against cloud security incidents. Among the following options, which constitutes the best practice for achieving this goal?

- A. Regularly conduct penetration testing exclusively on their most critical cloud-based assets.
- B. Focus on physical security measures at the company's offices to prevent data breaches.
- C. Centralize logging and monitoring across all cloud services for improved visibility and anomaly detection.
- D. Implement a single cloud service provider strategy to simplify security management.

Answer: C (LEAVE A REPLY)

Centralized logging and monitoring is a core best practice in cloud incident detection and response under ECIH. Cloud environments are distributed and dynamic, making visibility a major challenge.

Option C is correct because aggregating logs from multiple cloud platforms enables correlation, faster detection, and effective incident triage. ECIH emphasizes centralized visibility as essential for identifying cross-platform threats.

Options A and D are limited in scope. Option B does not address cloud-specific risks.

NEW QUESTION: 144

Eric works as a system administrator in ABC organization. He granted privileged users with unlimited permissions to access the systems. These privileged users can misuse their rights unintentionally or maliciously or attackers can trick them to perform malicious activities. Which of the following guidelines helps incident handlers to eradicate insider attacks by privileged users?

- A. Do not use encryption methods to prevent administrators and privileged users from accessing backup tapes and sensitive information
- B. Do not control the access to administrators and privileged users
- C. Do not enable the default administrative accounts to ensure accountability
- D. Do not allow administrators to use unique accounts during the installation process

Answer: C (LEAVE A REPLY)

The guideline that helps incident handlers to eradicate insider attacks by privileged users is to ensure accountability by not enabling default administrative accounts. Instead, organizations should require administrators and privileged users to use individual accounts that can be audited and traced back to specific actions and users. This practice enhances security by ensuring that all actions taken on the system can be attributed to individual users, reducing the risk of misuse of privileges and making it easier to identify the source of malicious activities or policy violations.

The other options listed either present insecure practices or misunderstandings of security protocols that would not help in eradicating insider attacks.

NEW QUESTION: 145

Which of the following is a term that describes the combination of strategies and services intended to restore data, applications, and other resources to the public cloud or dedicated service providers?

- A. Mitigation
- B. Analysis
- C. Eradication
- D. Cloud recovery

Answer: D (LEAVE A REPLY)

The term that describes the combination of strategies and services intended to restore data, applications, and other resources to the public cloud or dedicated service providers is "Cloud recovery." This term encompasses disaster recovery efforts focused on ensuring that an organization's digital assets can be quickly and effectively restored or moved to cloud environments in the event of data loss, system failure, or a disaster. Cloud recovery strategies are part of a broader disaster recovery and business continuity planning, ensuring minimal downtime and data loss by leveraging cloud computing's scalability and flexibility. Mitigation, analysis, and eradication are terms associated with other aspects of incident response and risk management, not specifically with the restoration of resources to cloud environments.

NEW QUESTION: 146

In response to suspicious communications originating from executive accounts, the organization's response team traced the root to spoofed identity relays exploiting unsecured DNS entries. The attack had triggered internal responses but required deeper remediation to eliminate recurring forged message injections and restore the integrity of

interdepartmental mail routing. What action reflects an appropriate eradication strategy in this context?

- A. Requesting legal review of communication failures post-incident.
- B. Sharing phishing indicators with external peer communities.
- C. Investigating the delay in threat detection due to slow analysis.
- D. Strengthening SPF, DKIM, and DMARC configurations.

Answer: D ([LEAVE A REPLY](#))

Strengthening SPF, DKIM, and DMARC helps verify authorized mail sources, validate message integrity, and enforce domain-based authentication policies. This directly addresses spoofed identity relays and reduces recurring forged email injections.

NEW QUESTION: 147

The incident handling and response(IH&R) team of a large multinational corporation recently identified a security incident. Using the Microsoft Baseline Security Analyzer (MBSA) and buck- security tools, they discovered several missing security patches and misconfigurations on their Windows and Linux systems, respectively. In the incident management process, what should be the next appropriate step the team needs to perform after the detection and analysis of vulnerabilities?

- A. Proceed with the eradication of vulnerabilities and patch the system.
- B. Evaluate the extent of damage caused by the security incident and perform damage control.
- C. Initiate the implementation of an incident response plan for similar future incidents.
- D. Re-scan the systems to validate the accuracy of the initial vulnerability reports.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 148

A multinational consultancy firm recently conducted a mobile security awareness session after noticing repeated incidents of suspicious activity on corporate-linked Android devices. During the session, IT discovered that several employees had been sideloading APK files from unofficial third-party websites to access premium apps for free. These unauthorized installations introduced malware that compromised login credentials, triggered unauthorized data exfiltration, and bypassed existing security filters. Further investigation revealed that the company lacked enforcement of application certification checks on enrolled Android devices, and employees were unaware of the risks of using unverified sources. What security control should be prioritized to prevent such behavior in the future?

- A. Require full-disk encryption for both device storage and application data.
- B. Enforce MDM Policies that allow only signed app installations.
- C. Restrict Bluetooth and NFC-based application communication channels.
- D. Enable remote location tracking for corporate Android devices.

Answer: ([SHOW ANSWER](#))

Enforcing mobile device management policies that permit only signed and trusted application installations prevents users from sideloading unverified APKs from unofficial sources. This directly reduces the risk of malware introduced through unauthorized mobile applications.

NEW QUESTION: 149

Which of the following does not represent a primary objective of an incident response plan?

- A.** Resolving interpersonal disputes within the human resources team
- B.** Leveraging insights from previous incidents to improve future responses and enhance defense mechanisms
- C.** Facilitating rapid recovery from cyber incidents to minimize service disruption, data loss, and theft
- D.** Effectively handling legal implications that arise during or after an incident

Answer: A ([LEAVE A REPLY](#))

The main goal of incident response is to efficiently manage cybersecurity events that threaten an organization's data, systems, or operations. The process aims to limit damage, ensure rapid recovery, maintain business continuity, and learn from each incident to strengthen defenses moving forward. However, resolving internal staff conflicts--such as disputes in the HR department--is outside the scope of cybersecurity incident response, making Option A the correct answer.

Incident response frameworks are developed to handle security breaches, malware infections, data leaks, denial-of-service attacks, and other related cyber events. A well-defined incident response plan consists of several phases: preparation, detection and analysis, containment, eradication, recovery, and lessons learned. These stages ensure that organizations react in a timely, structured, and legally compliant manner.

NEW QUESTION: 150

As a Certified Incident Handler at a multinational corporation, you are notified of a possible data breach incident in one of the departments. During the initial investigation, you confirmed that one workstation was used to execute the malicious activity. You need to ensure the integrity of the evidence for further forensic analysis. What should your first response action be regarding the affected workstation?

- A.** Photograph the workstation and document the hardware configuration.
- B.** Shut down the workstation immediately to stop potential data loss.
- C.** Use an antivirus to scan the workstation and delete any detected malware.
- D.** Immediately disconnect the workstation from the network but leave it running.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 151

You are an incident handler for a large corporation and have identified suspicious network activity involving repeated ICMP ECHO requests from an unknown IP. Utilizing your knowledge of network reconnaissance techniques, you suspect a ping sweep attack is in progress. What should be your next course of action to validate your suspicions using the tools and techniques mentioned in the lab scenario?

- A. Monitor VSFTPD logs to identify suspicious file transfers.
- B. Apply the filter `icmp.type==8` or `icmp.type==0` in Wireshark to detect the ping sweep attempts.
- C. Execute the command `nmap -sP 10.10.10.1/24` on the Ubuntu machine to identify active hosts.
- D. Start a new packet capture in Wireshark and apply the filter `tcp.flags.syn==1` to observe the SYN scan attack.

