EC-COUNCIL.212-89.v2026-07-03.q125

Exam Code:	212-89
Exam Name:	EC Council Certified Incident Handler (ECIH v3)
Certification Provider:	EC-COUNCIL
Free Question Number:	125
Version:	v2026-07-03
# of views:	104
# of Questions views:	1250
https://www.freepdfdumps.com/EC-COUNCIL.212-89.v2026-07-03.q125.html	

NEW QUESTION: 1
Shiela is working at night as an incident handler. During a shift, servers were affected by a massive cyberattack. After she classified and prioritized the incident, she must report the incident, obtain necessary permissions, and perform other incident response functions. What list should she check to notify other responsible personnel?
A. HR log book
B. Point of contact
C. Email list
D. Phone number list
Answer: B (LEAVE A REPLY)
In the context of incident handling, the "point of contact" list is essential for ensuring that Sheila, the incident handler working at night, can quickly notify the responsible personnel within the organization about the cyberattack. This list typically includes the contact information of key stakeholders and decision-makers who need to be informed about security incidents, allowing for timely communication, decision-making, and response coordination.
References:Incident Handler (ECIH v3) courses and study guides stress the importance of having a well-maintained point of contact list as part of an organization's incident response plan to facilitate efficient and effective communication during and after cybersecurity incidents.

NEW QUESTION: 2
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: A (LEAVE A REPLY)
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.
Option B relates to policy review, not field evidence handling. Option C involves technical log analysis performed later during investigation. Option D concerns witness interviews, which are separate from physical evidence handling.
Rachel's actions clearly describe the packaging and transporting of electronic evidence while maintaining forensic standards and documentation integrity.

NEW QUESTION: 3
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 ano 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.
References:The ECIH v3 program emphasizes the importance of managing privileged access and ensuring accountability among users with elevated permissions to protect against insider threats and misuse of administrative rights.

NEW QUESTION: 4
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: 5
David, a certified digital first responder, arrives at the scene of a reported security breach in the HR department of a corporate office. The breach involves multiple digital endpoints, including desktop systems and mobile devices. Upon entering the scene, David observes that one desktop computer is still powered ON and logged in, showing a sensitive financial dashboard on the screen. Realizing the importance of preserving this evidence, David refrains from interacting directly with the keyboard or running applications. Instead, he takes high-resolution photographs of the screen to capture the current session details, including open applications and time-sensitive data. To avoid altering the system state, David gently moves the mouse without clicking, just enough to dismiss a screen saver without triggering any on-screen changes. He records the system's behavior, notes any visible alerts or programs running, and tags all connected cables and peripheral ports for proper documentation. What step in the evidence handling process is David demonstrating?
A. Seizing off-site backups
B. Preserving volatile evidence from an active system
C. Executing a shutdown script on Linux
D. Handling a powered-off device
Answer: B (LEAVE A REPLY)

This scenario demonstrates preservation of volatile evidence, a critical first-response principle in the ECIH forensic readiness module. Volatile evidence includes data that exists only while a system is powered on, such as active sessions, running processes, open files, and on-screen information.
Option B is correct because David documents the live system state without interacting in a way that would alter evidence. Photographing the screen, recording visible activity, and documenting connections are all recommended ECIH practices when dealing with powered-on systems.
Option A is unrelated. Option C alters system state. Option D applies only to inactive devices.
ECIH stresses that mishandling active systems can destroy crucial evidence. David's actions align precisely with first responder best practices, making Option B correct.

NEW QUESTION: 6
Michael, a digital forensic responder, enters a server room after a suspected data breach. He ensures all individuals not involved in the investigation are escorted out, avoids altering any device configurations, and isolates the server from the network without powering it down. What is the main goal of Michael's actions?
A. Creating a chain of custody
B. Collecting volatile memory
C. Securing and evaluating the crime scene
D. Cloning the affected server
Answer: (SHOW ANSWER)
Michael's actions reflect crime scene control, a foundational first-response principle in the ECIH forensic readiness module. Securing the area, preventing unauthorized access, and avoiding system changes preserve evidence integrity.
Option C is correct because his primary objective is to secure and evaluate the digital crime scene before evidence collection begins. ECIH stresses that scene control prevents contamination, tampering, and accidental evidence destruction.
Options A, B, and D may follow but are not the immediate objective.

NEW QUESTION: 7
Farheen is an incident responder at reputed IT Firm based in Florida. Farheen was asked to investigate a recent cybercrime faced by the organization. As part of this process, she collected static data from a victim system. She used DD tool command to perform forensic duplication to obtain an NTFS image of the original disk. She created a sector-by-sector mirror imaging of the disk and saved the output image file as image.dd.
Identify the static data collection process step performed by Farheen while collecting static data.
A. Comparison
B. Administrative consideration

C. System preservation
D. Physical presentatio
Answer: C (LEAVE A REPLY)
Farheen's activity of using the DD tool to create a sector-by-sector mirror image of the original disk is an example of system preservation. This process is crucial in digital forensics for creating an exact copy of a storage device to ensure that the original data remains unchanged during the investigation. By making a forensic duplication, or image, of the disk, Farheen ensures that the static data on the disk is preserved in its current state for thorough analysis, without altering the original evidence. This step allows investigators to work with a precise replica of the data, protecting the integrity of the original evidence.
References:The Incident Handler (ECIH v3) certification materials discuss various methods and tools for data acquisition and preservation, highlighting the importance of system preservation in the initial stages of forensic analysis.

NEW QUESTION: 8
Which of the following is an attack that attempts to prevent the use of systems, networks, or applications by the intended users?
A. Denial of service (DoS) attack
B. Fraud and theft
C. Unauthorized access
D. Malicious code or insider threat attack
Answer: (SHOW ANSWER)
A Denial of Service (DoS) attack aims to make a computer resource, network, or application unavailable to its intended users, thereby preventing legitimate users from using the service. This is achieved by overwhelming the target with a flood of internet traffic or sending information that triggers a crash. In contrast, fraud and theft involve the unauthorized acquisition of data or assets, unauthorized access refers to gaining entry into systems without permission, and malicious code or insider threat attacks relate to software designed to cause harm or unauthorized actions by trusted users within the organization. The specific intent of a DoS attack is to disrupt service, making it a distinct category focused on denial of availability.
References:The Incident Handler (ECIH v3) certification materials discuss various types of cybersecurity threats, including DoS attacks, outlining their methods, objectives, and impacts on targeted systems or networks.

NEW QUESTION: 9
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: C (LEAVE A REPLY)
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.
References:The role of threat correlation in improving the efficiency of incident response activities by reducing false positives and focusing on high-priority issues is outlined in various cybersecurity frameworks and incident response guides, including those related to the ECIH v3 certification. These resources emphasize the importance of applying context and intelligence to security alerts to accurately identify and respond to genuine threats.

NEW QUESTION: 10
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?
A. Contacting email domain registrars to request WHOIS masking of sender information
B. Launching email-based simulation drills to evaluate user response to phishing
C. Reviewing the email training curriculum related to financial transaction safety
D. Creating email-specific URL deny-lists from decoded message components
Answer: D (LEAVE A REPLY)
This scenario describes a persistent phishing campaign leveraging spoofed domains and variant-based delivery mechanisms. According to the EC-Council Incident Handler (ECIH) curriculum under Email Security Incident Handling and Eradication, once detection and containment measures (such as blocking malicious IP addresses and purging emails) have been implemented, the eradication phase must focus on eliminating root causes and recurring technical vectors.
The key phrase in the question is "eliminate recurring delivery mechanisms and close technical loopholes." ECIH emphasizes that phishing campaigns frequently evolve by modifying URLs, sender domains, encoding techniques, and payload structures to bypass simple IP blocking controls. Therefore, security teams must analyze decoded message components, extract malicious URLs, and generate URL-based deny-lists at the secure email gateway, web proxy, and firewall layers.

Creating email-specific URL deny-lists directly disrupts the attack infrastructure and prevents repeated access to malicious domains-even when attackers use variant IP addresses or modified content. This is a technical eradication control aligned with eliminating delivery vectors.
Options B and C (training and simulations) are preventive awareness measures and fall under the preparation or post-incident improvement phase-not eradication. Option A (WHOIS masking) is unrelated to preventing phishing delivery.
ECIH guidance stresses strengthening email filtering rules, updating domain and URL blacklists, implementing SPF/DKIM/DMARC validation, and hardening secure email gateways as core eradication techniques. Therefore, option D best aligns with the eradication objective.

NEW QUESTION: 11
Nervous Nat often sends emails with screenshots of what he thinks are serious incidents, but they always turn out to be false positives. Today, he sends another screenshot, suspecting a nation-state attack. As usual, you go through your list of questions, check your resources for information to determine whether the screenshot shows a real attack, and determine the condition of your network. Which step of IR did you just perform?
A. Recovery
B. Preparation
C. Remediation
D. Detection anc analysis (or identification)
Answer: D (LEAVE A REPLY)
When you receive a screenshot from Nervous Nat and go through a list of questions, check resources for information to determine the nature of the screenshot, and assess the condition of your network, you are engaging in the Detection and Analysis (or Identification) phase of Incident Response (IR). This phase is about identifying potential security incidents based on reported concerns, anomalies detected by security tools, or through the analysis of security alerts. In this scenario, despite the historical context of false positives, each report is treated seriously, requiring you to collect and analyze information to determine whether a real attack is happening. This involves verifying the validity of the incident, assessing its nature, scope, and impact, and deciding on the appropriate next steps. The detection and analysis phase is critical for determining the course of the IR process, including whether escalation is needed and what response measures should be initiated.
References:The ECIH v3 certification materials outline the Incident Response process, detailing steps from preparation, detection and analysis, containment, eradication, and recovery, to post-incident activities, highlighting the importance of thorough detection and analysis as the foundation for effective incident management.

NEW QUESTION: 12

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: A (LEAVE A REPLY)

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.

References:The EC-Council's Certified Incident Handler (ECIH v3) program covers various types of malware, including Trojans, in detail, explaining their mechanisms, how they can be identified, and the steps to take in response to such threats.

NEW QUESTION: 13

Daniel, a system administrator, was discovered accessing encrypted project files that had no relevance to his job responsibilities. A security audit revealed that his account had unrestricted access to all file servers, and there were no alerts or enforcement mechanisms in place to block or flag such access. Which countermeasure should have been in place to prevent this abuse?

A. Manual surveillance at workstations

B. Strictly configured personal firewall rules

C. Disabling the use of removable media

D. User segmentation through Zero Trust access

Answer: D (LEAVE A REPLY)

The EC-Council Incident Handler (ECIH) curriculum identifies excessive privileges as a major contributor to insider threats. In this scenario, Daniel had unrestricted access to all file servers, violating the Principle of Least Privilege (PoLP). The absence of enforcement mechanisms or alerts further indicates a lack of access governance.

Zero Trust architecture operates on the principle of "never trust, always verify." It enforces strict identity verification, continuous authentication, micro-segmentation, and role-based

access control. Under Zero Trust, users are granted access only to specific resources required for their job role, and all access attempts are logged and monitored.
User segmentation ensures that even administrators are restricted to only authorized systems and datasets.
ECIH stresses the importance of monitoring privileged accounts, implementing least privilege, enabling access auditing, and enforcing real-time alerting for unauthorized data access attempts.
Option A (manual surveillance) is impractical and ineffective at scale. Option B (personal firewall rules) protects network traffic but does not restrict file server permissions. Option C (disabling removable media) addresses data exfiltration via USB devices, not unauthorized file access.
Therefore, user segmentation through Zero Trust access would have prevented Daniel from accessing irrelevant encrypted project files and aligns directly with ECIH insider threat mitigation strategies.

