ECCouncil.312-50v13.v2026-05-30.q249

Exam Code:	312-50v13
Exam Name:	Certified Ethical Hacker Exam (CEHv13)
Certification Provider:	ECCouncil
Free Question Number:	249
Version:	v2026-05-30
# of views:	258
# of Questions views:	2490
https://www.freepdfdumps.com/ECCouncil.312-50v13.v2026-05-30.q249.html	

NEW QUESTION: 1
During an internal assessment, a penetration tester gains access to a hash dump containing NTLM password hashes from a compromised Windows system. To crack the passwords efficiently, the tester uses a high- performance CPU setup with Hashcat, attempting millions of password combinations per second. Which technique is being optimized in this scenario?
A. Spoof NetBIOS to impersonate a file server
B. Leverage hardware acceleration for cracking speed
C. Dump SAM contents for offline password retrieval
D. Exploit dictionary rules with appended symbols
Answer: B (LEAVE A REPLY)
Password cracking is a core component of the system hacking phase. CEH materials highlight that once password hashes are obtained, attackers often perform offline cracking to avoid detection and bypass account lockout policies. Tools like Hashcat make use of hardware acceleration-specifically, GPU or multi-core CPU computing-to significantly increase cracking throughput. Hardware acceleration allows the system to perform thousands to millions of hash calculations simultaneously, dramatically improving cracking efficiency compared to traditional CPU-bound methods. While dumping SAM contents is part of credential extraction, it is not the optimization described in the scenario. Dictionary rules influence cracking strategy but not raw speed. NetBIOS spoofing is unrelated to password cracking. The emphasis here is on maximizing computational power to accelerate the hash-cracking process, aligning directly with CEH's explanation of hardware-accelerated offline cracking techniques.

NEW QUESTION: 2

During a red team assessment at Alpine Manufacturing Corp., network security consultant Marcus Lee is instructed to evaluate the security of internal communications within their switched LAN environment.
Without altering any switch configurations, Marcus manages to intercept credentials being transmitted between a payroll administrator's workstation and the backend authentication server. He subtly reroutes the communication path through his testing machine, though no proxy or VPN was involved. Analysis shows the redirection was achieved by injecting crafted messages that silently altered how the two hosts identified each other on the local network.
Which sniffing technique did Marcus most likely use?
A. DNS Spoofing
B. Switch Port Stealing
C. ARP Spoofing
D. MAC Flooding
Answer: C (LEAVE A REPLY)
The described behavior aligns precisely with ARP spoofing, also known as ARP poisoning, a common man- in-the-middle attack technique covered extensively in CEH materials.
ARP operates at Layer 2 of the OSI model and is responsible for mapping IP addresses to MAC addresses within a local network. Because ARP lacks authentication mechanisms, any host can send forged ARP replies to other devices on the LAN.
In this scenario, Marcus injects crafted messages that alter how two hosts identify each other. This strongly indicates forged ARP replies were sent to both the payroll workstation and the authentication server. By telling each system that his machine's MAC address corresponds to the other party's IP address, Marcus positions himself logically between the two endpoints. As a result, traffic is transparently routed through his system without requiring changes to switch configurations, proxies, or VPN tunnels.
This technique enables interception and potential modification of credentials in transit.
DNS spoofing affects domain name resolution rather than direct Layer 2 host identification.
MAC flooding overflows the switch CAM table to force broadcast behavior but does not specifically manipulate IP-to-MAC mappings between two targeted hosts. Switch port stealing targets MAC table entries but does not rely on altering host identity mappings in the same way ARP poisoning does.
Therefore, ARP spoofing is the most accurate technique described in this scenario.

NEW QUESTION: 3
You are a security analyst at Sentinel IT Services, monitoring the web application of GreenValley Credit Union in Portland, Oregon. During a log analysis, you identify an SQL injection attempt on the customer login portal, where the attacker inputs a malicious string to manipulate the query logic. The application mitigates this by replacing special characters with their escaped equivalents to prevent query manipulation before the query is executed,

ensuring the SQL statement remains unchanged. Based on the observed defense mechanism, which SQL injection countermeasure is the application employing?

A. Perform user input validation

B. Encoding the single quote

C. Restrict database access

D. Use parameterized queries or prepared statements

Answer: B (LEAVE A REPLY)

The behavior described matches the countermeasure commonly referred to in CEH materials as escaping or encoding special characters, most notably the single quote character. SQL injection frequently relies on breaking out of a quoted string in the SQL statement using the single quote, then appending logical operators such as OR 1=1, comments, or additional clauses. When an application replaces special characters with escaped equivalents before the SQL statement is executed, it attempts to ensure the input is treated purely as data rather than executable SQL syntax. A classic example is transforming a single quote into an escaped form such as \' or doubling it to '' depending on the database and escaping rules. By doing so, the database parser interprets the quote as part of the literal string value, preventing the attacker from terminating the string and altering query logic.

Option B is therefore the best fit because it precisely describes encoding or escaping the single quote, which is the most commonly targeted delimiter in SQL injection payloads. Option A, user input validation, is broader and typically refers to allowlisting accepted characters and formats, but the question specifically emphasizes replacement with escaped equivalents rather than rejecting invalid input. Option D, parameterized queries or prepared statements, is the strongest modern control recommended in CEH guidance because it separates code from data at the API level, but it is different from character escaping and does not rely on rewriting input characters. Option C limits damage but does not prevent injection. The observed mechanism is clearly single- quote encoding.

NEW QUESTION: 4

Noah Kim, an ethical hacker at Quantum Cyber Solutions in Austin, Texas, is assessing iPhones used for proprietary development. On one device, he demonstrates a technique that allows it to boot normally without a computer, but the elevated access is temporarily lost after restart until the user launches a special on-device app to reapply the modifications. Which jailbreaking method is this?