Answer: ([SHOW ANSWER](#))

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam! Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:
https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 152

An EC-Council Certified Incident Handler (ECIH) is preparing a cloud-based company for potential security incidents. She's focusing on best practices to fortify the company's defenses against such events. Given the following measures, which one should the ECIH prioritize?

- A. Limiting the use of third-party applications within the cloud environment.
- B. Regularly updating and patching all cloud-based systems.
- C. Frequently changing all users' passwords in the cloud environment.
- D. Implementing a zero-trust architecture across all network resources.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 153

Stanley works as an incident responder at a top MNC based in Singapore. He was asked to investigate a cybersecurity incident that recently occurred in the company. While investigating the incident, he collected evidence from the victim systems. He must present this evidence in a clear and comprehensible manner to the members of a jury so that the evidence clarifies the facts and further helps in obtaining an expert opinion on the incident

to confirm the investigation process. In the above scenario, which of the following characteristics of the digital evidence did Stanley attempt to preserve?

- A. Completeness
- B. Admissibility
- C. Believability
- D. Authenticity

Answer: B (LEAVE A REPLY)

In the scenario described, Stanley's effort to present evidence in a clear and comprehensible manner to the members of a jury, with the intention of clarifying facts and aiding in obtaining expert opinion, aligns with the characteristic of admissibility. The admissibility of digital evidence pertains to its acceptability in a court of law, which hinges on the evidence being collected, handled, and presented in a manner that complies with legal standards and procedures. This includes ensuring the evidence is relevant, reliable, and not overly prejudicial. By preparing to present the evidence in a way that the jury can understand and use to confirm the investigation process, Stanley is focusing on ensuring that the evidence meets the criteria for admissibility in the legal proceedings.

Completeness, believability, and authenticity are also important characteristics of digital evidence, but the context provided indicates that Stanley's primary focus is on meeting the legal requirements for the evidence to be considered valid in court.

NEW QUESTION: 154

As an incident handler, you received an email that appeared suspicious. You performed an email header analysis using the online tool MxToolbox. The results showed SPF Authenticated as Failed." " DKIM Authenticated as Failed," "SPF Alignment as Pass," and "DKIM Alignment as Pass." According to these results, which of the following conclusions is most accurate?

- A. The email is likely malicious because SPF authentication failed but safe because DKIM alignment passed.
- B. The email is safe and legitimate because the SPF and DKIM alignments both passed.
- C. The email is likely safe because SPF alignment passed, even though DKIM authentication failed.
- D. The email is likely malicious because SPF and DKIM authentications both failed.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 155

Which of the following is not called volatile data?

- A. Open sockets or open ports
- B. The date and time of the system
- C. Creation dates of files
- D. State of the network interface

Answer: C (LEAVE A REPLY)

Volatile data refers to information that is stored temporarily and is lost when a computer is turned off or restarted, such as RAM contents, including open sockets and open ports, the date and time of the system, and the state of the network interface. The creation dates of files, however, are considered non-volatile data because they are preserved on the hard drive and remain available after the system is restarted or turned off. Non-volatile data is stored on persistent storage mediums like hard drives, SSDs, and magnetic tapes, where it remains until it is deleted or overwritten.

NEW QUESTION: 156

You are the Azure security incident response lead for a large organization. Your team has identified a potential security incident in one of the Azure subscriptions. Upon investigation, you find that an unauthorized user has gained access to an Azure Storage account containing sensitive data. What is the MOST appropriate immediate action to take?

- A.** Notify the organization's data protection officer (DPO) and initiate a data breach assessment.
- B.** Enable Azure Security Center to enhance monitoring and threat detection.
- C.** Create a backup of the compromised Azure Storage account for forensic analysis.
- D.** Disable access keys for the compromised Azure Storage account.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 157

An IT security analyst at a logistics firm is alerted to unusual outbound traffic originating from an employee's mobile device connected to the corporate VPN. Antivirus scans fail to remove the malware, indicating persistence. The organization cannot afford further data leakage. Which action should the incident handler take next?

- A.** Disable the SIM card.
- B.** Switch the device to airplane mode.
- C.** Perform a factory reset or reinstall the mobile OS.
- D.** Restrict background app refresh for social apps.

Answer: C ([LEAVE A REPLY](#))

Persistent mobile malware that survives antivirus scans indicates deep system compromise. The ECIH Endpoint and Mobile Incident Handling guidance states that when malware cannot be reliably removed, reimaging or OS reinstallation is the safest remediation.

Option C is correct because performing a factory reset or reinstalling the OS ensures complete removal of malicious components and restores device integrity. ECIH cautions that partial containment actions may stop symptoms but not eradicate threats.

Options A and B are temporary containment steps. Option D is ineffective against malware.

Therefore, full OS reinstallation is the correct next action.

NEW QUESTION: 158

John is performing memory dump analysis in order to find out the traces of malware. He has employed volatility tool in order to achieve his objective. Which of the following volatility framework commands he will use in order to analyze running process from the memory dump?

- A. `python vol.py svcscan --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem | more`
- B. `python vol.py pslist --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem`
- C. `python vol.py hivelist --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem`
- D. `python vol.py imageinfo -f /root/Desktop/memdump.mem`

Answer: B (LEAVE A REPLY)

The Volatility framework is a widely used tool for analyzing volatile memory (RAM) dumps. It is especially useful in digital forensics and malware analysis. One of the fundamental tasks in memory analysis is to list the processes that were running on the system at the time the memory dump was taken. The `pslist` command in the Volatility framework serves this purpose by listing all processes from the process list in memory, which can provide valuable insights into what was happening on the system, including the presence of any malicious processes. The syntax provided in the answer option corresponds to the usage of the `pslist` command with the Volatility tool, specifying the memory dump file to be analyzed (`-f /root/Desktop/memdump.mem`) and the profile of the system from which the dump was taken (`--profile=Win2008SP1x86`). This information is crucial for accurate analysis, as the profile helps Volatility interpret the memory structures correctly.

NEW QUESTION: 159

A company facing a wave of spoofed payment emails launched an investigation and found that employees had unknowingly interacted with malicious sender domains. Despite blocking initial IPs and purging visible email content, similar threats resurfaced using altered variants. The team moved to eliminate recurring delivery mechanisms and close technical loopholes. Which step is most aligned with this eradication initiative? Which data theft method was most likely used in this incident?

- A. Creating email-specific URL deny-lists from decoded message components.
- B. Launching email-based simulation drills to evaluate user response to phishing.
- C. Reviewing the email training curriculum related to financial transaction safety.
- D. Contacting email domain registrars to request WHOIS masking of sender information.

Answer: (SHOW ANSWER)

Creating URL deny-lists from decoded email components directly targets recurring phishing delivery infrastructure, including altered sender domains and embedded malicious links. The likely data theft method was phishing through spoofed payment emails designed to trick employees into interacting with malicious domains.

NEW QUESTION: 160

A global retail enterprise operating across multiple e-commerce platforms and physical locations has recently been targeted by a well-orchestrated cyberattack that disrupted transaction processing systems and led to a temporary shutdown of online services. Following the incident, customer confidence dropped, and the board demanded immediate corrective and preventive measures to strengthen cybersecurity resilience. The Chief Information Security Officer (CISO) directed the incident response team to establish a forward-looking approach that not only mitigates such incidents but also ensures that all stakeholders are trained in advance. This includes defining clear roles and responsibilities, creating and training a dedicated response team, conducting simulation exercises, reviewing existing IR tools, auditing organizational assets, and developing a comprehensive set of policies and playbooks. Which phase of the IH&R process should the organization focus on to achieve this?