NEW QUESTION: 14
NovoMed discovers encrypted data transfers of drug research and participant data to an unknown location and receives an extortion-like message implying the formula may be released. What is the most prudent course of action?
A. Immediately recall the drug from the market.
B. Publicly announce the breach warning competitors and authorities.
C. Negotiate with the attackers discreetly to buy time and retrieve data.
D. Engage local law enforcement and international cybercrime agencies to trace the transfer's origins.
Answer: (SHOW ANSWER)
Explanation (incident response governance):
This scenario combines data theft + extortion involving highly sensitive IP and regulated participant data.
The prudent course is to trigger formal legal/incident governance: engage law enforcement and appropriate cybercrime agencies (D), preserve evidence, and coordinate with legal counsel, regulators (if required), and cyber-insurance response processes. Law enforcement engagement can support intelligence sharing, preservation orders, and broader investigation into the infrastructure receiving the exfiltrated data.
(A) recalling the drug is not directly tied to the incident's immediate technical or legal response; it's a business decision that may be unnecessary and harmful without evidence of counterfeit risk. (B) immediate public announcement may be legally required in some jurisdictions, but it must be accurate and coordinated; doing it prematurely can worsen harm. (C) negotiation is risky and typically handled only through controlled legal and executive channels; it does not ensure data return and can incentivize further extortion.

Thus, (D) reflects best-practice escalation: treat it as a serious crime, preserve chain of custody, and coordinate response through legal and investigative authorities while technical teams contain and scope.

NEW QUESTION: 15
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.
References:The use of MxToolbox in incident handling and email security analysis is commonly recommended in Incident Handler (ECIH v3) study materials as a practical tool for email header analysis and spoofing investigation.

NEW QUESTION: 16
Which of the following options describes common characteristics of phishing emails?
A. Written in French
B. Sent from friends or colleagues
C. Urgency, threatening, or promising subject lines
D. No BCC fields
Answer: C (LEAVE A REPLY)
Phishing emails often share common characteristics designed to manipulate the recipient into taking immediate action. One of the hallmark features is the use of urgency, threatening language, or promising subject lines in the emails. These tactics are intended to create a sense of urgency or fear, compelling the recipient to respond quickly without giving due consideration to the legitimacy of the email. Phishing emails may claim that the recipient's account has been compromised, that they need to confirm personal information

immediately, or that they have won a prize. The goal is to trick the recipient into clicking on malicious links, opening attachments, or providing sensitive information.
References:The Certified Incident Handler (ECIH v3) program by EC-Council covers the identification and handling of phishing incidents, including the analysis of phishing emails and the importance of educating users on recognizing and responding to phishing attempts.

NEW QUESTION: 17
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: 18
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.
Option A involves email-based delivery, which is not described. Option B relates to manipulating search engine rankings but does not inherently describe memory-based exploit execution. Option D involves malicious advertisements; however, the scenario specifically references compromised websites rather than third-party ad platforms.
ECIH emphasizes patch management, browser hardening, memory analysis, and exploit mitigation technologies to defend against drive-by downloads. Therefore, the most consistent technique is a drive-by download attack exploiting vulnerabilities.

NEW QUESTION: 19

Zaimasoft, a prominent IT organization, was attacked by perpetrators who directly targeted the hardware and caused irreversible damage to the hardware. In result, replacing or reinstalling the hardware was the only solution.
Identify the type of denial-of-service attack performed on Zaimasoft.
A. ddos
B. DoS
C. PDoS
D. DRDoS
Answer: C (LEAVE A REPLY)
A Permanent Denial-of-Service (PDoS) attack, also known as "phlashing," is a form of attack that targets hardware, causing irreversible damage to the hardware components, thereby making the device unusable without a replacement or significant hardware intervention. In the scenario described with Zaimasoft, the attackers' actions leading to the damage of hardware components align with the characteristics of a PDoS attack. Unlike Distributed Denial-of-Service (DDoS) or Denial-of-Service (DoS) attacks, which generally aim to overwhelm a system's resources temporarily, or DRDoS (Distributed Reflection Denial of Service), which involves amplification techniques using third-party servers, a PDoS attack directly damages the physical hardware, necessitating its replacement or reinstallation. This makes PDoS particularly severe due to its permanent impact on the targeted organization's hardware infrastructure.
References:Incident Handler (ECIH v3) educational resources detail various types of denial-of-service attacks, including PDoS, highlighting the distinct nature of each attack and its implications on the affected systems, with PDoS being noted for its physical, irreparable impact on hardware components.

NEW QUESTION: 20
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: 21
Andrew, an incident responder, is performing risk assessment of the client organization. As a part of risk assessment process, he identified the boundaries of the IT systems, along with the resources and the information that constitute the systems.
Identify the risk assessment step Andrew is performing.
A. Control analysis
B. System characterization
C. Likelihood determination
D. Control recommendations
Answer: B (LEAVE A REPLY)
In the risk assessment process, "System characterization" is the initial step where the scope of the assessment is defined. This involves identifying and documenting the boundaries of the IT systems under review, the resources (hardware, software, data, and personnel) that constitute these systems, and any relevant information about their operation and environment. This foundational step is essential for understanding what needs to be protected and forms the basis for subsequent analysis, including identifying vulnerabilities, assessing potential threats, and determining the impact of risks to the organization.
References:The step of system characterization within the risk assessment process is discussed in detail in information security frameworks and incident response guides, including those related to the ECIH v3 certification. These guides stress the importance of accurately characterizing the system to ensure that the risk assessment is comprehensive and tailored to the specific context of the organization.

NEW QUESTION: 22
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: B (LEAVE A REPLY)
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.
References:The Certified Incident Handler (ECIH v3) curriculum by EC-Council discusses various information security incidents, including espionage, highlighting the need for comprehensive security measures, incident detection capabilities, and effective response strategies to protect against and respond to such threats.

NEW QUESTION: 23
An attack on a network is BEST blocked using which of the following?
A. IPS device inline
B. HIPS
C. Web proxy
D. Load balancer
Answer: A (LEAVE A REPLY)
An Intrusion Prevention System (IPS) device placed inline is best suited to block attacks on a network actively. Being inline allows the IPS to analyze and take action on the traffic as it passes through the device, effectively preventing malicious traffic from reaching its target. The IPS can detect and block a wide range of attacks in real-time by using various detection methods, such as signature-based detection, anomaly detection, and policy-based detection. Unlike Host-based Intrusion Prevention Systems (HIPS), web proxies, or load balancers, an inline IPS is specifically designed to inspect and act on incoming and outgoing network traffic to prevent attacks before they reach network devices or applications.
References:The Incident Handler (ECIH v3) certification materials discuss network security controls and emphasize the role of intrusion prevention systems in protecting networks against threats.

NEW QUESTION: 24
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)
Explanation (first response priorities):
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: 25
Dan is a newly appointed information security professional in a renowned organization. He is supposed to follow multiple security strategies to eradicate malware incidents. Which of the following is not considered as a good practice for maintaining information security and eradicating malware incidents?
A. Do not download or execute applications from third-party sources
B. Do not click on web browser pop-up windows
C. Do not open files with file extensions such as .bat, .com, ,exe, .pif, .vbs, and so on
D. Do not download or execute applications from trusted sources
Answer: D (LEAVE A REPLY)
The statement "Do not download or execute applications from trusted sources" is incorrect and not considered a good practice for maintaining information security and eradicating malware incidents. In contrast, downloading or executing applications from trusted sources is a fundamental security best practice. Trusted sources are vetted and are generally considered safe for downloading software, updates, and applications. This practice helps to minimize the risk of introducing malware into the organizational environment. The other options (A, B, C) represent good practices that help in reducing the likelihood of malware infections by avoiding potentially harmful actions.
References:The ECIH v3 materials from EC-Council provide guidance on best practices for malware prevention and response, underscoring the importance of relying on trusted

sources for software and application downloads as part of a robust information security strategy.

NEW QUESTION: 26
BadGuy Bob hid files in the slack space, changed the file headers, hid suspicious files in executables, and changed the metadata for all types of files on his hacker laptop. What has he committed?
A. Anti-forensics
B. Adversarial mechanics
C. Felony
D. Legal hostility
Answer: A (LEAVE A REPLY)
Anti-forensics refers to techniques used to hinder the forensic analysis of a computer system. By hiding files in slack space, changing file headers, embedding suspicious files in executables, and altering metadata, BadGuy Bob is attempting to make it difficult for forensic analysts to find, analyze, and attribute the malicious activities and data on his laptop. These actions are designed to conceal evidence, manipulate digital artifacts, and obstruct investigations, making them clear examples of anti-forensic techniques. While such actions could be part of broader criminal activities, constituting a felony, and could be seen as adversarial mechanics or legal hostility in specific contexts, the most accurate classification of these techniques is anti- forensics.
References:The ECIH v3 certification program includes discussions on forensic analysis and the challenges posed by anti-forensic techniques, teaching incident handlers how to recognize and counteract attempts to obstruct investigations.

NEW QUESTION: 27
OmegaTech Corp identified unauthorized remote access to its primary server and data exfiltration tunnels.
Simultaneously, IoT device firmware corruption was reported. As the first responder, what should Olivia prioritize?
A. Start reinstalling IoT firmware
B. Begin isolating the primary server and cutting off remote access
C. Alert all divisions to initiate a system-wide shutdown
D. Engage the AI-driven security system to trace unauthorized access
Answer: B (LEAVE A REPLY)
ECIH prioritizes containment of the most critical threat vector. The primary server actively exfiltrating data represents the highest risk.
Option B is correct because isolating the primary server immediately stops data loss and attacker control. IoT remediation can follow once core assets are secured.
Options A and D delay containment. Option C causes unnecessary disruption.

ECIH stresses that responders must address the most damaging threat first, making Option B correct.

NEW QUESTION: 28
Which of the following techniques helps incident handlers to detect man-in-the-middle attack by finding the new APs and trying to connect an already established channel, even if the spoofed AP consists similar IP and MAC addresses as of the original AP?
A. Wireless client monitoring
B. Network traffic monitoring
C. General wireless traffic monitoring
D. Access point monitoring
Answer: D (LEAVE A REPLY)
Access point monitoring is the technique that helps incident handlers to detect man-in-the-middle (MitM) attacks by continuously observing and managing the wireless access points (APs) within a network. This includes identifying unauthorized or new APs attempting to connect to the network or mimic existing APs, even if they present similar IP and MAC addresses to legitimate access points. Through access point monitoring, incident handlers can quickly identify and mitigate spoofed APs, thus preventing MitM attacks that exploit wireless networks by intercepting and manipulating communications.
References:Incident Handler (ECIH v3) courses and study materials discuss network security monitoring strategies, including the importance of monitoring access points to detect and prevent MitM attacks and other threats to wireless networks.