A. Tethered Jailbreaking

B. Untethered Jailbreaking

C. Semi-untethered Jailbreaking

D. Semi-tethered Jailbreaking

Answer: (SHOW ANSWER)

The scenario describes a jailbreak that boots normally without requiring a computer, but after a reboot the device loses the jailbroken (elevated) state until the user runs an on-device app to re-enable jailbreak features.
That behavior matches semi-untethered jailbreaking.
In iOS jailbreaking terminology, the key differentiator is what happens after a restart and whether a computer is required to regain jailbroken functionality. With a semi-untethered jailbreak, the device can reboot on its own into a normal, usable iOS state (so it is not "bricked" or stuck at boot), but jailbreak features such as elevated privileges, unsigned code execution, and tweaks are not active immediately after reboot. To reapply the jailbreak, the user launches a jailbreak app installed on the device, which triggers the exploit chain again and re-enables the modified state until the next reboot. This aligns exactly with "temporarily lost after restart until the user launches a special on-device app."
Why the other choices don't match:
Tethered jailbreaking (A) requires the device to be connected to a computer to boot; without tethering, the device cannot boot properly or remains unusable. The scenario explicitly says it can "boot normally without a computer," so it is not tethered.
Untethered jailbreaking (B) persists across reboots; the device remains jailbroken after restarting with no extra steps. That contradicts the described need to reapply modifications after restart.
Semi-tethered jailbreaking (D) is similar in that the device can boot without a computer, but typically the device boots into a non-jailbroken mode and may require a computer or additional steps to return to a jailbroken state depending on the method; the scenario specifically highlights re-enabling via an on-device app, which is the hallmark most commonly associated with semi-untethered jailbreaks.
Therefore, the jailbreaking method shown is C. Semi-untethered Jailbreaking.

NEW QUESTION: 5
A Certified Ethical Hacker (CEH) is auditing a company's web server that employs virtual hosting. The server hosts multiple domains and uses a web proxy to maintain anonymity and prevent IP blocking. The CEH discovers that the server's document directory (containing critical HTML files) is named "certrcx" and stored in /admin/web. The server root (containing configuration, error, executable, and log files) is also identified. The CEH also notes that the server uses a virtual document tree for additional storage. Which action would most likely increase the security of the web server?
A. Moving the document root directory to a different disk
B. Regularly updating and patching the server software
C. Changing the server's IP address regularly
D. Implementing an open-source web server architecture such as LAMP
Answer: B (LEAVE A REPLY)
CEH guidance for web server hardening prioritizes controls that reduce exploitable conditions across the broadest set of threats. While obscuring paths (for example, unusual

directory names like "certrcx" or storing content under "/admin/web") may slightly slow down casual discovery, CEH emphasizes that security through obscurity is not a reliable control. If an attacker can identify the server root, document root, and virtual directory structure (through misconfigurations, directory listing, error leakage, backup exposure, or known-path enumeration), then the real risk becomes unpatched vulnerabilities in the web server, modules, libraries, and underlying OS.
Regularly updating and patching the server software is the most direct, high-impact countermeasure because it closes known vulnerabilities attackers routinely exploit (RCE, privilege escalation, auth bypass, path traversal, request smuggling, etc.). CEH materials also stress that virtual hosting expands the attack surface (multiple sites, shared services, shared misconfigurations), making systematic patching and configuration management even more important.
Option A (moving the document root to a different disk) may help with organization and, in some cases, recovery planning, but it does not inherently reduce vulnerabilities. Option C (changing IPs) is not a security control; it may complicate blocking lists but doesn't fix the underlying weakness. Option D (using LAMP) is an architectural choice, not a security measure by itself-an open-source stack can still be insecure if misconfigured or unpatched. Therefore, CEH-aligned best practice is regular patching and updates.

NEW QUESTION: 6
Attackers exfiltrate data using steganography embedded in images. What is the best countermeasure?
A. Block all outbound traffic
B. Deploy IPS
C. Monitor outbound traffic for anomalies
D. Use steganalysis tools
Answer: D (LEAVE A REPLY)
CEH v13 explains that steganography-based exfiltration hides data within benign-looking files, making it extremely difficult to detect via firewalls or IPS alone. Blocking all outbound traffic is impractical, and IPS systems are not designed to analyze file content deeply for hidden data.
The most effective countermeasure is steganalysis, which involves inspecting files for statistical anomalies, altered pixel distributions, or hidden payload patterns. CEH v13 identifies steganalysis tools as the only reliable method to detect and decode hidden data. Traffic monitoring (Option C) helps identify suspicious transfers but cannot confirm steganography.
Therefore, Option D is correct.