- A.** Execute recovery processes as per system restoration guidelines and predefined operational procedures
- B.** Initiate the preparation phase as outlined by standard incident readiness practices and team coordination steps
- C.** Perform eradication procedures as required by internal protocols following threat containment and internal review
- D.** Begin triage activities to assess and organize incidents according to classification and prioritization criteria

Answer: B (LEAVE A REPLY)

The EC-Council Incident Handler (ECIH) curriculum clearly defines the Preparation Phase as the foundation of an effective Incident Handling and Response (IH&R) program. This phase focuses on establishing readiness before incidents occur. Activities include defining roles and responsibilities, forming and training the incident response team, conducting simulation and tabletop exercises, auditing assets, reviewing response tools, and developing formal policies and playbooks.

The scenario explicitly describes forward-looking corrective and preventive measures such as simulation exercises, stakeholder training, asset auditing, and policy development. These are hallmark activities of the Preparation phase. ECIH emphasizes that organizations lacking structured preparation often experience delayed response, unclear accountability, and increased operational impact during cyber incidents.

NEW QUESTION: 161

If a hacker cannot find any other way to attack an organization, they can influence an employee or a disgruntled staff member. What type of threat is this?

- A.** Phishing attack
- B.** Insider attack
- C.** Footprinting
- D.** Identity theft

Answer: B (LEAVE A REPLY)

If a hacker influences an employee or a disgruntled staff member to gain access to an organization's resources or sensitive information, this is classified as an insider attack. Insider attacks are perpetrated by individuals within the organization, such as employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems. The threat from insiders can be intentional, as in the case of a disgruntled employee seeking to harm the organization, or unintentional, where an employee is manipulated or coerced by external parties without realizing the implications of their actions. Phishing attacks, footprinting, and identity theft represent different types of cybersecurity threats where the attacker's method or objective differs from that of insider attacks.

NEW QUESTION: 162

An IoT device deployed in a smart city infrastructure project begins transmitting data at an unusually high rate, signaling a potential security compromise. This device is part of a critical system that monitors traffic flow and controls street lighting, making unauthorized access or manipulation a significant concern for public safety and urban efficiency. What should be the first action taken by the smart city's incident response team to handle this IoT-based security incident effectively?

- A.** Update the firmware of all IoT devices within the smart city infrastructure as a precautionary measure.
- B.** Launch a city-wide campaign to raise awareness about the security risks associated with IoT devices.
- C.** Immediately isolate the compromised IoT device from the network to prevent further unauthorized activity.
- D.** Collaborate with the device manufacturer to investigate the cause of the unusual data transmission.

Answer: C (LEAVE A REPLY)

In IoT and OT environments, the ECIH curriculum emphasizes that containment is the highest first-response priority, especially when public safety and critical services are involved. The abnormal data transmission strongly suggests compromise, and allowing the device to remain connected risks lateral movement, data exfiltration, and operational disruption.

Option C is correct because immediate isolation of the affected IoT device prevents further unauthorized communication while preserving the system's current state for forensic analysis.

Isolation limits the blast radius without unnecessarily disrupting the entire infrastructure. Option A introduces risk by changing system states during an active incident. Option B is preventive and not an incident response action. Option D is appropriate after containment but not before.

Thus, isolating the compromised device aligns with ECIH endpoint and IoT incident handling principles.

NEW QUESTION: 163

A multinational corporation has been receiving a large number of phishing attacks lately. As the newly appointed Incident Handler, you have been tasked with improving the company's ability to detect and handle these attacks. The existing infrastructure consists of several virtual machines running Windows Server 2016, Windows 10, and Ubuntu, and administrative privileges are available to install and run the required tools. Which of the following methods should you primarily implement to enhance the company's ability to handle these email security incidents?

- A.** Implementing PGP encryption for all email communications to prevent unauthorized access to email content.
- B.** Installing the Netcraft Toolbar on all company systems to block phishing websites.
- C.** Using PhishTank to verify and track all suspicious links in emails received by the company.
- D.** Training employees to detect phishing attacks and encouraging them to report suspicious emails.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 164

WebMega, a leading e-commerce giant with over a billion users, suffered a massive data breach, compromising sensitive user data, including financials. During the containment phase, IH&R teams discovered a meticulous attack pattern that bypassed multiple security layers, hinting at an insider's involvement. Investigations revealed that three recently fired employees, with ties to a rival company, had possible motives and means. How should WebMega proceed?

- A.** Reinforce security measures across the board, with a focus on employee access controls, without addressing the potential insider threat directly.
- B.** Collaborate with external forensic experts and law enforcement agencies to conduct a thorough investigation while maintaining confidentiality.
- C.** Reach out to the rival company's leadership, seeking an off-the-record resolution without involving legal channels.
- D.** Publicly accuse the rival company of corporate espionage and initiate legal proceedings based on the initial evidence.

Answer: ([SHOW ANSWER](#)**)**

This scenario involves a suspected malicious insider threat with potential external collusion, which significantly elevates legal, regulatory, and evidentiary requirements. The ECIH curriculum emphasizes that when insider activity is suspected--especially involving terminated employees and possible corporate espionage--organizations must prioritize forensic integrity, confidentiality, and lawful investigation.

Option B is correct because collaborating with external forensic experts and law enforcement ensures a neutral, legally defensible investigation. ECIH stresses that insider

cases often require specialized forensic capabilities, evidence preservation, and legal authority that internal teams alone may not possess. Maintaining confidentiality protects the organization from reputational damage and legal exposure while facts are being established.

Option A ignores the insider dimension and risks repeat incidents. Option C bypasses legal safeguards and could be interpreted as obstruction or collusion. Option D is premature and exposes the organization to defamation and legal risk without substantiated evidence. ECIH guidance is clear that complex insider incidents should be escalated appropriately with legal and forensic rigor. Therefore, Option B aligns best with recommended practice.

NEW QUESTION: 165

During routine monitoring, a cloud-based application hosting provider detects an anomaly suggesting an ongoing DDoS attack targeting one of its hosted applications. The provider's incident response team must quickly mitigate the attack while ensuring minimal service disruption. Which of the following strategies should they prioritize?

- A.** Immediately scale up application resources to absorb the attack impact.
- B.** Enable geo-restriction to block incoming traffic from regions not serviced by the application.
- C.** Temporarily take the affected application offline to stop the attack.
- D.** Implement rate limiting and challenge-response tests to differentiate between legitimate and malicious traffic.

Answer: D (LEAVE A REPLY)

The ECIH Network Security Incident Handling module emphasizes maintaining availability while mitigating denial-of-service attacks. The objective is not simply to stop traffic, but to distinguish malicious traffic from legitimate user requests.

Option D is correct because rate limiting and challenge-response mechanisms (such as CAPTCHA or SYN cookies) allow legitimate traffic to continue while throttling or blocking malicious requests. This approach minimizes service disruption while effectively containing the attack.

Option A may increase costs and still fail against large-scale DDoS attacks. Option B can unintentionally block legitimate users. Option C contradicts ECIH guidance by unnecessarily impacting availability.

ECIH stresses proportional and intelligent mitigation strategies that preserve business continuity.

Therefore, implementing rate limiting and challenge-response mechanisms is the preferred strategy.

NEW QUESTION: 166

An employee accidentally emails confidential customer information to a personal email address.

What is the biggest challenge faced by the incident response team in this scenario?