NEW QUESTION: 29
Logan, an incident handler, ensures the chain of custody is documented while handling backup media post- attack. The goal is to preserve evidence integrity while restoring critical systems. Which recovery principle is Logan adhering to?
A. Forensic compliance
B. Network segmentation
C. Immutable infrastructure
D. Enhanced authentication
Answer: A (LEAVE A REPLY)
The EC-Council Incident Handler (ECIH) curriculum stresses the importance of maintaining evidence integrity during recovery operations. Documenting the chain of custody ensures that evidence remains admissible in legal proceedings and maintains forensic validity. Chain of custody documentation tracks who handled the evidence, when it was accessed, how it was stored, and what actions were performed. This aligns directly with forensic compliance principles, which require proper evidence preservation, documentation, and controlled handling procedures.
While restoring systems, responders must ensure that backup media and affected systems are handled in a way that does not compromise evidence. ECIH emphasizes that recovery

should not destroy or contaminate forensic artifacts that may be required for legal, regulatory, or disciplinary action.
Option B (Network segmentation) relates to containment strategies. Option C (Immutable infrastructure) refers to architectural resilience models. Option D (Enhanced authentication) concerns access control, not evidence handling.
Therefore, Logan is adhering to forensic compliance principles during recovery.

NEW QUESTION: 30
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.
References:ECIH v3 courses and study guides elaborate on the vulnerability assessment process, detailing the steps involved in identifying, evaluating, and addressing security vulnerabilities within an organization's IT infrastructure.

NEW QUESTION: 31
Which of the following is an Inappropriate usage incident?
A. Access-control attack
B. Reconnaissance attack
C. Insider threat
D. Denial-of-service attack
Answer: (SHOW ANSWER)
An Inappropriate Usage incident refers to instances where computing resources are misused or abused, often violating organizational policies or laws. While access-control attacks, reconnaissance attacks, and denial-of- service (DoS) attacks represent different types of external threats or methods of attack, an Insider Threat is an example of inappropriate usage. Insider threats come from individuals within the organization, such as employees or contractors, who misuse their access to harm the organization's interests. This can include stealing confidential information, intentionally disrupting systems, or other malicious activities that leverage their legitimate access to the organization's resources.
References:EC-Council's Incident Handler (ECIH v3) materials often discuss various types of security incidents, including inappropriate usage, and emphasize the importance of recognizing and preparing for insider threats as a critical component of an organization's incident response strategy.

NEW QUESTION: 32
Malicious Micky has moved from the delivery stage to the exploitation stage of the kill chain. This malware wants to find and report to the command center any useful services

on the system. Which of the following recon attacks is the MOST LIKELY to provide this information?

A. IP range sweep

B. Packet sniffing

C. Session hijack

D. Port scan

Answer: (SHOW ANSWER)

When malware moves from the delivery stage to the exploitation stage in the cyber kill chain, its objective often shifts to identifying exploitable vulnerabilities within the targeted system. A port scan is a technique used to discover services that are listening on ports within a system. By scanning the system's ports, the malware can identify open ports and the services running on them, providing valuable information about potential entry points for further exploitation. This type of reconnaissance attack is aimed at gathering intelligence on the target system's network services, which can then be reported back to a command and control center for further malicious activity planning.

Port scanning is more relevant than IP range sweeps, packet sniffing, or session hijacking for identifying useful services on a system because it directly targets the discovery of accessible network services and their corresponding ports. While the other methods can also be part of the reconnaissance phase, they serve different purposes: IP range sweeps aim to identify active IP addresses, packet sniffing intercepts data packets to gather information, and session hijacking involves taking over a valid user session. In contrast, port scanning is specifically designed to enumerate services that could be exploited.

References:The ECIH v3 certification materials discuss various reconnaissance techniques used by attackers, including port scanning, as part of the exploitation stage of the kill chain. Understanding these techniques is crucial for incident handlers in identifying how attackers gather information and plan their attacks.

NEW QUESTION: 33

Michael is an incident handler at CyberTech Solutions. He is performing detection and analysis of a cloud security incident. He is analyzing the file systems, slack spaces, and metadata of the storage units to find hidden malware and evidence of malice.

Identify the cloud security incident handled by Michael.

A. Network-related incident

B. Storage-related incident

C. Application-related incident

D. Server-related incident

Answer: B (LEAVE A REPLY)

Michael's activities, which involve analyzing file systems, slack spaces, and metadata of storage units to find hidden malware and evidence of malice, indicate that he is handling a storage-related cloud security incident.

This type of incident pertains to unauthorized access, alteration, or exfiltration of data stored in cloud environments. By focusing on the storage aspects such as file systems and metadata, Michael is looking for signs of compromise that specifically affect the storage of data, which is indicative of a storage-related security incident in the cloud.
References:Incident Handler (ECIH v3) certification materials cover the various types of cloud security incidents, detailing how to detect and respond to them, including those related to storage where sensitive data might be targeted or compromised.

NEW QUESTION: 34
Otis is an incident handler working in Delmont organization. Recently, the organization is facing several setbacks in the business and thereby its revenues are going down. Otis was asked to take the charge and look into the matter. While auditing the enterprise security, he found the traces of an attack, where the proprietary information was stolen from the enterprise network and was passed onto the competitors.
Which of the following information security incidents Delmont organization faced?
A. Network and resource abuses
B. Unauthorized access
C. Espionage
D. Email-based abuse
Answer: C (LEAVE A REPLY)
The Delmont organization faced an espionage incident, which involves the unauthorized access and theft of proprietary or confidential information for passing it onto competitors or other external entities. Espionage is targeted at obtaining secrets or intellectual property to gain a competitive advantage or for other strategic purposes. Unlike network and resource abuses or email-based abuse, which might not specifically target sensitive information, espionage directly aims at stealing valuable data. Unauthorized access is a method that could be used in an espionage attempt but does not fully capture the motive of passing stolen information to competitors.
References:Incident Handler (ECIH v3) courses and study materials discuss various types of information security incidents, including espionage, highlighting its impact on businesses and strategies for detection and prevention.

NEW QUESTION: 35
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 SMB 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: 36
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.
References:While specific documentation from GPG18 and SPF might detail these principles, the ECIH v3 program by EC-Council covers the concept of forensic readiness planning, including adopting scenario-based approaches and learning from past incidents

as a fundamental aspect of enhancing an organization's incident response and forensic capabilities.

NEW QUESTION: 37
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: B (LEAVE A REPLY)
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: 38
During an internal audit following a surge in unauthorized financial transactions, a multinational investment firm's IR team uncovers evidence of an orchestrated campaign targeting senior staff. The attackers had pieced together fragments of sensitive data by mining executive digital footprints, reviewing online publications, and analyzing company-related mentions on external platforms. Later, they engaged directly with employees under fabricated personas, conducting scripted interviews to extract missing identifiers. With the assembled profile data, the adversaries submitted diversion requests for financial correspondence and used these to impersonate executives and execute fraudulent transfers. Forensic analysis revealed no signs of malware infection or system-level compromise. Which technique best aligns with the adversary's method of obtaining the initial sensitive information?

A. Phishing through spoofed emails embedded with malicious macros targeting employee laptops
B. Social engineering using open-source intelligence followed by pretexting
C. Pharming attack that redirected login traffic from internal systems to malicious replicas
D. Skimming magnetic card data through modified payment devices in the company cafeteria
Answer: B (LEAVE A REPLY)
The EC-Council Incident Handler (ECIH) curriculum classifies social engineering as a human-based attack technique that manipulates individuals into disclosing confidential information without exploiting technical vulnerabilities. In this scenario, the attackers first gathered publicly available information-also known as Open-Source Intelligence (OSINT)-by mining executive digital footprints, analyzing online publications, and reviewing external mentions. This reconnaissance phase aligns directly with OSINT-based profiling.
The adversaries then conducted scripted interviews under fabricated personas to extract additional identifiers.
This behavior is characteristic of pretexting, a specific social engineering technique where attackers create a false scenario to persuade victims to provide sensitive information.
ECIH explains that pretexting often involves impersonation and carefully constructed narratives to build credibility and trust.
The absence of malware infection or system-level compromise further confirms that this was not a technical exploit such as phishing with malicious macros (Option A) or pharming (Option C). Additionally, skimming (Option D) is a physical data theft technique unrelated to executive impersonation or digital profiling.
ECIH emphasizes that insider threat and financial fraud investigations frequently reveal social engineering campaigns leveraging OSINT, impersonation, and psychological manipulation rather than malware.
Preventive controls include executive awareness training, strict identity verification for financial change requests, multi-factor authentication, and callback verification procedures.
Therefore, the technique that best aligns with the adversary's method is social engineering using open-source intelligence followed by pretexting.

NEW QUESTION: 39
Stanley works as an incident responder at a top MNC based out of Singapore. He was asked to investigate a cybersecurity incident that recently occurred in the company.
While investigating the crime, he collected the evidence from the victim systems. He must present this evidence in a clear and comprehensible manner to the members of jury so that the evidence explains the facts clearly and further helps in obtaining an expert opinion on the same to confirm the investigation process.
In the above scenario, what is the characteristic of the digital evidence Stanley tried to preserve?
A. Believable

B. Complete
C. Authentic
D. Admissible
Answer: D (LEAVE A REPLY)
In the scenario described, Stanley aims to ensure that the digital evidence he collected is admissible in court.
This means the evidence must be gathered, handled, and presented in a manner that complies with legal standards, ensuring it can be legally used in a trial. Admissibility is a crucial characteristic of digital evidence, as it must be relevant, authentic, and obtained without violating any laws or rights to privacy. The evidence must also be presented in a clear and comprehensible manner to be understood by the members of the jury, which further supports its admissibility in court.
References:The Incident Handler (ECIH v3) certification materials cover the legal aspects of handling digital evidence, including the principles ensuring evidence is admissible in court.

NEW QUESTION: 40
Investigator Ian gives you a drive image to investigate. What type of analysis are you performing?
A. Real-time
B. Static
C. Dynamic
D. Live
Answer: (SHOW ANSWER)
When Investigator Ian gives you a drive image to investigate, the type of analysis you are performing is static analysis. Static analysis involves examining the contents of a drive, file, or binary without executing the system or the application. It's about analyzing the data at rest. This type of analysis is crucial for forensics investigations because it allows for the examination of files, directories, and system information without altering any state or data, thereby preserving the integrity of the evidence. Static analysis is contrasted with dynamic analysis, which involves analyzing a system in operation (real-time or live) or executing the application to observe its behavior.
References:Incident Handler (ECIH v3) courses and study guides highlight the importance of static analysis in digital forensics, detailing methods for examining disk images, files, and other digital artifacts to gather evidence without compromising its integrity.

NEW QUESTION: 41
A global bank's IH&R team is investigating an intricate cyber-espionage campaign. Advanced persistent threat (APT) actors exfiltrated sensitive financial data over several months using both software vulnerabilities and human errors. What is the MOST appropriate immediate action for the IH&R team?