NEW QUESTION: 7
During a penetration test at Sunshine Media ' s streaming platform in Miami, ethical hacker Sofia Alvarez examines whether the company ' s web server exposes sensitive resources

through poor configuration. She finds that a crawler directive at the server ' s root allows unintended indexing of restricted areas. This oversight reveals internal paths that may expose hidden links, confidential files, or other sensitive information.
Which technique is Sofia most likely using in this assessment?
A. Vulnerability Scanning
B. Information Gathering from robots.txt File
C. Web Server Footprinting/Banner Grabbing
D. Directory Brute Forcing
Answer: (SHOW ANSWER)
The scenario points directly to information gathering from the robots.txt file. A robots.txt file is typically located at the root of a website (e.g., https://example.com/robots.txt) and is intended to instruct search engine crawlers which paths should or should not be indexed. During web reconnaissance, testers often review robots.
txt because it can unintentionally disclose sensitive directories, administrative panels, staging paths, backup locations, or restricted areas that the organization hoped would remain obscure. The scenario explicitly says Sofia found "a crawler directive at the server's root" that "allows unintended indexing of restricted areas," and that this "reveals internal paths." That is exactly the kind of leakage that can come from misconfigured or overly revealing crawler directives.
This is considered an early-stage reconnaissance / information gathering technique because it does not require exploitation. It leverages publicly accessible configuration hints to map the application's hidden structure.
Even when robots.txt is used correctly, the listed disallowed entries can still serve as a roadmap of interesting targets; if configured incorrectly (for example, allowing indexing or exposing sensitive paths), it can increase exposure by helping those paths surface in search results or be discovered faster by attackers.
Why the other options are less accurate:
Vulnerability Scanning (A) implies using scanners to identify known flaws; here, the tester is manually
/strategically inspecting a crawler directive for exposed paths.
Web Server Footprinting/Banner Grabbing (C) focuses on identifying server type/version and technologies via headers or responses, not discovering hidden paths from crawler directives.
Directory Brute Forcing (D) uses wordlists to guess directories; Sofia's discovery comes from a disclosed list of paths, not brute-force guessing.
Therefore, the technique is B. Information Gathering from robots.txt File.

NEW QUESTION: 8
During a penetration test at a telecom provider in Denver, Colorado, Maria, a senior ethical hacker, notices that her scans are immediately flagged by intrusion detection systems. She modifies her technique, and as a result, the IDS devices are unable to reassemble the

packets correctly, allowing her probes to slip through without detection. Which scanning evasion technique is Maria applying in this case?

A. Packet Fragmentation

B. Source Routing

C. Decoy Scanning

D. IP Spoofing

Answer: A (LEAVE A REPLY)

The described evasion relies on preventing the IDS from correctly reassembling packets, which points directly to packet fragmentation. In fragmentation-based evasion, the attacker breaks the probe payload into multiple IP fragments. Some IDS sensors-especially if misconfigured, overloaded, or using limited reassembly logic-may fail to fully reconstruct the original packet stream, causing the malicious or suspicious content to evade signature matching and detection. Meanwhile, the target host (or a downstream device) may correctly reassemble the fragments and process the probe normally. This mismatch between what the IDS "sees" and what the target ultimately receives is the core concept behind fragmentation evasion.

The scenario explicitly says "IDS devices are unable to reassemble the packets correctly," which is essentially the textbook rationale for fragmentation as an IDS evasion method. Attackers may vary fragment size, overlap fragments, or manipulate offsets to stress or confuse reassembly engines. Even when modern IDS systems support reassembly, fragmentation can still be used to reduce detection reliability if sensors are under resource pressure or if traffic normalization is not enforced.

Why the other options don't match:

Source routing (B) attempts to influence the path packets take through the network; it does not inherently prevent IDS reassembly.

Decoy scanning (C) floods the target/IDS with scans from multiple spoofed addresses to obscure the true scanner source. This is about attribution noise, not packet reassembly failure.

IP spoofing (D) for scanning can disguise origin, but it does not inherently cause IDS reassembly problems.

Therefore, Maria is applying A. Packet Fragmentation.

NEW QUESTION: 9

In the sunlit tech oasis of Phoenix, Arizona, ethical hacker Nadia Patel explores the security posture of LearnSphere, a U.S.-based e-learning platform serving thousands of students. During her testing, Nadia intentionally submits invalid inputs to the platform ' s content delivery system. Instead of returning a generic failure notice, the application responds with detailed system information, including database query strings and directory paths. Such responses provide attackers with valuable insights into the application ' s internal workings, which could be used to craft more precise and damaging attacks.

Which issue is being demonstrated?

A. Improper Error Handling
B. Directory Traversal
C. Verbose Error Messages
D. CORS Misconfiguration
Answer: C (LEAVE A REPLY)
The issue described is verbose error messages, where an application reveals excessive technical details when handling invalid input. The scenario states that the platform returns "detailed system information, including database query strings and directory paths" instead of a generic error. Exposing internal paths and query strings is a common symptom of verbose error handling: stack traces, SQL statements, file system locations, framework versions, and configuration hints can appear in responses when exception handling is misconfigured or when debug settings are enabled in production.
These details are valuable to attackers because they reduce guesswork. Directory paths can reveal the operating system, deployment layout, and sensitive file locations; database query strings can reveal table
/column names and query structure, enabling more effective SQL injection payloads or targeted data extraction. Verbose errors can also leak usernames, internal hostnames, API endpoints, and even secrets if mishandled. Even if the initial invalid request does not compromise the system, the leaked information can significantly improve the attacker's ability to craft subsequent attacks with higher precision.
Why the other options are less accurate:
Improper error handling (A) is a broader category and could include verbose errors, but the question's best match is the specific symptom: detailed internal information disclosure.
Directory traversal (B) involves manipulating path input to access unauthorized files; here, the application is revealing paths due to errors, not being coerced into reading arbitrary files.
CORS misconfiguration (D) relates to cross-origin browser access controls and is unrelated to leaking stack traces or database queries.
Therefore, the correct answer is C. Verbose Error Messages.

NEW QUESTION: 10
Why is NTP responding with internal IP addresses and hostnames?
A. TCP fallback abuse
B. DNS poisoning
C. Honeypot redirection
D. Misconfigured NTP daemon allowing external queries
Answer: D (LEAVE A REPLY)
CEH v13 explains that NTP (UDP port 123) can leak sensitive network information if misconfigured. When an NTP daemon allows unrestricted external queries (e.g., monlist or ntpq commands), attackers can enumerate internal IP addresses and hostnames.