- A. Balancing the need for confidentiality and transparency with stakeholders
- B. Identifying the source of the email server used to send the email
- C. Identifying the extent of the damage caused by the incident
- D. Determining the intent of the employee

Answer: A (LEAVE A REPLY)

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam!
Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:
https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 167

An insider threat response plan helps an organization minimize the damage caused by malicious insiders. One of the approaches to mitigate these threats is setting up controls from the human resources department. Which of the following guidelines can the human resources department use?

- A. Access granted to users should be documented and vetted by a supervisor.
- B. Disable the default administrative account to ensure accountability.
- C. Implement a person-to-person rule to secure the backup process and physical media.
- D. Monitor and secure the organization's physical environment.

Answer: A (LEAVE A REPLY)

One of the key approaches to mitigating insider threats is ensuring that access control policies are strictly implemented and monitored. This includes the guideline that access granted to users should be thoroughly documented and vetted by a supervisor. This control helps ensure that users have only the access necessary to perform their job functions, reducing the risk of inappropriate access or misuse of information. Proper documentation and supervisor approval also ensure accountability and traceability of access decisions, which is crucial for detecting and responding to insider threats. The human resources department plays a vital role in this process, working closely with IT and security teams to enforce access control policies, conduct regular reviews of access rights, and manage the onboarding and offboarding process to ensure that access rights are appropriately updated.

NEW QUESTION: 168

Tara, a certified first responder in a digital forensics team, is dispatched to investigate a suspected insider attack targeting a critical workstation in the finance department. Upon arriving at the scene, she takes a methodical approach: she begins labeling all connected

network cables, photographs the back panel of the workstation, documents cable connections, and records the power status of each connected device, including peripherals like external drives and monitors.

She also notes the orientation and placement of equipment on the desk and the surrounding environment. These actions are part of her protocol to ensure that, if the devices need to be moved for forensic analysis, investigators can accurately replicate the system's physical setup at the time of the incident. What is Tara aiming to achieve with these actions?

- A. Create a physical reconstruction reference
- B. Maintain the continuity of system uptime
- C. Capture device logs in real-time
- D. Execute evidence integrity hashing

Answer: (SHOW ANSWER)

This scenario directly reflects crime scene documentation and physical reconstruction, a core principle in the Forensic Readiness and First Response module of the ECIH curriculum. First responders must assume that every physical detail may later become relevant in court proceedings or advanced forensic reconstruction.

Option A is correct because Tara's actions--photographing cable connections, labeling ports, documenting power states, and noting spatial orientation--are explicitly designed to allow investigators to recreate the original physical environment. ECIH emphasizes that improper documentation of physical layout can invalidate conclusions about device usage, peripheral connections, or data paths.

Option B is incorrect because uptime continuity is not her objective. Option C refers to live system analysis, which she is not performing. Option D applies to digital evidence integrity after acquisition, not scene documentation.

ECIH stresses that physical reconstruction references are especially important in insider threat investigations, where proving who had access, which devices were connected, and how data could have been transferred is critical. Tara's approach ensures forensic soundness, minimizes contamination risk, and preserves contextual evidence.

NEW QUESTION: 169

At NeoTech, after a suspected insider threat incident, a smartphone believed to be a key piece of evidence was secured. While waiting for forensic experts, what should the incident handler do to maintain the phone's data integrity?

- A. Keep the phone turned on and prevent it from locking.
- B. Charge the phone continuously to avoid power loss.
- C. Take photos of all opened apps and active screens for documentation.
- D. Place the phone in a Faraday bag to prevent remote wiping or communication.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 170

Your organization uses the Google Cloud Platform for its operations. You, as an EC-Council Certified Incident Handler, have been alerted of a potential security incident involving unauthorized access to sensitive data. Which of the following should be your first step in handling this incident?

- A. Perform an initial analysis of the GCP audit logs.
- B. Shut down all instances on GCP.
- C. Disable all user accounts on GCP.
- D. Initiate an immediate backup of all data.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 171

Which of the following has been used to evade IDS and IPS?

- A. Fragmentation
- B. TNP
- C. HTTP
- D. SNMP

Answer: A ([LEAVE A REPLY](#))

Fragmentation is a technique used by attackers to evade detection by Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). By breaking down packets into smaller fragments, attackers can make it more difficult for these security systems to detect malicious payloads or signature-based patterns associated with known attacks. This method exploits the fact that some IDS/IPS solutions may not properly reassemble packet fragments for analysis, thereby allowing malicious fragments to pass through undetected.

NEW QUESTION: 172

Which of the following risk mitigation strategies involves execution of controls to reduce the risk factor and brings it to an acceptable level or accepts the potential risk and continues operating the IT system?

- A. Risk assumption
- B. Risk avoidance
- C. Risk planning
- D. Risk transference

Answer: A ([LEAVE A REPLY](#))

Risk assumption involves accepting the potential risk and continuing to operate the IT system while implementing controls to reduce the risk to an acceptable level. This strategy acknowledges that some level of risk is inevitable and focuses on managing it through mitigation measures rather than eliminating it entirely. Risk avoidance would entail taking actions to avoid the risk entirely, risk planning involves preparing for potential risks, and risk transference shifts the risk to another party, typically through insurance or outsourcing. Risk assumption is a pragmatic approach that balances the need for operational continuity with the imperative of risk management.

NEW QUESTION: 173

QualTech Solutions is a leading security services enterprise. Dickson works as an incident responder with this firm. He is performing vulnerability assessment to identify the security problems in the network, using automated tools to identify the hosts, services, and vulnerabilities present in the enterprise network.

Based on the above scenario, identify the type of vulnerability assessment performed by Dickson.

- A. Internal assessment
- B. Active assessment
- C. Passive assessment
- D. External assessment

Answer: B (LEAVE A REPLY)

An active assessment involves using automated tools to scan and probe the network actively to identify hosts, services, and vulnerabilities. This type of assessment directly interacts with the network components to gather information about the existing security posture, unlike passive assessments, which analyze traffic without sending packets to the target systems. Dickson's approach, employing automated tools to identify the network's hosts, services, and vulnerabilities, fits the definition of an active assessment. This method provides a more immediate understanding of the network's vulnerabilities, allowing for timely remediation actions.

NEW QUESTION: 174

Eric is an incident responder and is working on developing incident-handling plans and procedures. As part of this process, he is performing an analysis on the organizational network to generate a report and develop policies based on the acquired results. Which of the following tools will help him in analyzing his network and the related traffic?

- A. Whois
- B. Burp Suite
- C. FaceNiff
- D. Wireshark

Answer: D (LEAVE A REPLY)

Wireshark is a widely used network protocol analyzer that helps in capturing and interactively browsing the traffic on a network. It is an essential tool for incident responders like Eric who are developing incident-handling plans and procedures. By analyzing network traffic, Wireshark allows users to see what is happening on their network at a microscopic level, making it invaluable for troubleshooting network problems, analyzing security incidents, and understanding network behavior. Whois is used for querying databases that store registered users or assignees of an Internet resource. Burp Suite is a tool for testing web application security, and FaceNiff is used for session hijacking within a WiFi network, which makes Wireshark the best choice for analyzing network traffic.

NEW QUESTION: 175

An incident responder for a multinational organization has successfully installed ActivTrak on the Windows Server 2016 machine, aiming to monitor and detect insider threats. After a day of monitoring, the incident responder notices a user accessing social media websites extensively during work hours and also finds multiple entries for a highly confidential internal web application in the TOP SITES pie chart of the ActivTrak dashboard. What should be the incident responder's immediate action?