A. Conduct organization-wide cybersecurity awareness training.
B. Publicize the breach to comply with laws.
C. Focus solely on patching known vulnerabilities.
D. Leverage an Incident Response Automation and Orchestration (IRAO) tool to correlate data and automate threat hunting.
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: 42
Joseph is an incident handling and response (IH&R) team lead in Toro Network Solutions Company. As a part of IH&R process, Joseph alerted the service providers, developers, and manufacturers about the affected resources.
Identify the stage of IH&R process Joseph is currently in.
A. Eradication
B. Containment
C. Incident triage
D. Recovery
Answer: B (LEAVE A REPLY)
When Joseph, the IH&R team lead, alerted service providers, developers, and manufacturers about the affected resources, he was engaged in the Containment stage of the Incident Handling and Response (IH&R) process. Containment involves taking steps to limit the spread or impact of an incident and to isolate affected systems to prevent further damage. Alerting relevant stakeholders, including service providers and developers, is part of containment efforts to ensure that the threat does not escalate and that measures are taken to protect unaffected resources. This stage precedes eradication and recovery, focusing on immediate response actions to secure the environment.
References:The ECIH v3 certification program outlines the IH&R process stages, explaining the roles and actions involved in containment, including communication with external and internal stakeholders to manage and mitigate the incident's effects.

NEW QUESTION: 43

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.

References:The Incident Handler (ECIH v3) certification program covers a variety of cyber attacks and techniques, including DNS poisoning and pharming, explaining how attackers exploit vulnerabilities to redirect users to fraudulent sites.

NEW QUESTION: 44

TechStream, a rising tech start-up, developed an AI-powered chatbot for its clients' websites. Shortly after deployment, users reported receiving malicious links and phishing messages from the chatbot. Preliminary investigation traced the issue to an attacker exploiting the chatbot's AI training module. Which of the following steps would be the most efficient in addressing this vulnerability?

A. Introducing CAPTCHA challenges before users can interact with the chatbot.

B. Implementing strict input validation for any data fed to the chatbot.

C. Disabling the chatbot until a complete security review is done.

D. Limiting the chatbot's ability to share links or external content.

Answer: (SHOW ANSWER)

The root cause of this incident is unvalidated input poisoning the AI training process, resulting in malicious output. ECIH web application security principles emphasize that input validation is the primary control against injection and manipulation attacks.

Option B is correct because strict validation ensures that malicious or untrusted data cannot influence training or response generation. This addresses the vulnerability at its source.

Option A adds friction but does not stop poisoning. Option C is disruptive and not efficient. Option D limits functionality without fixing the underlying issue.
ECIH stresses fixing vulnerabilities at the root rather than applying superficial controls, making Option B correct.

NEW QUESTION: 45
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. BeEf
B. IDAPro
C. Omnipeek
D. shARP
Answer: C (LEAVE A REPLY)
Omnipeek is a network analyzer tool that allows for the capture and analysis of data packets transmitted across a network. It is designed to provide deep insights into network traffic, enabling users to examine various aspects of the data packets, including network protocols, ports, devices, and potential issues in network transmission. This tool would be ideal for Chandler, who is targeting the Technote organization with the intent of intercepting and analyzing network traffic to obtain sensitive organizational information. Omnipeek's capabilities in packet analysis make it suitable for such activities, offering detailed visibility into the network's operation and data flows.
References:The ECIH v3 certification program includes discussions on network monitoring and analysis tools, including packet sniffers like Omnipeek, and their role in both cybersecurity defense and offensive activities like hacking.

NEW QUESTION: 46
AlphaTech 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?
A. Searching for IOCs related to known APT campaigns and comparing them with observed patterns.
B. Collaborating with industry peers to understand similar threats and observed TTPs.
C. Obtaining historical data on common cyber threats to predict future movements.
D. Gathering information from open-source forums and integrating it internally.
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: 47
A colleague wants to minimize their security responsibility because they are in a small organization. They are evaluating a new application that is offered in different forms. Which form would result in the least amount of responsibility for the colleague?
A. On-prom installation
B. saaS
C. laaS
D. PaaS
Answer: (SHOW ANSWER)
Software as a Service (SaaS) offers the least amount of security responsibility for the end-user or organization, as the service provider manages the underlying infrastructure, software maintenance, security patching, and updates. Choosing a SaaS application means the colleague's organization would not be responsible for the physical servers, operating systems, or the application's security configurations, making it the best option for minimizing their security responsibilities.
References:In the Certified Incident Handler (ECIH v3) course materials, the various cloud service models (IaaS, PaaS, SaaS) are discussed with a focus on their implications for security responsibilities and management.

NEW QUESTION: 48
Khai was tasked with examining the logs from a Linux email server. The server uses Sendmail to execute the command to send emailsand Syslog to maintain logs. To validate

the data within email headers, which of the following directories should Khai check for information such as source and destination IP addresses, dates, and timestamps?
A. /Var/log/mailog
B. /ar/log/sendmail
C. /va r/log/mai11og
D. /va r/log/sendmail/mailog
Answer: (SHOW ANSWER)
In a Linux environment, email servers such as Sendmail log events, including details about sent and received emails, in a specific log file. The correct directory and file for examining email logs, particularly for Sendmail and using Syslog for logging, is /Var/log/maillog. Thisfile contains vital information for forensic and incident response purposes, including source and destination IP addresses, email addresses, timestamps, and other data relevant to the email traffic handled by the server. By analyzing this log, incident responders can gather evidence related to email-based incidents, trace the source of malicious emails, and understand the scope of an incident. It's crucial for individuals like Khai, who are tasked with examining logs, to know the correct log file locations and their contents to effectively validate and analyze email header information and other relevant data.
References:Incident Handler (ECIH v3) study materials often cover the logging mechanisms of common services and applications on Linux systems, including email servers like Sendmail, and the importance of log files like /var/log/maillog in incident investigation and response activities.

NEW QUESTION: 49
After a recent cloud migration, AeroFlights, an airline company, spotted unauthorized data access.
Preliminary checks hinted at malware that used cloud resources to spread, impacting flight schedules.
Equipped with a cloud-specific security tool and a real-time scheduling monitor, what should be the primary action?
A. Temporarily halt all flight operations until the issue is resolved.
B. Deploy the cloud security tool to identify and counteract the malware.
C. Notify passengers about possible delays and offer compensation.
D. Monitor flight schedules in real-time to avoid potential disruptions.
Answer: B (LEAVE A REPLY)
This scenario involves an active cloud malware incident affecting operational systems. According to the ECIH cloud incident handling process, the priority after detection is containment and eradication using appropriate tooling. Cloud-specific security tools provide visibility into workloads, API activity, lateral movement, and malicious persistence mechanisms unique to cloud environments.

Option B is correct because deploying the cloud security tool enables identification of infected resources, malicious processes, compromised identities, and abnormal API usage. This allows responders to contain spread, remove malware, and restore integrity without unnecessary disruption.
Option A is an extreme business decision that could cause severe operational and financial damage and should only occur if safety is directly threatened. Option C is a communication step that must be based on verified impact. Option D is monitoring, not response.
ECIH emphasizes that incident response actions must be proportional, evidence-based, and targeted.
Leveraging cloud-native or cloud-aware security tools is the most effective primary response in such incidents, making Option B correct.

NEW QUESTION: 50
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.
Option A implies legitimate remote work within policy boundaries, which is contradicted by the unauthorized software installation. Option B suggests a third-party compromise, but logs indicate activity from an internal user account. Option D (DoS attack) involves service disruption via traffic flooding, which is not described here.
ECIH stresses enforcing acceptable use policies, monitoring user behavior, restricting unauthorized software installation, and applying least privilege controls to mitigate insider misuse. Therefore, this scenario best fits inappropriate usage due to policy violation and unauthorized software installation.

NEW QUESTION: 51
Emily, a member of the cybersecurity response team, receives an alert indicating suspicious login attempts on the company's internal HR portal. Upon inspection, she finds several failed login attempts from a foreign IP address targeting administrative accounts. Further investigation reveals that one of the accounts was compromised and its privileges were escalated. What indicator most strongly suggests this is an unauthorized access incident?
A. New system process creation
B. Log entries showing access to critical files
C. High CPU utilization
D. Suspicious DNS activity
Answer: B (LEAVE A REPLY)
The ECIH incident validation phase emphasizes the importance of direct evidence when confirming unauthorized access. Log entries that show access to sensitive or restricted files provide concrete proof that an attacker successfully breached controls.
Option B is correct because access logs tied to critical resources confirm both authentication success and unauthorized activity. Failed logins or system performance issues alone do not confirm compromise.
Option A, C, and D are indirect indicators that may signal suspicious behavior but cannot independently confirm unauthorized access.
Therefore, verified log evidence is the strongest indicator, aligning with ECIH incident triage and validation principles.

NEW QUESTION: 52
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.
References:The ECIH v3 certification materials discuss various data preprocessing techniques used in the analysis of cyber attacks, including the concept of sessionization to better understand user behavior and detect threats.

NEW QUESTION: 53
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: (SHOW ANSWER)
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.
Option A is unrelated. Option B may disrupt business operations prematurely. Option D (rebooting) does not address the attack and may temporarily relieve symptoms without mitigation.
ECIH emphasizes evidence preservation, traffic validation, and controlled response during DoS incidents.
Therefore, the first step is to inspect network traffic to confirm the attack pattern and verify source behavior.

NEW QUESTION: 54
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: (SHOW ANSWER)

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.

References:Incident Handler (ECIH v3) courses and study guides emphasize the importance of using digital forensic tools, such as BrowsingHistoryView, for analyzing web browser data during investigations.

NEW QUESTION: 55

DeltaCorp, a global e-commerce company, received an email sent to the financial department claiming to be from the CEO, requesting an urgent transfer of funds. To determine the legitimacy of this potentially deceptive email, which of the following should be the primary focus of the investigation?

A. Inspect the email headers for spoofing or sender IP irregularities.

B. Contact the vendor mentioned in the email.

C. Review past emails for similar language.

D. Scan the email server for malware.

Answer: A (LEAVE A REPLY)

ECIH email incident response guidance emphasizes email header analysis as the primary validation technique for suspected spoofing or impersonation attacks.

Option A is correct because headers reveal sender IPs, routing paths, and authentication results (SPF, DKIM, DMARC). This evidence directly confirms whether the email originated from a legitimate source.

Options B, C, and D are supplementary actions but do not provide authoritative validation.

NEW QUESTION: 56

In an online retail company, a severe security incident occurred where attackers exploited a zero-day vulnerability in the website's backend. This exploit allowed the theft of thousands of customers' credit card details. While the tech team races to patch the vulnerability, what should be the primary focus of the IH&R team?

A. Coordinating with financial institutions to monitor suspicious transactions.
B. Commencing legal actions against the attackers.
C. Immediately emailing all customers advising them to cancel cards.
D. Analyzing server logs using Incident Response Automation and Orchestration tools to understand the breach's origin.
Answer: D (LEAVE A REPLY)
In the ECIH Incident Handling lifecycle, once a breach is detected, the IH&R team must focus on analysis and scoping to understand how the attack occurred, what systems were affected, and whether the attacker still has access.
Option D is correct because analyzing logs with Incident Response Automation and Orchestration (IRAO) tools allows rapid correlation of events, identification of attacker entry points, and determination of breach scope. ECIH stresses that zero-day incidents require deep forensic and timeline analysis to ensure complete containment and prevent recurrence.
Options A and C are important but depend on accurate breach understanding. Option B is premature without full incident context.
Therefore, log analysis and origin tracing is the correct primary focus.