This exposure is a known reconnaissance weakness and has been exploited in both information disclosure and amplification attacks. CEH v13 strongly recommends restricting NTP query access using access control lists.
DNS poisoning and honeypots do not explain legitimate NTP enumeration responses. Therefore, option D is correct.

NEW QUESTION: 11
At a power distribution facility in Phoenix, Arizona, ethical hacker Sameer Das is performing an OT security assessment. He demonstrates that a programmable controller accepts modifications delivered over the network without checking the origin or cryptographic validity of the package. By uploading altered instructions, he changes how the controller processes commands during operations. Which IoT/OT threat best represents this technique?
A. Firmware update attack
B. Forged malicious device
C. Remote access using backdoor
D. Exploit kits
Answer: A (LEAVE A REPLY)
The correct answer is A. Firmware update attack because the scenario describes an attacker delivering an unauthenticated, non-cryptographically verified update/package to a controller and successfully altering its operational logic. In IoT/OT environments, controllers (PLCs, RTUs, PACs, and embedded industrial devices) often support updating firmware or logic over the network for maintenance. If the device does not verify the source, integrity, and authenticity of update packages-typically through signed firmware, certificates, and secure update channels-an attacker can replace legitimate code with a maliciously modified version.
Sameer's demonstration maps directly to a firmware/logic update compromise: he uploads "altered instructions" and changes how the controller processes commands during operations. This is exactly the type of risk highlighted in OT security: unauthorized modification of controller logic can cause unsafe states, disrupt production, damage equipment, or create stealthy manipulation that is difficult to detect. The explicit mention of "without checking the origin or cryptographic validity" indicates missing controls like digital signatures, hash verification, and trusted update mechanisms, which are central to firmware update security.
Why the other options are less accurate: Forged malicious device usually refers to introducing a rogue or cloned device into the environment to impersonate legitimate equipment. Remote access using backdoor implies an existing hidden access mechanism rather than abuse of the update mechanism itself. Exploit kits are typically collections of exploits used to compromise systems, commonly discussed more in endpoint/web contexts; they don't specifically describe the act of pushing an altered firmware/logic package that the controller accepts due to missing validation.

Therefore, the technique is best categorized as a firmware update attack, leveraging weak or absent authenticity/integrity checks on update packages to modify OT controller behavior.

NEW QUESTION: 12
In Miami, Florida, a luxury resort deploys smart climate control units in guest rooms. During a red team engagement, ethical hacker Sophia Bennett discovers that once a compromised device is restarted, it continues running altered instructions without any integrity check before the operating system loads. This allows tampered firmware to run as if it were legitimate. Which secure development practice would most directly prevent this weakness?
A. Allow code signing
B. Secure firmware or software updates
C. Utilize secure communication protocols
D. Ensure secure boot
Answer: (SHOW ANSWER)
The weakness described is that a device can reboot and still execute tampered firmware or pre-boot code
"without any integrity check before the operating system loads." The secure development practice that most directly prevents this is Secure Boot. Secure boot establishes a chain of trust starting at power-on, where each stage of the boot process verifies the integrity and authenticity of the next stage (bootloader, kernel, firmware components) before execution. If the verification fails (because firmware was modified, unsigned, or improperly signed), the device can halt, fall back to a known-good image, or enter a recovery mode- preventing malicious pre-OS code from running as if it were legitimate.
This matters especially for IoT devices such as smart climate control units, where attackers may attempt to persist by modifying firmware so that malware survives reboots. Without pre-boot integrity verification, a compromised device can continually load attacker-controlled instructions, making detection and remediation difficult.
Why the other options are less direct:
Code signing (A) is important, but by itself it does not guarantee the device will verify signatures at boot time.
Secure boot is the enforcement mechanism that validates signed boot components before they run.
Secure firmware/software updates (B) reduce the chance of malicious updates being installed (e.g., signed OTA updates, authenticated update channels), but they do not necessarily prevent execution of already- tampered firmware at startup if boot-time verification is missing.
Secure communication protocols (C) protect data in transit and device communications, but they do not address firmware integrity during the boot process.

Therefore, the most direct preventive practice for this pre-OS integrity gap is D. Ensure secure boot.

NEW QUESTION: 13
You are an ethical hacker at HorizonSec Consulting, hired by Liberty Insurance in Philadelphia, Pennsylvania, to test the resilience of their online claim submission portal. During testing, you modify the claim ID parameter in the URL with conditions such as AND and AND 1=2. When the first condition is used, the portal displays claim details as normal; when the second condition is used, the page displays no results.
You repeat this process to determine how the application responds to true and false conditions without error messages or delays.
Based on the observed behavior, which SQL injection technique are you employing?
A. UNION SQL Injection
B. Error-based SQL Injection
C. Time-based Blind SQL Injection
D. Boolean Exploitation
Answer: (SHOW ANSWER)
The behavior described matches Boolean-based blind SQL injection, which is represented here as Boolean Exploitation. In this technique, the tester injects conditions that evaluate to TRUE or FALSE and then infers the backend query behavior by observing differences in the application's response-such as returning normal content versus returning an empty page-without relying on explicit database error messages or time delays.
The scenario's key indicators are:
The injected payloads include conditional logic like AND 1=2, which is a classic always-false test.
When a true condition is used, the portal returns the expected claim details; when a false condition is used, it returns "no results." The tester repeats these true/false tests specifically "without error messages or delays," which rules out error- based and time-based approaches and confirms the "blind" inference method.
Why the other options don't fit:
UNION SQL Injection (A) relies on combining a malicious UNION SELECT with the original query to extract additional rows/columns directly into the response. The scenario is not extracting unioned data; it is observing response differences from boolean conditions.
Error-based SQL Injection (B) depends on triggering database errors and reading error output. The scenario explicitly notes no error messages are involved.
Time-based Blind SQL Injection (C) infers truth values by forcing delays (e.g., SLEEP()), which is explicitly not occurring here.
Therefore, the technique is best identified as D. Boolean Exploitation (Boolean-based blind SQL injection).