- A. Proceed with system isolation of the user's workstation and revoke user access privileges
- B. Engage the human resources team to talk to the user regarding time spent on social media.
- C. Ignore the findings, as they do not directly indicate any malicious activity.
- D. Consult with the security team to analyze the user's activities and the accessed data for potential threats.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 176

After experiencing a large-scale distributed denial-of-service (DDoS) attack that caused service outages, a national telecom provider recovered its web platform. The IH&R team must now implement post-recovery measures to enhance resilience against future DDoS attempts. Which action would be most effective?

- A. Remove antivirus to speed up application response
- B. Configure a CDN and implement blackhole routing
- C. Add guest user accounts for remote diagnostics
- D. Increase FTP access for easier maintenance

Answer: B (LEAVE A REPLY)

This question focuses on post-incident recovery and resilience, a key ECIH concept. After restoring services, organizations must strengthen defenses to prevent recurrence.

Option B is correct because Content Delivery Networks (CDNs) distribute traffic and absorb volumetric attacks, while blackhole routing discards malicious traffic upstream.

ECIH identifies these as industry-standard controls for DDoS resilience.

Options A, C, and D weaken security or increase attack surface and contradict ECIH guidance.

ECIH stresses that recovery is not complete until preventive measures are implemented.

CDN deployment and upstream traffic control significantly improve availability during future attacks.

NEW QUESTION: 177

Mr. Smith is a lead incident responder of a small financial enterprise having few branches in Australia. Recently, the company suffered a massive attack losing USD 5 million through

an inter-banking system. After in-depth investigation on the case, it was found out that the incident occurred because 6 months ago the attackers penetrated the network through a minor vulnerability and maintained the access without any user being aware of it. Then, he tried to delete users' fingerprints and performed a lateral movement to the computer of a person with privileges in the inter-banking system.

Finally, the attacker gained access and did fraudulent transactions.

Based on the above scenario, identify the most accurate kind of attack.

- A. Ransomware attack
- B. Denial-of-service attack
- C. APT attack
- D. Phishing

Answer: (SHOW ANSWER)

The scenario described fits the characteristics of an Advanced Persistent Threat (APT) attack.

APTs are sophisticated, stealthy, and continuous computer hacking processes often orchestrated by groups targeting a specific entity. These attackers penetrate the network through vulnerabilities, maintain access without detection, and achieve their objectives, such as data exfiltration or financial theft, over an extended period. The fact that attackers exploited a minor vulnerability, maintained access for six months, and performed lateral movements to access critical systems for fraudulent transactions highlights the strategic planning and persistence typical of APT attacks.

NEW QUESTION: 178

Darwin is an attacker residing within the organization and is performing network sniffing by running his system in promiscuous mode. He is capturing and viewing all the network packets transmitted within the organization. Edwin is an incident handler in the same organization.

In the above situation, which of the following Nmap commands Edwin must use to detect Darwin's system that is running in promiscuous mode?

- A. `nmap -sV -T4 -O -F -version-light`
- B. `nmap -sU -p 500`
- C. `nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]`
- D. `nmap --script hostmap`

Answer: C (LEAVE A REPLY)

The GPG18 and Forensic readiness planning (SPF) principles outline various guidelines to enhance an organization's readiness for forensic investigation and response. Principle 5, which suggests that organizations should adopt a scenario-based Forensic Readiness Planning approach that learns from experience gained within the business, emphasizes the importance of being prepared for a wide range of potential incidents by leveraging lessons learned from past experiences. This approach helps in continuously improving

forensic readiness and response capabilities by adapting to the evolving threat landscape and organizational changes.

NEW QUESTION: 179

Adam is an attacker who along with his team launched multiple attacks on target organization for financial benefits. Worried about getting caught, he decided to forge his identity. To do so, he created a new identity by obtaining information from different victims. Identify the type of identity theft Adam has performed.

- A. Medical identity theft
- B. Tax identity theft
- C. Synthetic identity theft
- D. Social identity theft

Answer: C (LEAVE A REPLY)

Synthetic identity theft is a type of fraud where the perpetrator combines real (often stolen) and fake information to create a new identity. This can include combining a real social security number with a fictitious name, or other variations that result in an identity that is not entirely real but has elements that can pass through verification processes. In the scenario described, Adam is creating a new identity using information from different victims, which is characteristic of synthetic identity theft. This type of fraud is particularly challenging to detect and counter because it does not directly impersonate a single real individual but creates a plausible new identity that can be used to open accounts, obtain credit, and conduct transactions that can be financially beneficial to the attacker.

NEW QUESTION: 180

GlobalTech recently faced a series of advanced attacks. Post-incident analysis led them to discover a malicious software disguised as an update module for their ERP system. The malware exhibited intricate behavior, making its detection challenging. The security team needs to determine its functionality and potential damage. What should be their primary approach?

- A. Conduct a behavior analysis of the malware in an isolated, controlled environment.
- B. Update all systems and deploy a network-wide antivirus scan.
- C. Notify stakeholders and clients of a potential data breach.
- D. Seek vendor guidance on ERP-related vulnerabilities.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 181

Which of the following confidentiality attacks do attackers try to lure users by posing themselves as authorized AP by beaconing the WLAN's SSID?

- A. Evil twin AP
- B. Session hijacking
- C. Honeypot AP

D. Masqueradin

Answer: A (LEAVE A REPLY)

In the described attack, where attackers pose as legitimate access points (APs) by beaconing the WLAN's SSID to lure users, the attack is known as an Evil twin AP attack. This type of attack involves setting up a rogue AP with the same SSID as a legitimate wireless access point, making it appear as an authorized network to users. Unsuspecting users may connect to this malicious AP, allowing attackers to intercept sensitive information, conduct man-in-the-middle attacks, or distribute malware. The Evil twin AP attack exploits the trust users have in known SSIDs to compromise their security.

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam! Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:
https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 182

A computer virus hoax is a message warning the recipient of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipient to forward it to everyone they know. Which of the following is not a symptom of virus hoax message?

- A. The message warns to delete certain files if the user does not take appropriate action
- B. The message from a known email id is caught by SPAM filters due to change in filter settings
- C. The message prompts the end user to forward it to his/her email contact list and gain monetary benefits in doing so
- D. The message prompts the user to install Anti-virus

Answer: C (LEAVE A REPLY)

NEW QUESTION: 183

AlphaTech, a cloud-based storage company, recently suffered data leakage. Investigation revealed an employee sent sensitive client data to a personal email. AlphaTech wants to implement a solution to monitor and prevent such incidents. What should they prioritize?

- A. Mandate employees to attend cyber hygiene workshops every month.
- B. Implement a Data Loss Prevention (DLP) tool to monitor sensitive data movement.
- C. Limit email attachments to 5MB for all employees.
- D. Block all personal email domains on the company network.

Answer: B (LEAVE A REPLY)

This scenario represents a classic insider data exfiltration incident, where a legitimate user abuses authorized access to move sensitive information outside organizational boundaries. The ECIH Insider Threat module clearly identifies Data Loss Prevention (DLP) as the primary technical control for detecting and preventing such activity.

Option B is correct because DLP solutions are designed to monitor, classify, and control sensitive data in motion, at rest, and in use. DLP can detect when regulated or confidential data is sent via email, uploaded to cloud services, or copied to external destinations, and can block or alert on policy violations in real time. ECIH emphasizes that DLP is especially effective against low-and- slow insider leaks that bypass perimeter defenses.

Option A improves awareness but does not enforce controls. Option C is overly restrictive and does not prevent other exfiltration channels. Option D is blunt and easily bypassed while disrupting legitimate business use.

ECIH guidance stresses layered insider threat defenses combining policy, monitoring, and enforcement. DLP provides visibility and control without relying solely on user behavior, making it the most effective priority action.