NEW QUESTION: 57
Which of the following has been used to evade IDS and IPS?
A. Fragmentation
B. TNP
C. HTTP
D. SNMP
Answer: (SHOW ANSWER)
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.
References:In its coverage of network security mechanisms and evasion techniques, the ECIH v3 certification details how attackers exploit vulnerabilities in the implementation of IDS and IPS systems, including the use of packet fragmentation.

NEW QUESTION: 58
An international logistics firm runs a smart hub where IT systems interface with warehouse automation for tasks like sorting, routing, and conveyor coordination via programmable units and dashboards. A recent cyberattack, initiated through a compromised third-party remote maintenance tunnel, disrupted communication between backend scheduling

applications and embedded automation units, leading to halted processing lines and shipment delays.
After isolating affected segments, removing malicious components, and restoring critical workflows, the recovery team begins validating the reinstated operations. While reviewing logs and configurations, they find excessive permissions granted between internal authentication servers and embedded automation modules.
They also detect anomalies in authentication tokens used to verify communications across system interfaces, including unidentified fingerprints not matching the original configuration. Which action should be prioritized as part of a secure restoration plan?
A. Apply new IDS signatures to detect malware variants targeting SCADA devices
B. Conduct red-team simulations to test OT segmentation defenses
C. Reboot all systems to verify stable firmware operation
D. Enforce granular role-based access policies across control systems and validate trusted device certificates
Answer: D (LEAVE A REPLY)
The EC-Council Incident Handler (ECIH) curriculum emphasizes that recovery must not only restore functionality but also eliminate residual security weaknesses that could enable reinfection or continued compromise. In operational technology (OT) and industrial environments, identity validation, certificate trust, and strict access control between interconnected systems are critical.
The scenario highlights two major issues: excessive permissions between authentication servers and automation modules, and anomalies in authentication tokens with unidentified fingerprints. These findings indicate compromised trust relationships and over-privileged system communications.
ECIH recovery guidance stresses revalidating authentication mechanisms, enforcing the Principle of Least Privilege, reviewing trust relationships, and ensuring certificate integrity before declaring systems fully restored. Implementing granular role-based access controls (RBAC) and validating trusted device certificates directly addresses both excessive permissions and authentication anomalies.
Option A improves detection but does not correct trust misconfigurations. Option B (red-team simulation) is useful but secondary to securing authentication controls. Option C (system reboot) does not resolve permission or certificate validation issues.
Therefore, enforcing granular role-based access policies and validating trusted device certificates is the most critical secure restoration action.

NEW QUESTION: 59
Which one of the following is Inappropriate Usage Incidents?
A. Access Control Attack
B. Reconnaissance Attack
C. Denial of Service Attack
D. Insider Threat

Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
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)
Explanation (preparation phase):
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 .

NEW QUESTION: 61
Ethan, an incident handler, reviews traffic logs showing abnormal connections from internal devices to high- risk external domains. He traces these back to a misconfigured IoT device using outdated firmware. What kind of indicator was key in identifying the issue?
A. Large ICMP payloads
B. Unauthorized ARP broadcast
C. Suspicious outbound connections
D. Incorrect DNS caching
Answer: C (LEAVE A REPLY)
The primary indicator here is suspicious outbound connections, a key detection category in ECIH network incident analysis. Unexpected communications to known high-risk domains often indicate malware, misconfiguration, or compromise.

Option C is correct because outbound traffic patterns revealed the issue. ECIH highlights that IoT devices frequently lack visibility and controls, making outbound monitoring critical. Options A, B, and D do not reflect the described behavior.
Monitoring outbound traffic is therefore essential for early detection of compromised or misconfigured devices.

NEW QUESTION: 62
Which of the following terms refers to an organization's ability to make optimal use of digital evidence in a limited period of time and with minimal investigation costs?
A. Threat assessment
B. Data analysis
C. Risk assessment
D. Forensic readiness
Answer: D (LEAVE A REPLY)
Forensic readiness refers to an organization's ability to maximize its capability to use digital evidence effectively in an investigation, while minimizing the cost of an investigation and disruption to its operations.
It involves having policies, procedures, and technologies in place to collect, preserve, and analyze digital evidence efficiently, so when an incident occurs, the organization is prepared to handle it quickly and with minimal costs. Forensic readiness not only helps in reducing the time and resources spent on investigations but also ensures that the evidence is reliable and can be used in legal proceedings if necessary.
References:The concept of forensic readiness is part of the Incident Handler (ECIH v3) curriculum, emphasizing the strategic importance of preparing for incidents in advance, including the preservation of evidence and the ability to conduct effective and efficient investigations.

NEW QUESTION: 63
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: A (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.

References:The ECIH v3 courses and study guides emphasize the importance of collecting volatile data during incident response and digital forensics investigations. They specifically highlight the use of built-in Windows tools like WMIC for gathering essential system information without compromising the integrity of the evidence.

NEW QUESTION: 64

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

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

A. Evidence gathering and forensics analysis

B. Eradication

C. Notification

D. Recovery

Answer: D (LEAVE A REPLY)

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

before being brought back online. This step is crucial for resuming business operations and mitigating the impact of the incident.

NEW QUESTION: 65
Ren is assigned to handle a security incident of an organization. He is tasked with forensics investigation to find the evidence needed by the management. Which of the following steps falls under the investigation phase of the computer forensics investigation process?
A. Secure the evidence
B. Risk assessment
C. Setup a computer forensics lab
D. Evidence assessment
Answer: (SHOW ANSWER)
Evidence assessment is a critical step in the investigation phase of the computer forensics process. This step involves evaluating the evidence collected to determine its relevance and significance to the case at hand. It includes analyzing the secured data to identify what information can be used as evidence, its integrity, and how it can be related to the security incident. This phase is pivotal as it helps in building a coherent understanding of the incident and in establishing facts that can be presented in management reports or legal proceedings.
References:The Certified Incident Handler (ECIH v3) by EC-Council includes a comprehensive discussion on the computer forensics investigation process, detailing steps from securing evidence to analyzing and assessing it within the context of an investigation.

NEW QUESTION: 66
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: B (LEAVE A REPLY)
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. References:Incident Handler (ECIH v3) courses and study guides emphasize the role of the Incident Manager as integral to the incident handling process, underscoring their importance in bridging the gap between technical response actions and strategic management decisions.

NEW QUESTION: 67
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: (SHOW ANSWER)
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.
References:ECIH v3 courses and study guides often include discussions on various attack vectors used by cybercriminals, including email-based threats and their impact on organizational security.

NEW QUESTION: 68
You are a systems administrator for a company. You are accessing your file server remotely for maintenance.
Suddenly, you are unable to access the server. After contacting others in your department, you find out that they cannot access the file server either. You can ping the file server but not connect to it via RDP. You check the Active Directory Server, and all is well. You check the email server and find that emails are sent and received normally. What is the most likely issue?
A. An e-mail service issue
B. The file server has shut down
C. A denial-of-service issue
D. An admin account issue

Answer: C (LEAVE A REPLY)
In this scenario, the inability to access the file server via Remote Desktop Protocol (RDP), despite the server being pingable and other services functioning normally, suggests a service-specific disruption rather than a complete system shutdown or broader network issue. This pattern is indicative of a denial-of-service (DoS) attack targeted at the file server's RDP service or network congestion that specifically affects RDP connectivity. A DoS attack aims to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. The fact that other services (like email) are operational rules out broader system or admin account issues, pointing towards a specific problem with accessing the file server, most likely due to a denial-of-service condition.
References:Incident Handler (ECIH v3) courses teach systems administrators and security professionals to diagnose and respond to various security incidents, including DoS attacks, by understanding symptoms and isolating issues based on the services affected.

NEW QUESTION: 69
A large retail company recently migrated its customer data to a public cloud service. Shortly after, they noticed suspicious activities indicating a potential data breach. The incident response team faces multiple challenges due to the cloud's shared responsibility model, including limited access to underlying infrastructure and logs. Which action is most critical for the incident response team to perform first?
A. Request immediate access to all infrastructure logs from the cloud service provider.
B. Begin an internal audit of all cloud service configurations and permissions.
C. Notify customers about the potential data breach to comply with data protection regulations.
D. Isolate affected systems by modifying cloud security group settings.
Answer: (SHOW ANSWER)
ECIH cloud incident handling guidance emphasizes that containment must be immediate and within the organization's control. Modifying cloud security groups allows responders to restrict network access instantly, preventing further data exfiltration.
Option D is correct because it is actionable without CSP dependency and directly limits attacker movement.
Option A may take time. Option B is investigative. Option C is regulatory and premature. Containment through security group modification is therefore the most critical first step.

NEW QUESTION: 70
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: B (LEAVE A REPLY)
In the ECIH email incident response framework, eradication extends beyond internal cleanup and includes threat intelligence sharing. Option B is correct because sharing phishing indicators with trusted security communities helps disrupt attacker infrastructure and prevents reuse of the same campaign against other organizations.
Option A is unrelated. Option C is ineffective against phishing. Option D is overly destructive and unnecessary.
ECIH promotes collaborative defense as part of post-detection eradication and prevention.

NEW QUESTION: 71
Alice is a disgruntled employee. She decided to acquire critical information from her organization for financial benefit. To acccomplish this, Alice started running a virtual machine on the same physical host as her victim's virtual machine and took advantage of shared physical resources (processor cache) to steal data (cryptographic key/plain text secrets) from the victim machine. Identify the type of attack Alice is performing in the above scenario.
A. Side channel attack
B. Service hijacking
C. SQL injection attack
D. Man-in-the-cloud attack
Answer: A (LEAVE A REPLY)
A side channel attack, as described in the scenario, involves an attacker using indirect methods to gather information from a system. In this case, Alice is exploiting the shared physical resources, specifically the processor cache, of a virtual machine host to steal data from another virtual machine on the same host. This type of attack does not directly breach the system through conventional means like breaking encryption but instead takes advantage of the information leaked by the physical implementation of the system, such as timing information, power consumption, electromagnetic leaks, or, as in this case, shared resource utilization, to infer the secret data.
References:The EC-Council's Certified Incident Handler (ECIH v3) program covers various types of cyber attacks, including advanced techniques like side channel attacks, highlighting the need for comprehensive security strategies that consider both direct and indirect attack vectors.

NEW QUESTION: 72

Which of the following is NOT a network forensic tool?
A. Capsa Network Analyzer
B. Tcpdurnp
C. Advancec NTFS Journaling Parser
D. Wireshark
Answer: C (LEAVE A REPLY)
Network forensic tools are designed to capture, record, and analyze network traffic. Tools like Capsa Network Analyzer, Tcpdump, and Wireshark are specifically designed for this purpose, providing capabilities to capture live traffic, analyze packets, and understand network activities. Capsa Network Analyzer is a comprehensive network monitoring tool, Tcpdump is a powerful command-line packet analyzer, and Wireshark is a widely used network protocol analyzer that provides detailed information about network traffic.
Advanced NTFS Journaling Parser, on the other hand, is not a network forensic tool but a tool used for forensic analysis of NTFS file systems. It parses the NTFS journal ($LogFile), which contains a log of changes made to files on an NTFS volume. This tool is valuable for forensic analysts who are investigating the file system activities on a Windows system, such as file creation, modification, and deletion times, rather than analyzing network traffic. Therefore, it does not fit the category of a network forensic tool.
References:The ECIH v3 curriculum from EC-Council covers a range of tools useful for incident handlers and forensic analysts, distinguishing between network forensic tools and those used for other types of forensic analysis, such as file system investigation.