NEW QUESTION: 14

Multiple failed login attempts using expired tokens are followed by successful access with a valid token.
What is the most likely attack scenario?
A. Capturing a valid token before expiry
B. Token replay attack using expired tokens
C. Brute-forcing token generation
D. Exploiting a race condition in token validation
Answer: D (LEAVE A REPLY)
This scenario strongly suggests a race condition attack in the application's token validation logic, as described in CEH v13 Web Application Hacking. A race condition occurs when an application processes multiple requests simultaneously and fails to properly synchronize validation checks.
The presence of multiple failed attempts using expired tokens followed by successful access within a short time window indicates the attacker exploited a timing flaw. During this window, the system may have inconsistently validated token expiration, allowing an expired token to be accepted.
Option A is unlikely because the logs specifically reference expired tokens. Option B is incorrect because replaying expired tokens should fail unless a validation flaw exists. Option C is highly improbable due to token entropy.
CEH v13 highlights race conditions as advanced logic flaws that are difficult to detect and often missed during standard testing. They are commonly exploited in authentication, payment processing, and session management systems.
Therefore, Option D is the correct and CEH-aligned answer.

NEW QUESTION: 15
During a penetration test at Lone Star Healthcare in Austin, ethical hacker Liam evaluates the hospital ' s perimeter defenses by generating controlled traffic flows through the firewall. He uses a tool that can create and replay diverse traffic patterns to test how well the firewall enforces its rules against both legitimate and malicious traffic types. This allows him to demonstrate whether the device properly identifies evasion attempts under simulated attack conditions.
Which tool is Liam most likely using in this test?
A. Nmap
B. Traffic IQ Professional
C. Colasoft Packet Builder
D. Metasploit
Answer: B (LEAVE A REPLY)
The scenario best matches Traffic IQ Professional because it describes a tool used to generate and replay diverse traffic patterns through a firewall to validate rule enforcement and detection under simulated attack conditions. The key functions here are traffic

generation, replay, and the ability to model both legitimate and malicious flows to test whether the firewall correctly handles evasion attempts and policy enforcement.
Traffic generation/replay platforms are used in security validation and firewall testing to emulate real-world network behaviors at scale and to assess how devices respond to crafted or replayed traffic profiles.
Why the other tools are less suitable:
Nmap (A) is primarily a scanner for host discovery, port scanning, and service enumeration, with some scripting capabilities. It is not chiefly a traffic generation/replay system for exercising a firewall with diverse controlled flows.
Colasoft Packet Builder (C) can craft packets and build custom traffic at the packet level, which is useful for creating specific test packets. However, the scenario emphasizes broader "diverse traffic patterns" and replay of flows in a way typically associated with traffic modeling/validation suites rather than single-packet construction.
Metasploit (D) is an exploitation framework used to develop and execute exploits and payloads. While it can generate certain traffic, its primary purpose is not comprehensive traffic generation and replay to validate firewall policies under many traffic types.
Traffic IQ Professional is the best fit because it aligns with a firewall test plan focused on simulating legitimate and malicious traffic profiles, including evasion-style patterns, and demonstrating how the perimeter device behaves under controlled conditions. This approach is often used to evaluate whether a firewall can consistently enforce security policies, detect anomalies, and resist evasion techniques without overblocking legitimate traffic.
Therefore, the most likely tool is B. Traffic IQ Professional.

NEW QUESTION: 16
During an IDS audit, you notice numerous alerts triggered by legitimate user activity. What is the most likely cause?
A. Regular users are unintentionally triggering security protocols
B. The firewall is failing to block malicious traffic
C. The IDS is outdated and unpatched
D. The IDS is configured with overly sensitive thresholds
Answer: D (LEAVE A REPLY)
According to the CEH IDS/IPS module, false positives occur when legitimate activity is incorrectly flagged as malicious. The most common cause is overly sensitive IDS rules or thresholds.
Option D correctly identifies this issue.
Option A describes the symptom, not the root cause.
Option B is unrelated to IDS alert behavior.
Option C can cause missed detections, not excessive alerts.
CEH recommends proper tuning and baseline profiling.

NEW QUESTION: 17
Which advanced mobile attack is hardest to detect and mitigate?
A. Mobile MitM
B. Jailbreaking/Rooting
C. Mobile Remote Access Trojan (RAT)
D. Clickjacking
Answer: C (LEAVE A REPLY)
Mobile Remote Access Trojans (RATs) are highlighted in CEH v13 Mobile Platform Hacking as one of the most dangerous threats. Once installed, a mobile RAT provides attackers persistent, covert access to devices, allowing screen capture, keystroke logging, microphone activation, and data exfiltration.
Unlike MitM or clickjacking, RATs operate post-compromise, often disguised as legitimate apps. Jailbreaking is detectable via integrity checks, but RATs can remain hidden even on non-rooted devices.
CEH v13 emphasizes that RATs bypass traditional defenses, including antivirus and MDM, making them extremely difficult to detect. Hence, Option C is correct.