NEW QUESTION: 184

Francis received a spoof email asking for his bank information. He decided to use a tool to analyze the email headers. Which of the following should he use?

- A.** EventLog Analyzer
- B.** MxToolbox
- C.** Email Checker
- D.** PoliteMail

Answer: B (LEAVE A REPLY)

MxToolbox is a comprehensive tool designed for analyzing email headers and diagnosing various email delivery issues. When Francis received a spoofed email asking for his bank information, using MxToolbox to analyze the email headers would be appropriate. This tool helps in examining the source of the email, tracking the email's path across the internet from the sender to the receiver, and identifying any signs of email spoofing or malicious activity. It provides detailed information about the email servers encountered along the way and can help in verifying the authenticity of the email sender. Other options like EventLog Analyzer, Email Checker, and PoliteMail are tools used for different purposes such as analyzing system event logs, checking email address validity, and managing email communications, respectively, and do not specifically focus on analyzing email headers to the extent required for investigating a spoofed email incident.

NEW QUESTION: 185

Which of the following techniques prevent or mislead incident-handling process and may also affect the collection, preservation, and identification phases of the forensic investigation process?

- A.** Scanning

- B. Footprinting
- C. Enumeration
- D. Anti-forensics

Answer: ([SHOW ANSWER](#))

Anti-forensics techniques are designed to prevent, mislead, or interfere with the incident handling process, affecting the collection, preservation, and identification phases of the forensic investigation process. These techniques include methods to erase, encrypt, or alter information, make data recovery difficult, hide data (e.g., steganography), or otherwise obstruct forensic analysis and investigation efforts. Anti-forensics can significantly challenge the efforts of incident responders and forensic investigators in establishing the facts of a security incident or crime.

NEW QUESTION: 186

During an email security incident, the Incident Handler & Response (IH&R) team in a certain organization decided to use Pretty Good Privacy (PGP) protocols via the Gpg4win tool to secure email communications. While creating a backup of keys, one of the IH&R team members forgot to make a note of the location of the backup files. What could be the potential impact of this mistake?

- A. The member will be unable to sign the outgoing messages with his private key.
- B. The member will not be able to retrieve the public key for future communications.
- C. The member will fail to decrypt received messages encrypted with his public key.
- D. The member will not be able to encrypt messages using the recipient's public key.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 187

A cybersecurity analyst at a technology firm discovers suspicious activity on a network segment dedicated to research and development. The initial indicators suggest a possible compromise of several endpoints with potential intellectual property theft. Given the sensitive nature of the data involved, what is the most effective method for the analyst to detect and validate the security incident?

- A. Immediately notify law enforcement and regulatory bodies.
- B. Isolate the affected network segment and manually inspect each endpoint.
- C. Deploy an endpoint detection and response (EDR) solution to identify and investigate suspicious activities.
- D. Conduct a network-wide vulnerability scan.

Answer: C ([LEAVE A REPLY](#))

The ECIH Endpoint Security module stresses that modern endpoint incidents require advanced detection capabilities beyond traditional antivirus or manual inspection. Intellectual property theft often involves stealthy techniques that evade basic controls. Option C is correct because an Endpoint Detection and Response (EDR) solution provides deep visibility into endpoint behavior, including process execution, memory activity, file

changes, and lateral movement. EDR enables analysts to detect, investigate, and validate incidents efficiently across multiple endpoints.

Option B is slow and error-prone. Option A is premature without validation. Option D identifies vulnerabilities, not active compromise.

ECIH highlights EDR as a cornerstone technology for endpoint incident detection and validation, especially in high-value environments such as R&D networks.

NEW QUESTION: 188

FinFusion, a leading finance firm, discovered a slow leak of financial data over several months.

Surprisingly, the leak was attributed to a high-ranking executive who was selling data to competitors. Keen on avoiding future breaches, what should be FinFusion's foremost action?

- A.** Use advanced Employee Monitoring Tools that offer real-time threat alerts.
- B.** Limit executive access to sensitive databases.
- C.** Require weekly reports from executives on their data access and usage.
- D.** Install security cameras in executive offices.

Answer: ([SHOW ANSWER](#))

This scenario involves a high-privilege insider threat, one of the most difficult risks to detect. ECIH emphasizes that senior executives often have broad access, making role-based restrictions impractical.

Option A is correct because advanced employee monitoring and behavioral analytics can detect abnormal access patterns, data exfiltration trends, and deviations from established baselines-- even for executives. These tools operate within legal and policy frameworks while providing actionable alerts.

Options B and C reduce efficiency and are easily bypassed. Option D is intrusive and ineffective for digital exfiltration.

ECIH identifies behavioral monitoring as the most effective control for detecting malicious insiders with legitimate access, making Option A correct.

NEW QUESTION: 189

Identify the malicious program that is masked as a genuine harmless program and gives the attacker unrestricted access to the user's information and system. These programs may unleash dangerous programs that may erase the unsuspecting user's disk and send the victim's credit card numbers and passwords to a stranger.

- A.** Worm
- B.** Adware
- C.** Virus
- D.** Trojan

Answer: D ([LEAVE A REPLY](#))

A Trojan, or Trojan horse, is a type of malware that disguises itself as a legitimate, harmless program or file to trick users into downloading and installing it. Once activated, a Trojan can perform a range of malicious activities, including giving attackers unauthorized access to the infected system. This can lead to the theft of sensitive information, such as credit card numbers and passwords, and can also allow the attacker to install additional malware, potentially leading to further damage, such as the erasure of data. Unlike viruses and worms, Trojans do not replicate themselves but rely on the deception of users to spread.

NEW QUESTION: 190

Which of the following tools helps incident responders effectively contain a potential cloud security incident and gather required forensic evidence?

- A.** Alert Logic
- B.** CloudPassage Quarantine
- C.** Qualys Cloud Platform
- D.** Cloud Passage Halo

Answer: D (LEAVE A REPLY)

Cloud Passage Halo is a security platform designed to provide comprehensive visibility and protection for cloud environments, making it an effective tool for incident responders dealing with potential cloud security incidents. It offers capabilities for detecting, responding to, and containing threats across public, private, and hybrid cloud environments. With features like automated security policies, compliance monitoring, and threat detection, Cloud Passage Halo enables incident responders to quickly contain incidents and gather the required forensic evidence to investigate the scope and impact of a breach or security issue. Tools like Alert Logic and Qualys Cloud Platform also provide security and compliance solutions for cloud environments, but Cloud Passage Halo is specifically recognized for its robust incident response and containment capabilities.

NEW QUESTION: 191

An Azure administrator discovers unauthorized access to a storage account containing sensitive documents. The initial investigation suggests compromised credentials. In response to this incident, what should be the administrator's first action to secure the account?

- A.** Move sensitive documents to a new storage account with restricted access.
- B.** Reset the credentials of the compromised account and review all recent access logs.
- C.** Contact Azure support for an immediate investigation and assistance.
- D.** Enable Azure Multi-Factor Authentication (MFA) for all user accounts accessing the storage.

Answer: B (LEAVE A REPLY)

This incident indicates credential compromise, a common cloud security issue addressed in the ECIH Cloud Incident Handling module. When credentials are suspected to be

compromised, the immediate priority is to stop unauthorized access and determine the scope of misuse.

Option B is correct because resetting the compromised credentials immediately cuts off the attacker's access. Reviewing recent access logs allows responders to validate what actions were taken, which data was accessed, and whether additional accounts were affected. ECIH emphasizes immediate credential revocation as a first-response action in identity-based cloud incidents.