NEW QUESTION: 73
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: C (LEAVE A REPLY)
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.
References:Incident Handler (ECIH v3) certification materials discuss APTs in detail, including their methodologies, objectives, and the importance of comprehensive security strategies to detect and mitigate such threats.

NEW QUESTION: 74
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: C (LEAVE A REPLY)
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.
References:The ECIH v3 course details various forms of malware, including Trojans, their modes of operation, and their impact on information security. Understanding the nature of these threats is crucial for effective incident handling and response.

NEW QUESTION: 75
Miko was hired as an incident handler in XYZ company. His first task was to identify the PING sweep attempts inside the network. For this purpose, he used Wireshark to analyze the traffic. What filter did he use to identify ICMP ping sweep attempts?
A. tcp.typc == icmp
B. icrrip.lype == icmp
C. icmp.type == 8 or icmp.type ==0
D. udp.lype - 7
Answer: C (LEAVE A REPLY)
In Wireshark, to identify ICMP ping sweep attempts, the filtericmp.type == 8 or icmp.type ==0is used. This filter captures ICMP echo requests and echo replies, which are indicative of ping commands. Type 8 represents an echo request used when a source sends a ping,

and type 0 represents an echo reply, which is the response from the target. By filtering for these ICMP types, Miko can detect a surge in ping requests across the network, which could indicate a ping sweep attempt-an exploratory activity often used by attackers to discover active hosts on a network by sending ping requests to multiple addresses.
References:Incident Handler (ECIH v3) courses and study guides often incorporate training on using network analysis tools like Wireshark, including how to use filters to detect specific types of network activities and potential threats.

NEW QUESTION: 76
Alex is an incident handler for Tech-o-Tech Inc. and is tasked to identify any possible insider threats within his organization. Which of the following insider threat detection techniques can be used by Alex to detect insider threats based on the behavior of a suspicious employee, both individually and in a group?
A. behaviorial analysis
B. Physical detection
C. Profiling
D. Mole detection
Answer: C (LEAVE A REPLY)
Behavioral analysis is a technique used to detect insider threats by analyzing the behavior of employees, both individually and in group settings, to identify any actions that deviate from the norm. This method relies on monitoring and analyzing data related to user activities, access patterns, and other behaviors that could indicate malicious intent or a potential security risk from within the organization. Behavioral analysis can detect unusual access to sensitive data, abnormal data transfer activities, and other indicators of insider threats. This approach is proactive and can help in identifying potential insider threats before they result in significant harm to the organization.
References:The Incident Handler (ECIH v3) certification materials cover various insider threat detection techniques, including the importance of behavioral analysis as a key method for identifying potential security risks posed by insiders.

NEW QUESTION: 77

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: (SHOW ANSWER)

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: 78

A US Federal Agency network was the target of a DoS attack that prevented and impaired the normal authorized functionality of the networks. According to agency's reporting timeframe guidelines, this incident should be reported within 2 h of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity.

Which incident category of US Federal Agency does this incident belong to?

A. CAT 6

B. CAT 2

C. CAT 1

D. CAT 5

Answer: (SHOW ANSWER)

In the context of US Federal Agencies, incidents are categorized based on their impact on operations, assets, or individuals. A DoS attack that prevents or impairs the authorized functionality of networks and is still ongoing without successful mitigation efforts typically falls under Category 2 (CAT 2). This category is designated for incidents that have a significant impact, requiring immediate reporting and response. The reporting timeframe of

within 2 hours as mentioned aligns with the urgency associated with CAT 2 incidents, emphasizing the need for swift action to address the attack and restore normal operations.
References:US Federal incident response guidelines and the Incident Handler (ECIH v3) courses outline the categorization of cybersecurity incidents, detailing the response protocols for each category, including the reporting timeframes.

NEW QUESTION: 79
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.
References:The Incident Handler (ECIH v3) courses and study guides often emphasize the importance of a Defense-in-depth strategy in creating robust security infrastructures to protect against a wide range of cyber threats.

NEW QUESTION: 80
In the lead-up to a major product launch, a technology company reviews its endpoint security strategy to safeguard intellectual property. What is the most essential element to incorporate into their incident response strategy for endpoints?
A. An employee training program focused on phishing defense
B. A dedicated crisis management team
C. A robust endpoint detection and response (EDR) system with automated response
D. Comprehensive encryption strategies for data at rest and in transit

Answer: (SHOW ANSWER)
The ECIH Endpoint Security module identifies EDR systems as the cornerstone of modern endpoint incident response. Advanced attacks targeting intellectual property often bypass traditional antivirus controls.
Option C is correct because EDR provides continuous monitoring, behavioral detection, rapid containment, and automated response across endpoints. This capability is critical during high-risk periods such as product launches.
Options A, B, and D are important but insufficient alone for real-time detection and response.
Therefore, deploying a robust EDR system is essential.

NEW QUESTION: 81
During a routine security audit, an executive's mobile device began exhibiting signs of compromise, including frequent crashes, unrecognized applications, and abnormal data consumption. The organization's IR team conducted multiple antivirus scans and attempted standard malware removal procedures, but the threat continued to persist. Further investigation suggested that the malware was embedded in a background service configured to reinitialize upon reboot. Concerned about the potential risk of data exfiltration or further infection, the team decided to isolate the device and initiate a tailored eradication strategy to remove the threat without activating it. Which eradication step is most appropriate in this situation?
A. Switch the phone to emergency or safe mode before cleanup
B. Enable lost device tracking to monitor further incidents
C. Revoke unnecessary cloud permissions for affected users
D. Perform full network scans to trace lateral movement
Answer: A (LEAVE A REPLY)
The EC-Council Incident Handler (ECIH) curriculum explains that certain advanced mobile malware strains embed themselves as background services configured to restart automatically upon reboot. In such cases, traditional antivirus scans may fail to fully remove the threat because the malicious service remains active.
Switching the mobile device to safe mode (or emergency mode) prevents third-party applications and background services from automatically launching during startup. This isolates the malicious process and prevents it from reinitializing, allowing responders to perform forensic analysis and removal without triggering additional payload execution or data exfiltration.
ECIH emphasizes that during malware eradication, responders must prevent the malware from executing while conducting cleanup procedures. Safe mode supports controlled analysis and minimizes risk during remediation.
Option B (lost device tracking) is a monitoring measure, not an eradication technique.
Option C (revoking cloud permissions) is relevant to access control but does not remove

embedded malware. Option D (network scans) supports broader investigation but does not directly eliminate the persistent mobile threat.
ECIH guidance for malware eradication includes isolating infected devices, disabling malicious processes, applying clean firmware or OS reinstallation if necessary, and ensuring persistence mechanisms are removed.
Therefore, switching the phone to safe mode before cleanup is the most appropriate eradication step.

NEW QUESTION: 82
SevTech detected malicious code injected into its client data protection module, with indicators of a nation- state actor. In this high-pressure scenario, what should be SevTech's primary course of action?
A. Coordinate discreetly with governmental cyber units to gather intelligence.
B. Notify all clients and suggest immediate disconnection.
C. Immediately patch the discovered vulnerability and roll out updates without informing clients.
D. Execute a counter-hack to identify the attacker.
Answer: C (LEAVE A REPLY)
According to the ECIH Risk Assessment and Recovery module, neutralizing the vulnerability is the top priority during active exploitation, even in nation-state scenarios. Option C is correct because immediately patching and deploying updates removes the attacker's access vector and prevents further compromise. ECIH discourages counter-hacking and premature disclosure without containment.
Options A and B may follow after stabilization. Option D is illegal and prohibited.
Therefore, rapid patching is the correct primary action.

NEW QUESTION: 83
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: A (LEAVE A REPLY)
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.
References:ECIH v3 certification materials often cover software testing techniques, including fuzz testing, to identify vulnerabilities in applications by inputting unexpected or random data.

NEW QUESTION: 84
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: (SHOW ANSWER)
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: 85
Francis is an incident handler and security expert. He works at MorisonTech Solutions based in Sydney, Australia. He was assigned a task to detect phishing/spam mails for the client organization.
Which of the following tools can assist Francis to perform the required task?
A. Netcraft
B. Nessus
C. BTCrack
D. Cain and Abel

Answer: A (LEAVE A REPLY)
Netcraft is a tool that provides internet security services, including the detection of phishing and spam emails.
It offers a range of services that can help organizations identify fraudulent websites and phishing activities by analyzing web content and email messages for known phishing signatures and heuristics. This makes it a useful tool for incident handlers like Francis, who is tasked with detecting phishing and spam emails for client organizations. Other options listed, such as Nessus (a vulnerability scanner), BTCrack (a Bluetooth pin and link-key cracker), and Cain and Abel (a password recovery tool), do not specialize in detecting phishing or spam emails but serve different purposes in cybersecurity.
References:The Incident Handler (ECIH v3) curriculum includes discussions on tools and methodologies for detecting and mitigating various cyber threats, including phishing and spam, highlighting tools like Netcraft for their utility in these areas.

NEW QUESTION: 86
Tibson works as an incident responder for MNC based in Singapore. He is investigating a web application security incident recently faced by the company. The attack is performed on a MS SQL Server hosted by the company. In the detection and analysis phase, he used regular expressions to analyze and detect SQL meta-characters that led to SQL injection attack.
Identify the regular expression used by Tibson to detect SQL injection attack on MS SQL Server.
A. /exec(\s|\+)+(s|x)p\w+/ix
B. ((\.\.\\)|(\.\.\/))
C. ((\.|%2E)(\.|%2E)(\/|%2F|\\|%5C))
D. ((\%3C)|<)((\%2F)|\/)*(script)((\%3E)|>)
Answer: (SHOW ANSWER)
The regular expression/exec(\s|\+)+(s|x)p\w+/ixis designed to match patterns that resemble SQL injection attempts, specifically targeting MS SQL Server. This expression looks for the use of theexeccommand followed by one or more spaces or plus signs, and then patterns that start withsporxp, which are prefixes commonly used in SQL Server stored procedures and extended stored procedures. These are often targeted in SQL injection attacks to execute malicious SQL statements. The regular expression provided is a tool used by incident responders like Tibson to identify and analyze potential SQL injection attempts by looking for suspicious patterns in SQL queries.

NEW QUESTION: 87
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 filtertcp.flags==0X029, Rose can detect packets that have these specific flags set, indicating a potential TCP Xmas scan attempt.

References:The technique of using Wireshark to detect specific types of scans, including the TCP Xmas scan, is covered in cybersecurity training materials and documentation related to network analysis and incident handling, such as those associated with the ECIH certification.

NEW QUESTION: 88

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: (SHOW ANSWER)

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.

References:The ECIH v3 course materials include discussions on risk management processes, outlining the importance of risk assessment in identifying and preparing for potential security threats.