NEW QUESTION: 18
Which scenario best describes a tailgating attack?
A. Following an employee through a secured door
B. Phishing email requesting credentials
C. Phone-based impersonation
D. Leaving a malicious USB device
Answer: A (LEAVE A REPLY)
Tailgating, as defined in CEH v13 Social Engineering, is a physical social engineering attack where an unauthorized individual gains access by following an authorized person into a restricted area.
The attacker exploits human courtesy rather than technical vulnerabilities. Options B, C, and D describe phishing, pretexting, and baiting respectively.
Thus, option A is the correct representation of tailgating.

NEW QUESTION: 19

An ethical hacker needs to enumerate user accounts and shared resources within a company's internal network without raising any security alerts. The network consists of Windows servers running default configurations.
Which method should the hacker use to gather this information covertly?
A. Deploy a packet sniffer to capture and analyze network traffic
B. Perform a DNS zone transfer to obtain internal domain details
C. Exploit null sessions to connect anonymously to the IPC$ share
D. Utilize SNMP queries to extract user information from network devices
Answer: C (LEAVE A REPLY)
CEH v13 explains that Windows systems running older or default configurations often allow anonymous or null session connections to IPC$ shares, enabling attackers to enumerate users, groups, shares, and other system details without authentication. Null session enumeration is highlighted as a classic yet effective technique because it generates minimal detectable activity and does not require credentials, making it ideal for stealth operations. CEH stresses that SMB null sessions are frequently overlooked in legacy or poorly hardened environments, especially when default permissions remain unchanged. Packet sniffing (Option A) may provide some data but requires traffic visibility and may be detected through monitoring tools. DNS zone transfers (Option B) require misconfigurations and usually do not reveal user list details. SNMP queries (Option D) require community strings and often generate alerts. Therefore, exploiting null sessions is the most covert and effective method for enumerating Windows systems under default configurations.

NEW QUESTION: 20
During a penetration test at TechTrend Innovations in California, ethical hacker Jake Henderson reviews the company's web server exposure to network-based threats. He finds that the server is running with multiple open services and protocols that are not required for its operation, such as NetBIOS and SMB. Jake explains to the IT team that attackers could exploit these unnecessary services to gain unauthorized access to the server.
Which hardening measure should the IT team implement to mitigate this risk?
A. Use a dedicated machine as a web server
B. Conduct risk assessment for patching
C. Eliminate unnecessary files
D. Block all unnecessary ports, ICMP traffic, and protocols
Answer: D (LEAVE A REPLY)
The risk described is increased attack surface caused by unnecessary services and protocols running on a web server-specifically NetBIOS and SMB. The most direct hardening action to mitigate this is to block/disable unnecessary ports and protocols so they are not exposed to the network and cannot be abused by attackers.

Option D captures that principle: reduce exposure by closing ports and restricting protocols that are not required for the server's role.
A well-hardened web server should run only the services needed to deliver its intended web functionality (e.
g., HTTP/HTTPS and necessary management interfaces under strict control). Services like SMB (commonly TCP 445/139) and NetBIOS (UDP 137/138, TCP 139) are not normally required for public-facing web hosting and are frequent targets for enumeration and exploitation. Leaving such services open can enable attackers to perform credential attacks, exploit legacy vulnerabilities, access shared resources, or pivot further into the environment. By blocking or disabling these ports at the host firewall and/or perimeter firewall, the organization reduces reachable attack paths and limits what an external attacker can interact with.
Why the other options are less direct:
Dedicated machine (A) can help separation of duties, but if unnecessary services still run, the attack surface remains.
Risk assessment for patching (B) is important, but it doesn't immediately remove the exposure created by unneeded services.
Eliminating unnecessary files (C) addresses file-system exposure, not open network services like SMB
/NetBIOS.
Because the problem is explicitly about unnecessary open services/protocols, the best mitigation is D. Block all unnecessary ports, ICMP traffic, and protocols (i.e., minimize exposed services).

NEW QUESTION: 21
After a breach, investigators discover attackers used modified legitimate system utilities and a Windows service to persist undetected and harvest credentials. What key step would best protect against similar future attacks?
A. Disable unused ports and restrict outbound firewall traffic
B. Perform weekly backups and store them off-site
C. Ensure antivirus and firewall software are up to date
D. Monitor file hashes of critical executables for unauthorized changes
Answer: (SHOW ANSWER)
CEH materials describe this attack pattern as Living-off-the-Land (LotL), where attackers abuse legitimate tools to avoid detection. Because these binaries are normally trusted, traditional antivirus solutions may not flag them.
CEH recommends file integrity monitoring (FIM), which tracks cryptographic hashes of sensitive executables and alerts administrators when unauthorized modifications occur.
Option D is correct.
Options A and B support resilience but do not detect tampering.
Option C alone is insufficient against LotL attacks.