Option D (enabling MFA) is a critical hardening measure but does not immediately revoke compromised credentials. Option A is a recovery step that may not stop ongoing access.

Option C may be necessary later but should not delay immediate containment.

Therefore, resetting credentials and reviewing logs is the most effective first action, fully aligned with ECIH guidance.

NEW QUESTION: 192

An organization suffers a financial loss after an executive responds to a fraudulent email crafted as part of a spear phishing attack. After isolating affected systems and notifying internal stakeholders, the incident response team prepares a detailed report outlining the attack timeline, suspicious IP addresses, email metadata, phone scam details, and the amount lost. This report is forwarded to a government agency specializing in cybercrime to aid further investigation and potential restitution. Which aspect of the recovery process is the organization addressing?

A. Legal escalation and investigation support

B. Data redundancy planning

C. Endpoint protection deployment

D. Internal server reconfiguration

Answer: (SHOW ANSWER)

This scenario reflects the post-incident recovery and reporting phase outlined in the ECIH curriculum. After containment and eradication, organizations must address legal, regulatory, and investigative requirements, especially when financial fraud and executive compromise are involved.

Option A is correct because forwarding detailed incident reports to a government cybercrime agency constitutes legal escalation and investigation support. ECIH stresses the importance of cooperation with law enforcement in cases involving fraud, financial loss, or cross-border criminal activity. Proper documentation supports potential prosecution, restitution efforts, and regulatory compliance.

Options B, C, and D are technical recovery actions unrelated to legal follow-up.

By engaging authorities with verified evidence, the organization fulfills its recovery obligations beyond technical remediation, aligning with ECIH best practices.

NEW QUESTION: 193

An organization implemented an encoding technique to eradicate SQL injection attacks. In this technique, if a user submits a request using single-quote and some values, then the encoding technique will convert it into numeric digits and letters ranging from a to f. This prevents the user request from performing SQL injection attempt on the web application. Identify the encoding technique used by the organization.

- A. Unicode encoding
- B. Base64 encoding
- C. Hex encoding
- D. URL encoding

Answer: C ([LEAVE A REPLY](#))

Hex encoding (also known as hexadecimal encoding) involves converting binary data into hexadecimal representation. In the context described, when a user submits a request with potentially malicious input (such as a single quote and other characters in an attempt to perform SQL injection), the encoding technique converts this input into a string of hexadecimal digits (ranging from 0 to 9 and A to F). This prevents the direct interpretation of the input as SQL commands by the database, thereby mitigating the risk of SQL injection attacks. This method is a form of input sanitization that helps ensure that user input cannot be used to manipulate database queries directly.

NEW QUESTION: 194

A malicious, security-breaking program is disguised as a useful program. Such executable programs, which are installed when a file is opened, allow others to control a user's system. What is this type of program called?

- A. Trojan
- B. Worm
- C. Virus
- D. Spyware

Answer: ([SHOW ANSWER](#))

A Trojan, short for Trojan horse, is a type of malicious software that misleads users of its true intent. It disguises itself as a legitimate and useful program, but once executed, it allows unauthorized access to the user's system. Unlike viruses and worms, Trojans do not replicate themselves but can be just as destructive. They are often used to create a backdoor to a computer system, allowing an attacker to gain access to the system or to deliver other malware.

Trojans can be used for a variety of purposes, including stealing information, downloading or uploading files, monitoring the user's screen and keyboard, and more. The term "Trojan" comes from the Greek story of the wooden horse that was used to sneak soldiers into the city of Troy, which is analogous to the deceptive nature of this type of malware in cyber security.

NEW QUESTION: 195

Eric who is an incident responder is working on developing incident-handling plans and procedures. As part of this process, he is performing analysis on the organizational network to generate a report and to develop policies based on the acquired results. Which of the following tools will help him in analyzing network and its related traffic?

- A. FaceNiff
- B. Wireshark
- C. Burp Suite
- D. Whois

Answer: B (LEAVE A REPLY)

Wireshark is a network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network. It is a crucial tool for incident responders like Eric who are developing incident-handling plans and need to analyze network traffic and patterns. Wireshark can provide detailed information about the network, including protocols used, source and destination of packets, and potential signs of malicious activity, making it invaluable for developing informed policies and procedures.

NEW QUESTION: 196

Marley was asked by his incident handling and response (IH&R) team lead to collect volatile data such as system information and network information present in the registries, cache, and RAM of victim's system.

Identify the data acquisition method Marley must employ to collect volatile data.

- A. Validate data acquisition
- B. Static data acquisition
- C. Live data acquisition
- D. Remote data acquisition

Answer: C (LEAVE A REPLY)

Live data acquisition is the process of collecting volatile data from a system that is still running.

Volatile data includes information stored in system memory (RAM), cache, and system and network configuration settings that are lost when the system is powered off. This method is essential for capturing data that can provide insights into the state of the system at the time of an incident, including active network connections, running processes, and the contents of memory.

Marley must employ live data acquisition to ensure that this crucial and ephemeral data is not lost, which can be pivotal in understanding and responding to the incident effectively.

Valid 212-89 Dumps shared by Actual4test.com for Helping Passing 212-89 Exam!
Actual4test.com now offer the **newest 212-89 exam dumps**, the Actual4test.com
212-89 exam **questions have been updated** and **answers have been corrected** get

the **newest** Actual4test.com 212-89 dumps with Test Engine here:

https://www.actual4test.com/212-89_examcollection.html (359 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 197

During the vulnerability assessment phase, the incident responders perform various steps as below:

1. Run vulnerability scans using tools
2. Identify and prioritize vulnerabilities
3. Examine and evaluate physical security
4. Perform OSINT information gathering to validate the vulnerabilities
5. Apply business and technology context to scanner results
6. Check for misconfigurations and human errors
7. Create a vulnerability scan report

Identify the correct sequence of vulnerability assessment steps performed by the incident responders.

- A. 3-->6-->1-->2-->5-->4-->7
- B. 1-->3-->2-->4-->5-->6-->7
- C. 4-->1-->2-->3-->6-->5-->7
- D. 2-->1-->4-->7-->5-->6-->3

Answer: C (LEAVE A REPLY)

The correct sequence of steps performed by incident responders during the vulnerability assessment phase is as follows:

Perform OSINT information gathering to validate the vulnerabilities

(4): Initially, Open Source Intelligence (OSINT) is used to gather information about the organization's digital footprint and potential vulnerabilities.

Run vulnerability scans using tools

(1): Next, specialized tools are employed to scan the organization's networks and systems for vulnerabilities. Identify and prioritize vulnerabilities (2): The identified vulnerabilities are then analyzed and prioritized based on their severity and potential impact on the organization. Examine and evaluate physical security (3): Physical security assessments are also crucial as they can impact the overall security posture and protection of digital assets. Check for misconfigurations and human errors (6): This step involves looking for misconfigurations in systems and networks, as well as potential human errors that could lead to vulnerabilities. Apply business and technology context to scanner results (5): The results from the scans are evaluated within the context of the business and its technology environment to accurately assess risks.

Create a vulnerability scan report

(7): Finally, a comprehensive report is created, detailing the vulnerabilities, their severity, and recommended mitigation strategies. This sequence ensures a thorough assessment,

prioritizing vulnerabilities that pose the greatest risk and providing actionable insights for mitigation.

NEW QUESTION: 198

A national healthcare organization with multiple branches is facing growing cybersecurity challenges due to unmanaged systems, inconsistent configurations, and a lack of asset visibility.