NEW QUESTION: 89

Which of the following is a standard framework that provides recommendations for implementing information security controls for organizations that initiate, implement, or maintain information security management systems (ISMSs)?
A. ISO/IEC 27002
B. ISO/IEC 27035
C. PCI DSS
D. RFC 219G
Answer: A (LEAVE A REPLY)
ISO/IEC 27002 is a standard that provides best practice recommendations on information security controls for use by those responsible for initiating, implementing, or maintaining information security management systems (ISMSs). It covers areas such as risk assessment, human resource security, operational security, and communications security, among others, providing a framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS. ISO/IEC 27035 pertains to information security incident management, PCI DSS (Payment Card Industry Data Security Standard) deals with the security of cardholder data, and RFC 2196 is a guide for computer security incident response teams (CSIRTs), not a standard for implementing ISMSs.
References:The ECIH v3 curriculum includes the study of various standards and frameworks that support information security management and governance, including ISO/IEC 27002, highlighting its role in guiding organizations in implementing effective security controls.

NEW QUESTION: 90
Zoe, a security analyst, deploys a high-interaction honeypot in the DMZ that mimics critical systems and monitors logs for scans, exploit attempts, and lateral movement techniques. What is the main purpose of Zoe' s activity?
A. Deceiving attackers to study their behavior.
B. Preventing malware execution using sandboxing.
C. Blocking DDoS traffic through ACL rules.
D. Testing the organization's backup and recovery systems.
Answer: A (LEAVE A REPLY)
Explanation (aligned to threat intelligence & detection):
A high-interaction honeypot is designed to attract and engage adversaries, providing realistic services so defenders can observe tactics, techniques, and procedures (TTPs) with higher fidelity than a low-interaction decoy. The goal is not to "stop" attacks directly, but to detect and learn: identify scanning patterns, credential stuffing attempts, exploit chains, payload delivery methods, and post-exploitation behaviors such as enumeration and lateral movement. That intelligence is then used to improve controls-signatures, detections, segmentation, and hardening priorities.
Sandboxing (B) is typically about detonating suspicious files/URLs to observe behavior in a controlled environment; it's not what a DMZ honeypot primarily does. ACL rules and DDoS

blocking (C) are traffic filtering measures, not deception telemetry. Backup/recovery testing (D) is resilience planning, unrelated to studying attacker behavior in real-time.
In incident handling terms, honeypots support the "preparation" and "detection" posture-expanding visibility, generating early warning, and enriching threat intelligence. They can also reduce risk by luring opportunistic attackers away from production assets, but their primary value is behavioral observation and evidence collection.

NEW QUESTION: 91
Sam received an alert through an email monitoring tool indicating that their company was targeted by a phishing attack. After analyzing the incident, Sam identified that most of the targets of the attack are high-profile executives of the company. What type of phishing attack is this?
A. Pharming
B. Whaling
C. Puddle phishing
D. Spear phishing
Answer: (SHOW ANSWER)
Whaling is a specific type of phishing attack that targets high-profile executives or individuals within an organization, often with the intent to steal sensitive information or gain access to their accounts for financial fraud. The term "whaling" is used because it targets the "big fish" of an organization. Given that Sam identified the targets of the attack as high-profile executives, the described scenario is indicative of a whaling attack.
References:The ECIH v3 curriculum includes a section on different types of phishing attacks, including whaling, emphasizing the strategies attackers use to target individuals based on their roles within an organization.

NEW QUESTION: 92
SWA Cloud Services added PKI as one of their cloud security controls. What does PKI stand for?
A. Private key infrastructure
B. Private key in for ma lion
C. Public key information

D. Public key infrastructure

Answer: (SHOW ANSWER)

Public Key Infrastructure (PKI) is a framework used to manage digital certificates and public-key encryption.

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

References:The ECIH v3 program covers the importance of PKI in cloud security controls, emphasizing its role in establishing and maintaining a secure cloud computing environment.

NEW QUESTION: 93

In an international bank, the IT security team identified unusual network traffic indicating a potential malware infection. Further analysis revealed that several high-value transaction servers were communicating with an external command and control server. The team needs to decide the immediate action to best handle this malware incident triage. What should they prioritize to mitigate the threat and safeguard sensitive data effectively?

A. Disconnecting the affected servers from the network to prevent further data exfiltration

B. Initiating a controlled shutdown of the transaction servers to preserve their current state

C. Immediately updating antivirus signatures on all network devices and servers

D. Performing a memory dump of the affected servers for in-depth forensic analysis

Answer: A (LEAVE A REPLY)

This scenario describes an active malware infection with confirmed command-and-control (C2) communication, which represents an immediate and severe risk to sensitive financial data. According to the EC-Council ECIH malware incident handling process, the first priority in such cases is containment, specifically stopping ongoing malicious activity and preventing further data exfiltration.

Option A is correct because disconnecting the affected servers from the network immediately severs the attacker's control channel and halts outbound data leakage. ECIH emphasizes that when C2 traffic is observed, responders must act decisively to isolate compromised systems before pursuing deeper forensic analysis or remediation. Containment minimizes damage and reduces legal, financial, and reputational impact.

Option B may preserve system state but allows continued exfiltration until shutdown is complete and may disrupt critical banking operations. Option C is a preventive measure and does not stop an active infection.

Option D is valuable for investigation but should occur after containment, not before. ECIH guidance consistently prioritizes stopping harm over gathering evidence when critical assets are at risk.

Therefore, immediate network disconnection of affected servers is the correct triage action.

NEW QUESTION: 94
A mid-sized tech company leveraging a cloud-based infrastructure noticed unauthorized interactions between cloud-hosted applications. Upon investigation, the security team discovered confusion over whether internal teams or the cloud provider were tasked with overseeing certain services, which caused delays in the incident response. Which action would best support managing this cloud security incident?
A. Performing regular vulnerability scans on container images
B. Assigning all incident response tasks to external cloud support teams
C. Understanding shared responsibilities for incident response in cloud environments
D. Disabling automatic scaling features to prevent service misuse
Answer: (SHOW ANSWER)
The EC-Council Incident Handler (ECIH) curriculum highlights the Shared Responsibility Model in cloud environments. Cloud providers are responsible for security of the cloud (infrastructure), while customers are responsible for security in the cloud (applications, data, access control).
Confusion over responsibility leads to delayed incident response, misconfigurations, and security gaps. ECIH emphasizes clearly defining roles between cloud providers and internal teams before incidents occur, including logging, monitoring, access management, and incident handling responsibilities.
Option A improves security posture but does not resolve responsibility confusion. Option B improperly shifts all responsibility to the provider, which contradicts the shared model. Option D relates to operational configuration, not governance clarity.
Therefore, understanding shared responsibilities for incident response in cloud environments is critical to effectively managing cloud security incidents.

NEW QUESTION: 95
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 critical cloud assets.
B. Focus on physical security measures at company offices.
C. Centralize logging and monitoring across all cloud services for improved visibility and anomaly detection.
D. Implement a single cloud service provider strategy.
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: 96
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.
References:The importance of the preparation phase in the incident response lifecycle is emphasized in various cybersecurity frameworks and guidelines, including those covered in ECIH v3 certification materials, which detail the roles, responsibilities, and planning necessary to establish an effective incident response capability.

NEW QUESTION: 97
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: (SHOW ANSWER)
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: 98
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: (SHOW ANSWER)
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: 99
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. Enable remote location tracking for corporate Android devices
B. Restrict Bluetooth and NFC-based application communication channels
C. Acquire full-disk encryption for both device storage and application data
D. Enforce MDM policies that allow only signed app installations
Answer: D (LEAVE A REPLY)
The EC-Council Incident Handler (ECIH) curriculum stresses that mobile malware often enters enterprise environments through sideloaded applications obtained from untrusted sources. Android devices that allow installation from unknown sources significantly increase organizational risk.
Mobile Device Management (MDM) solutions are recommended to enforce application control policies, including restricting installations to digitally signed applications from approved app stores. By enforcing signed app installation policies, organizations prevent the execution of tampered or malicious APK files.
Option A (remote tracking) assists with lost device recovery but does not prevent malicious installations.

Option B (Bluetooth/NFC restriction) addresses wireless communication risks, not app integrity. Option C (full-disk encryption) protects stored data but does not stop malware from executing.
ECIH guidance highlights enforcing mobile security baselines, restricting unknown sources, implementing application whitelisting, and applying MDM-enforced controls to prevent sideloaded malware infections.
Therefore, enforcing MDM policies that allow only signed app installations is the most effective preventive control.

NEW QUESTION: 100
Drake is an incident handler in Dark CLoud 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: 101
Sameer, part of the incident response team, is alerted that several employees unknowingly entered credentials on a fake login page after receiving a spoofed internal notification. The domain name used in the attack had subtle character changes. What kind of unauthorized access incident did this attack begin with?
A. DNS footprinting
B. Port scanning
C. Social engineering
D. ARP spoofing
Answer: C (LEAVE A REPLY)
The ECIH Introduction to Incident Handling module identifies social engineering as a primary method attackers use to gain unauthorized access without exploiting technical vulnerabilities.

Option C is correct because the attack relied on deception-spoofed notifications and lookalike domains-to trick users into disclosing credentials. This is a classic social engineering technique, often used as the initial access vector.
Options A, B, and D are technical reconnaissance or network attacks, not human-focused deception.
Recognizing social engineering as the root cause is essential for selecting appropriate remediation actions such as user awareness training, phishing defenses, and MFA, all emphasized in ECIH guidance.

NEW QUESTION: 102
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.
Option A (Recovery) focuses on restoring systems after containment and eradication. Option C (Eradication) involves removing threats after containment. Option D (Triage) falls under detection and analysis. None of these address proactive readiness and organizational resilience.
Therefore, initiating the Preparation phase is the correct approach to strengthen long-term cybersecurity resilience in alignment with ECIH standards.

NEW QUESTION: 103
After a recent upgrade, users of Trend Spot encountered slow website load times. Analysis revealed attackers flooding the application with fake search requests, causing an application-layer DoS attack. How should Trend Spot primarily respond?
A. Regularly clear the server cache.
B. Shift to a more robust hosting provider.
C. Introduce rate limiting on search request functionality.
D. Implement IP address-based blocking for suspicious traffic.
Answer: C (LEAVE A REPLY)
This incident represents an application-layer DoS attack, which targets specific functions rather than bandwidth. ECIH emphasizes function-level protection in such scenarios.
Option C is correct because rate limiting restricts abusive request frequency while allowing legitimate usage.
It directly addresses the exploited feature without disrupting service availability.
Option D may block legitimate users behind shared IPs. Options A and B do not mitigate the attack vector.
Rate limiting aligns with ECIH guidance for preserving availability during Layer 7 attacks.

NEW QUESTION: 104
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.
References:While specific documentation from GPG18 and SPF might detail these principles, the ECIH v3 program by EC-Council covers the concept of forensic readiness planning, including adopting scenario-based approaches and learning from past incidents as a fundamental aspect of enhancing an organization's incident response and forensic capabilities.

NEW QUESTION: 105
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: 106
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.
References:The concept of disassociation attacks and their impact on wireless network connectivity is covered in cybersecurity training materials and incident response courses, including those related to the ECIH v3 certification. These materials explain the techniques used in various network attacks, including how disassociation attacks are performed and mitigated.

NEW QUESTION: 107
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).
References:The Incident Handler (ECIH v3) courses and study guides discuss different types of insider threats, emphasizing the importance of security awareness training to mitigate the risks associated with negligent insiders.