NEW QUESTION: 22
During an internal red team engagement at a software company in Boston, ethical hacker Meera gains access to a developer ' s workstation. To ensure long-term persistence, she plants a lightweight binary in a hidden directory and configures it to automatically launch every time the system is restarted. Days later, even after the host was rebooted during patching, the binary executed again without requiring user interaction, giving Meera continued access.
Which technique most likely enabled this persistence?
A. Scheduled Tasks
B. Creating a new service
C. Startup Folder
D. Registry run keys
Answer: D (LEAVE A REPLY)
The persistence described-"automatically launch every time the system is restarted" with no user interaction-most commonly aligns with Registry Run keys on Windows. Run keys are a classic persistence mechanism where an attacker adds a value referencing their executable to locations such as HKCU\Software\Microsoft\Windows\CurrentVersion\Run (per-user) or HKLM\Software\Microsoft\Windows\CurrentVersion\Run (system-wide). When Windows starts (and/or when a user logs in, depending on the key), the operating system processes these entries and launches the referenced program automatically. This provides reliable persistence across reboots and is frequently used because it is simple, effective, and blends with legitimate startup entries.
The scenario indicates Meera placed a binary in a hidden directory and configured it to auto-launch after restarts. Registry-based autoruns fit that exact pattern: the binary can reside anywhere (including a hidden folder), while the registry entry points to it. The persistence survives reboot and does not require the attacker to be present.
Why the other options are less likely given the phrasing:
Startup Folder (C) can also auto-launch programs, but it commonly implies a shortcut or executable placed in the user's startup directory and is generally tied to user logon behavior. The question emphasizes "every time the system is restarted" and is most often tested in CEH contexts as registry autorun persistence.
Scheduled Tasks (A) can run at startup or on triggers and is a valid persistence technique, but the scenario does not mention task scheduling, triggers, or task configuration.
Creating a new service (B) would typically imply installing a Windows service, often requiring elevated privileges and presenting as a managed service; the scenario frames it as a lightweight binary planted and configured to auto-launch, which aligns more naturally with Run keys.
Therefore, the most likely persistence technique is D. Registry run keys.

NEW QUESTION: 23

During a physical penetration test simulating a social engineering attack, a threat actor walks into the lobby of a target organization dressed as a field technician from a known external vendor. Carrying a fake ID badge and referencing a known company name, the attacker confidently claims they've been dispatched to perform a routine server room upgrade. Using internal-sounding terminology and referencing real employee names gathered via OSINT, the individual conveys urgency. The receptionist, recognizing the vendor name and the convincing language, allows access without verifying the credentials.

A. Perceived authority and reliance on third-party familiarity

B. Leaked credentials on public networks and forums

C. Trust in physical security logs used by security teams

D. Misconfigured network segmentation allowing unauthorized access

Answer: A (LEAVE A REPLY)

CEH's social engineering principles highlight psychological manipulation techniques such as authority, urgency, trust exploitation, and impersonation. In this scenario, the attacker leverages "perceived authority," a powerful influence tactic where the social engineer poses as someone with legitimate power or sanctioned access-such as a technician, auditor, or vendor representative. CEH emphasizes that referencing real employee names, using technical terminology, and impersonating trusted third-party partners increases believability and reduces verification resistance. The receptionist's acceptance of the attacker's presence without verifying credentials matches classical authority-based exploitation. Leaked credentials, physical security logs, and network segmentation issues do not relate to human-layer social engineering. The situation clearly reflects the manipulation of trust and authority as described in CEH's psychological attack vectors.

NEW QUESTION: 24

Which technique is most likely used to evade detection by an Intrusion Detection System (IDS)?

A. Fragmenting malicious packets into smaller segments

B. Using self-replicating malware

C. Sending phishing emails

D. Flooding the IDS with ping requests

Answer: (SHOW ANSWER)

CEH v13 explains that packet fragmentation is a classic and effective IDS evasion technique. By breaking malicious payloads into smaller fragments, attackers attempt to prevent the IDS from reconstructing the full packet stream correctly, thereby avoiding signature detection.

Many IDS systems rely on packet reassembly and pattern matching. Fragmented packets can confuse or overload the reassembly process, especially if the IDS is poorly configured. CEH v13 specifically lists fragmentation, overlapping fragments, and out-of-order packets as evasion techniques used to bypass network defenses.

Option B describes malware propagation, not IDS evasion. Option C is a social engineering attack, unrelated to IDS detection. Option D is a denial-of-service attempt, not a stealth evasion method.
CEH v13 highlights that defending against fragmentation-based evasion requires proper normalization and reassembly configuration in IDS/IPS systems. Therefore, Option A is the correct answer.

NEW QUESTION: 25
During a cloud security assessment, it was discovered that a former employee still had access to critical resources months after leaving the organization. Which practice would have most effectively prevented this issue?
A. Using multi-cloud deployment models
B. Implementing real-time traffic analysis
C. Conducting regular penetration tests
D. Enforcing timely user de-provisioning
Answer: D (LEAVE A REPLY)
According to CEH v13 Cloud Computing, improper identity and access management (IAM) is one of the most common causes of cloud security incidents. When former employees retain access to cloud resources, it represents a failure in user lifecycle management, specifically in the de-provisioning phase.
Timely user de-provisioning ensures that when an employee leaves the organization or changes roles, all associated access rights-API keys, IAM roles, credentials, tokens, and permissions-are immediately revoked. CEH v13 emphasizes that cloud environments magnify this risk because access is often centralized and remote, meaning former employees can access systems from anywhere.
Options A, B, and C are supportive security practices but do not directly address the root cause. Multi-cloud models do not prevent unauthorized access. Traffic analysis may detect misuse after the fact but does not prevent it. Penetration testing identifies vulnerabilities but does not manage user access.
CEH v13 explicitly identifies timely de-provisioning as a critical cloud security control to prevent insider threats, privilege abuse, and compliance violations. Therefore, Option D is the correct answer.

NEW QUESTION: 26
In the bustling digital marketplace of Miami's tech corridor, ethical hacker Sofia Alvarez probes the virtual defenses of RetailRush, a US-based online retailer hosting thousands of daily transactions. Tasked with exposing weaknesses in the web server's URL processing, Sofia submits crafted requests to manipulate resource paths. Her tests uncover a severe flaw: the server grants access to restricted system files, exposing sensitive configuration data. Further scrutiny reveals the issue stems from the server's failure to validate input paths, not from header manipulation, cached content tampering, or credential compromise.