In response, leadership has asked the security team to implement a proactive strategy aimed at minimizing exposure across all departments. This includes identifying hardware and software in use, enforcing consistent security settings, and establishing a routine process to detect system weaknesses before they can be exploited. The security team is seeking a well-established, practical framework that emphasizes prioritized, real-world security practices and can be implemented efficiently with available resources. Which of the following frameworks would BEST support this proactive security initiative?

- A.** Employing CIS Critical Security Controls for foundational defensive actions
- B.** Implementing NIST 800-61 for policy and incident lifecycle development
- C.** Applying ITIL for restoring disrupted business services
- D.** Using COBIT for strategic enterprise governance modeling

Answer: (SHOW ANSWER)

The EC-Council Incident Handler (ECIH) curriculum highlights the importance of proactive security controls, asset management, configuration management, and vulnerability management as foundational elements of forensic readiness and incident prevention.

The scenario describes challenges related to unmanaged systems, inconsistent configurations, and lack of asset visibility--core issues addressed by the CIS Critical Security Controls (CIS CSC). The CIS Controls provide prioritized, actionable cybersecurity best practices designed to mitigate the most common attack vectors. These include inventory and control of hardware assets, inventory and control of software assets, secure configuration of enterprise assets, continuous vulnerability management, and controlled use of administrative privileges.

ECIH emphasizes that organizations must first establish visibility into assets and enforce baseline security configurations to reduce attack surfaces. The CIS framework is specifically designed for practical implementation, making it ideal for organizations seeking efficient deployment using available resources.

NEW QUESTION: 199

Jack, a senior incident responder at a major financial institution, was urgently assigned to investigate a web application incident that had impacted several customers. The incident was first detected through customer complaints reporting redirection to suspicious external websites after logging in or interacting with the web platform.

As Jack dug into the server logs and update routines, he identified an alarming discovery: the application's auto-update mechanism had silently downloaded and integrated a

malicious update package from an unverified and untrusted third-party source. This update had been unintentionally trusted and applied without proper signature validation or integrity checks.

Post-compromise, the malicious update began injecting redirect scripts into various web pages, causing legitimate users to be redirected to unknown or phishing websites. This exposed both user data and institutional reputation to significant risk. Upon further inspection, Jack confirmed that the update process lacked secure code verification methods such as digital signature validation or secure update channels, which allowed the attacker to tamper with the software delivery pipeline. Identify the type of web application security throat discovered by Jack in the above scenario.

- A.** Software and data integrity failure
- B.** Identification and authentication failure
- C.** Security logging and monitoring failure
- D.** Security misconfiguration

Answer: A (LEAVE A REPLY)

The incident resulted from trusting and applying a malicious update without verifying its source, integrity, or digital signature. This matches a software and data integrity failure because the application allowed untrusted code to enter the update pipeline and alter legitimate web content.

NEW QUESTION: 200

Following a high-profile breach investigation at a multinational corporation, an incident handler is tasked with the critical role of preserving, packaging, and transporting digital evidence from a server believed to be compromised and utilized as part of a global botnet operation. The challenge lay not only in the technical complexities of the operation but also in adhering to stringent legal and procedural frameworks to ensure the evidence remained admissible in court.

The server, containing potentially millions of records of illicit transactions, represented a key piece of the puzzle in understanding the breadth of the breach. The incident handler had to navigate through multiple layers of security protocols to access the server, all while ensuring that the evidence was handled in a manner that prevented any form of tampering or degradation during the collection, packaging, and transport phases. The handler's decision would set a precedent for the handling of digital evidence within the organization, underlining the importance of adopting a method that upheld the highest standards of evidence integrity and forensic soundness. Which of the following options ensures the highest level of evidence integrity during its transport?

- A.** On-site encryption of the server's data, followed by its upload to a secure cloud storage solution, with the entire process meticulously documented for future verification.
- B.** Creating a forensic image of the server's drives, conducting a verification of the image hashes, storing these images on encrypted drives, and compiling a detailed log of the transport procedure.

- C.** Encasing the server in anti-static packaging, labelling it meticulously with the chain of custody documentation, and securing it in a locked container for transportation.
- D.** Transferring the server data onto a newly secured drive using a write blocker, placing it within a tamper-evident bag, and employing GPS tracking for the transport process.

Answer: B (LEAVE A REPLY)

ECIH forensic readiness guidance stresses that forensic imaging with hash verification is the gold standard for preserving evidence integrity. Option B is correct because it ensures data integrity, authenticity, and non-repudiation.

Creating a bit-by-bit forensic image preserves original evidence while allowing analysis on copies.

Hash verification confirms that no alterations occur during acquisition or transport.

Encrypted storage protects confidentiality, and detailed logs support chain of custody.

Options A, C, and D lack one or more critical forensic requirements such as hash validation or evidentiary isolation. ECIH explicitly warns against relying solely on physical transport or live data transfers.

NEW QUESTION: 201

What is the best staffing model for an incident response team if current employees' expertise is very low?

- A.** Fully insourced
- B.** Fully outsourced
- C.** All the above
- D.** Partially outsourced

Answer: B (LEAVE A REPLY)

NEW QUESTION: 202

QualTech Solutions is a leading security services enterprise. Dickson, who works as an incident responder with this firm, is performing a vulnerability assessment to identify the security problems in the network by using automated tools for identifying the hosts, services, and vulnerabilities in the enterprise network. In the above scenario, which of the following types of vulnerability assessment is Dickson performing?

- A.** Active assessment
- B.** External assessment
- C.** Internal assessment
- D.** Passive assessment

Answer: A (LEAVE A REPLY)

In the scenario described, Dickson is performing an active assessment. This type of vulnerability assessment involves using automated tools to actively scan and probe the network for identifying hosts, services, and vulnerabilities. Unlike passive assessments, which rely on monitoring network traffic without direct interaction with the targets, active assessments engage directly with the network infrastructure to discover vulnerabilities,

misconfigurations, and other security issues by sending data to systems and analyzing the responses. This approach provides a more immediate and detailed view of the security posture but can also generate detectable traffic that might be noticed by defensive systems or affect the performance of live systems.

NEW QUESTION: 203

After a successful exploitation attempt, a university web server started exhibiting anomalies such as high server load, random form submission errors, and repeated spam complaints. Hosting providers flagged the domain as suspicious and disabled the web application. The IH&R team discovered new unknown files within the web root directory. Which action would be most appropriate to contain the incident and avoid further damage?

- A.** Perform a scan to identify injection points and isolate the affected component from the network.
- B.** Reconfigure form validations for improved user experience.
- C.** Run a stress test to ensure hosting capacity is sufficient.
- D.** Immediately re-enable the application after restoring from backup.

Answer: A (LEAVE A REPLY)

This scenario reflects a compromised web application, likely due to injection attacks or file upload exploitation. The ECIH Web Application Incident Handling module emphasizes that containment must prevent further attacker access and stop malicious execution.

Option A is correct because identifying injection points and isolating affected components halts further exploitation and allows forensic investigation. ECIH warns against restoring or re-enabling applications without understanding the attack vector, as this often leads to reinfection.

Options B and C do not address security. Option D risks reintroducing malware if vulnerabilities remain.

Thus, targeted isolation and vulnerability identification is the correct containment action.

NEW QUESTION: 204

A company's IoT network is experiencing a DDoS attack, disrupting critical operations. What is the best course of action for the incident response team in this scenario?

- A.** Block all incoming traffic to the IoT network
- B.** Disconnect the affected IoT devices from the network
- C.** Increase bandwidth to the IoT network to handle the attack
- D.** Notify senior management and other stakeholders

Answer: B (LEAVE A REPLY)

212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-89 dumps with Test Engine here:

https://www.actual4test.com/212-89_examcollection.html (**359** Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)