NEW QUESTION: 108
Mei, a forensic analyst, is analyzing logs from a compromised blog platform. She finds evidence that an attacker posted content using a valid account, and later, users who visited the blog were redirected to a phishing site containing session cookies in the URL. What kind of attack does this best describe?
A. Reflected XSS
B. Man-in-the-middle attack
C. Stored XSS
D. Directory traversal
Answer: C (LEAVE A REPLY)
The EC-Council Incident Handler (ECIH) curriculum explains that Stored Cross-Site Scripting (Stored XSS) occurs when malicious scripts are permanently stored on a web server (e.g., within blog posts, comments, or database entries). When users access the infected content, the malicious script executes in their browser.
In this scenario, the attacker posted malicious content using a valid account, and subsequent users were redirected to a phishing site containing session cookies in the URL. This indicates that malicious code was embedded and stored within the blog platform, affecting multiple visitors.
Reflected XSS (Option A) requires the victim to click a crafted link and is not persistently stored. Man-in-the- middle (Option B) involves interception of communications. Directory traversal (Option D) involves accessing restricted directories on a server.
ECIH highlights that stored XSS attacks are particularly dangerous because they impact all users who access the compromised content and can lead to session hijacking, credential theft, and redirection to phishing sites.
Therefore, the attack described is Stored XSS.

NEW QUESTION: 109

Which stage of the incident response and handling process involves auditing the system and network log files?

A. Containment

B. Incident triage

C. Incident disclosure

D. Incident eradication

Answer: B (LEAVE A REPLY)

Auditing the system and network log files is a crucial step in the incident triage phase of the incident response and handling process. During incident triage, incident handlers assess and prioritize incidents based on their severity, impact, and the urgency of the response required. Part of this assessment involves reviewing log files to understand the nature of the incident, its scope, and the systems or networks affected. This information helps in categorizing the incident and deciding on the appropriate response actions. Unlike containment, which aims to limit the damage, incident disclosure, which involves communicating about the incident, or incident eradication, which focuses on removing the threat, incident triage is about evaluating and prioritizing the incident based on detailed log analysis among other factors.

References:The Incident Handler (ECIH v3) courses and study guides emphasize the role of incident triage in the early stages of the incident response process, highlighting the importance of log file analysis in assessing and prioritizing incidents.

NEW QUESTION: 110

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.

References:The OWASP Top 10 is a widely recognized standard for web application security, often referenced in cybersecurity training and certifications, including the EC-

Council's Incident Handler (ECIH v3) curriculum, which covers identification and mitigation of various web application vulnerabilities, including broken authentication.

NEW QUESTION: 111
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.
References:The concept and techniques of synthetic identity theft are covered in detail in the Incident Handler (ECIH v3) curriculum, where the focus is on identifying, understanding, and mitigating various forms of identity theft, including synthetic identity theft, as part of incident response activities.

NEW QUESTION: 112
Which of the following is the BEST method to prevent email incidents?
A. Installing antivirus rule updates
B. Disabling HTML in email content fields
C. Web proxy filtering
D. End-user training
Answer: D (LEAVE A REPLY)
While technical solutions like antivirus updates, disabling HTML in emails, and web proxy filtering play significant roles in securing email systems, the best method to prevent email incidents is often considered to be end-user training. This is because many email threats, such as phishing, rely on exploiting user behavior rather than technical vulnerabilities. By educating users on the risks associated with suspicious emails, how to recognize potentially harmful messages, and the importance of not clicking on unknown links or attachments, organizations can significantly reduce the risk of email-related incidents. End-

user training empowers individuals to act as a critical line of defense against email-based threats, complementing technical safeguards.
References:EC-Council's Certified Incident Handler (ECIH v3) curriculum emphasizes the importance of a holistic approach to cybersecurity, including the key role of end-user education in preventing email incidents and other security breaches.

NEW QUESTION: 113
Attackers or insiders create a backdoor into a trusted network by installing an unsecured access point inside a firewall. They then use any software or hardware access point to perform an attack. Which of the following is this type of attack?
A. Rogue- access point attack
B. Password-based attack
C. Malware attack
D. Email infection
Answer: (SHOW ANSWER)
A rogue-access point attack occurs when attackers or insiders install an unsecured access point within a trusted network, typically behind a firewall, to create a backdoor. This allows them to bypass network security measures and perform various malicious activities undetected. The use of any software or hardware access point to gain unauthorized access and conduct an attack characterizes a rogue-access point attack. This contrasts with password-based attacks, malware attacks, and email infections, which involve different methodologies and objectives, such as stealing credentials, distributing malicious software, or propagating through email systems, respectively.
References:The ECIH v3 certification materials discuss various types of network attacks, including rogue- access point attacks, highlighting the risk they pose by providing unauthorized network access to attackers.

NEW QUESTION: 114
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.
References:The ECIH v3 certification materials discuss various cyber attack strategies, including watering hole attacks, and provide insights into how attackers exploit trusted relationships between websites and their users.

NEW QUESTION: 115
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: 116
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.

References:The Incident Handler (ECIH v3) certification materials cover the legal aspects of incident response, including the importance of ensuring the admissibility of evidence in legal proceedings as a fundamental objective of the evidence collection and presentation process.

NEW QUESTION: 117

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

A. Risk transference

B. Risk assumption

C. Risk planning

D. Risk avoidance

Answer: B (LEAVE A REPLY)

NEW QUESTION: 118

Liam, a senior incident responder at a manufacturing company, is alerted to an email campaign distributing malware through fake invoice attachments. He confirms that some users opened the attachment, resulting in system slowdown and unauthorized access attempts. He disconnects affected machines, scans and removes malware, disables

compromised accounts, restores systems from clean backups, and documents file hashes, sender IPs, and malicious domains. Which of the following best describes Liam's objective?

A. To simulate future phishing scenarios

B. To conduct forensic preservation

C. To upgrade the internal mail server infrastructure

D. To eradicate all traces of the incident

Answer: (SHOW ANSWER)

This scenario clearly aligns with the eradication phase of the ECIH malware incident handling lifecycle.

After detection and containment, eradication focuses on completely removing malicious artifacts and ensuring the threat cannot re-emerge.

Option D is correct because Liam's actions-malware removal, account disabling, system restoration, and IOC documentation-are all aimed at fully eliminating the malware and attacker footholds. ECIH emphasizes that eradication must address malware binaries, persistence mechanisms, compromised credentials, and residual indicators.

Option B (forensic preservation) would avoid system changes, which Liam does not do.

Option A is a training activity unrelated to response. Option C is infrastructure improvement, not incident handling.

ECIH explicitly states that failure to eradicate all traces often leads to reinfection or continued attacker access.

Liam's comprehensive approach ensures the environment is returned to a trusted state and prepares detection systems for future prevention.

NEW QUESTION: 119

Which of the following types of digital evidence is temporarily stored in a digital device that requires constant power supply and is deleted if the power supply is interrupted?

A. Slack space

B. Process memory

C. Event logs

D. Swap file

Answer: B (LEAVE A REPLY)

Process memory (RAM) is a type of digital evidence that is temporarily stored and requires a constant power supply to retain information. If the power supply is interrupted, the information stored in process memory is lost. This type of evidence can include data about running programs, user actions, system events, and more, making it crucial for forensic analysis, especially in identifying actions taken by both users and malware.

Collecting data from process memory helps incident responders understand the state of the system at the time of an incident and can reveal valuable information that is not persisted elsewhere on the device.

References:Incident handling and response training, such as the ECIH v3 program, emphasize the importance of collecting and analyzing volatile data, including process memory, to effectively investigate and respond to cybersecurity incidents.

NEW QUESTION: 120
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.
References:ECIH v3 certification materials often reference Wireshark as a fundamental tool for network analysis, crucial for incident handlers in the analysis phase of incident response.

NEW QUESTION: 121
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: (SHOW ANSWER)
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.
Option B (SIEM event correlation) aggregates logs from multiple systems but does not typically capture screenshots or keystroke-level data. Option C (network forensics) focuses on packet captures and traffic analysis rather than user-level interaction evidence. Option D (host-based intrusion prevention systems) primarily block or detect malicious activity but do not provide comprehensive behavioral monitoring data like screenshots and keystroke logs.
ECIH emphasizes that insider threat cases rely heavily on behavioral indicators, digital activity reconstruction, and endpoint telemetry to determine intent and scope. Lina's reliance on user activity reconstruction and endpoint-level artifacts clearly aligns with user behavior analytics and endpoint monitoring.
Therefore, the correct answer is User behavior analytics and endpoint monitoring.

NEW QUESTION: 122
Alexis is working as an incident responder in XYZ organization. She was asked to identify and attribute the actors behind an attack that took place recently. In order to do so, she is performing threat attribution that deals with the identification of the specific person, society, or a country sponsoring a well-planned and executed intrusion or attack over its target.
Which of the following types of threat attributions Alexis performed?
A. Nation-state attribution
B. Intrusion-set attribution
C. True attribution
D. Campaign attributio
Answer: (SHOW ANSWER)

True attribution in the context of cyber incidents involves the identification of the actual individuals, groups, or entities behind an attack. This can include pinpointing specific persons, organizations, societies, or even countries that sponsor or carry out cyber intrusions or attacks. Alexis's efforts to identify and attribute the actors behind a recent attack by distinguishing the specific origins of the threat align with the concept of true attribution, which goes beyond mere speculation to provide concrete evidence about the perpetrators.
References:Threat attribution, especially true attribution, is a complex and nuanced area within cyber incident response, dealing with the identification of attackers. This concept is covered in cybersecurity courses and certifications, such as the ECIH v3 by EC-Council, focusing on the methodologies and challenges associated with attributing cyber attacks to their true sources.

NEW QUESTION: 123
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.
References:EC-Council's Certified Incident Handler (ECIH v3) program discusses various reconnaissance techniques, including ping sweeping, as a preliminary step in network analysis and vulnerability assessment.

NEW QUESTION: 124
Alice is an incident handler and she has been informed by her lead that the data on affected systems must be backed up so that it can be retrieved if it is damaged during the incident response process. She was also told that the system backup can also be used for further investigation of the incident. In which of the following stages of the incident handling and response (IH&R) process does Alice need to do a complete backup of the infected system?
A. Containment
B. Incident recording

C. Incident triage
D. Eradication
Answer: A (LEAVE A REPLY)
In the incident handling and response (IH&R) process, backing up the data on affected systems is a critical step that usually falls under the Containment phase. The Containment phase is crucial for limiting the scope and severity of an incident, ensuring that it does not spread further or affect additional systems. Backing up affected systems during containment is essential for several reasons: it preserves a snapshot of the system in its current state for forensic analysis, ensures that data is not lost if the system needs to be wiped or altered during the response process, and helps in the recovery process if data is corrupted or lost.
By performing a complete backup of the infected system during the Containment phase, Alice ensures that there is a reliable copy of all data and system states before any major actions, such as eradication or deeper forensic analysis, are taken. This step is also preparatory for the potential use of the backup in analyzing how the incident occurred and in restoring system functionality after the incident is resolved.
References:EC-Council's Certified Incident Handler (ECIH v3) courses and study guides highlight the importance of the Containment phase in the IH&R process, including the practice of backing up affected systems to prevent data loss and to aid in the investigation and recovery processes.

NEW QUESTION: 125
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.
References:The ECIH v3 certification program covers various risk mitigation strategies, emphasizing the selection of the appropriate approach based on the organization's risk tolerance and the specific context of the threat.

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 (**305** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)