Committed to hardening the platform, Sofia drafts a precise report to direct the security team toward immediate fixes.
Which web server attack type is Sofia most likely exploiting in RetailRush's web server?
A. Directory Traversal Attack
B. Web Cache Poisoning Attack
C. HTTP Response Splitting Attack
D. Password Cracking Attack
Answer: A (LEAVE A REPLY)
A Directory Traversal attack, also known as path traversal, exploits weaknesses in how a web server or web application processes user-supplied file and directory paths through URLs or parameters. In CEH-aligned terminology, the attacker crafts requests that use traversal sequences such as dot-dot-slash patterns or encoded equivalents to escape the intended web root or permitted directory and reach sensitive locations on the underlying file system. The question states Sofia "manipulates resource paths" and successfully accesses
"restricted system files," revealing "sensitive configuration data." This is the defining outcome of directory traversal: unauthorized access to files that should never be directly retrievable via the web interface, including application configuration files, server configuration, environment files, or other OS-level resources.
The prompt also eliminates other options by describing what the issue is not. It is not header manipulation, which would be more consistent with HTTP response splitting or header injection behaviors. It is not cached content tampering, which points to web cache poisoning. It is not credential compromise, which would indicate password cracking. Instead, the root cause is explicitly "failure to validate input paths," matching CEH emphasis on inadequate input validation and improper path normalization or canonicalization before file access. Defensive guidance typically focuses on strict allowlisting of accessible resources, canonicalizing paths and enforcing a fixed base directory, blocking traversal tokens and their encoded forms, using indirect references instead of raw file paths, and applying least-privilege permissions to reduce impact if traversal is attempted.

NEW QUESTION: 27
While performing a SYN (half-open) scan using Nmap, you send a SYN packet to a target IP address and receive a SYN/ACK response. How should this result be interpreted?
A. The scanned port is open and ready to establish a connection
B. The target IP is unreachable
C. The port is filtered by a firewall
D. The port is closed but acknowledged
Answer: A (LEAVE A REPLY)
According to the CEH Network Scanning module, a SYN scan works by analyzing TCP handshake responses.

SYN # SYN/ACK = Port OPEN
SYN # RST = Port CLOSED
No response = FILTERED
Option A is correct.
CEH emphasizes SYN scanning as stealthy because the handshake is never completed.

NEW QUESTION: 28
A penetration tester is evaluating the security of a mobile application and discovers that it lacks proper input validation. The tester suspects that the application is vulnerable to a malicious code injection attack. What is the most effective way to confirm and exploit this vulnerability?
A. Perform a brute-force attack on the application's login page to guess weak credentials
B. Inject a malicious JavaScript code into the input fields and observe the application's behavior
C. Use directory traversal to access sensitive files stored in the application's internal storage
D. Execute a dictionary attack on the mobile app's encryption algorithm
Answer: B (LEAVE A REPLY)
CEH teaches that insufficient input validation on mobile applications enables code injection attacks. Injecting JavaScript or crafted payloads into fields validates whether the application improperly processes untrusted data. If executed, it confirms that the app is vulnerable to injection-based attacks.

NEW QUESTION: 29
A malware analyst is tasked with evaluating a suspicious PDF file suspected of launching attacks through embedded JavaScript. Initial scans using pdfid show the presence of /JavaScript and /OpenAction keywords.
What should the analyst do next to understand the potential impact?
A. Upload the file to VirusTotal and rely on engine consensus
B. Disassemble the PDF using PE Explorer
C. Extract and analyze stream objects using PDFStreamDumper
D. Compute file hashes using HashMyFiles for signature matching
Answer: (SHOW ANSWER)
This question relates to Malware Analysis, specifically PDF-based malware, as covered in the CEH v13 Malware Threats module. The presence of /JavaScript and /OpenAction keywords identified by pdfid strongly indicates potentially malicious behavior triggered when the PDF is opened.
CEH v13 recommends static analysis of PDF stream objects as the next step to understand embedded malicious logic. Tools such as PDFStreamDumper allow analysts to extract, decompress, and inspect object streams within a PDF file, revealing obfuscated JavaScript code or exploit payloads.

The /OpenAction keyword indicates that the embedded JavaScript executes automatically when the document is opened, a common technique used in PDF-based attacks to exploit reader vulnerabilities or download secondary payloads.
Other options are insufficient:
VirusTotal provides detection results but not behavioral insight.
PE Explorer is irrelevant because PDFs are not Portable Executable files.
Hashing only helps identify known malware, not analyze behavior.
CEH v13 emphasizes manual inspection of embedded scripts to determine intent, making PDFStreamDumper the correct next step.

NEW QUESTION: 30
While conducting a red team exercise at a corporate office in San Diego, California, you observe employees working in an open-plan area. By discreetly watching their screens and hand movements as they log into internal systems, you are able to capture several usernames and partial passwords without touching any devices or interacting with the staff.
Which social engineering technique does this scenario best illustrate?
A. Shoulder Surfing
B. Dumpster Diving
C. Impersonation
D. Tailgating
Answer: A (LEAVE A REPLY)
This scenario most clearly illustrates shoulder surfing, a social engineering technique where an attacker obtains sensitive information by observing a victim's screen, keystrokes, or written notes-often from a nearby position-without directly interacting with the victim or their device. The key indicators are that the tester is "discreetly watching their screens and hand movements" during login and is able to capture
"usernames and partial passwords" without touching anything. That is the defining pattern of shoulder surfing: passive observation to harvest credentials or other confidential information.
Shoulder surfing is particularly effective in open-plan offices, shared workspaces, airports, cafes, or any environment where people can be observed entering credentials. Attackers may watch directly, use reflections (e.g., glass surfaces), or position themselves to see the keyboard and screen. Even partial password capture can be valuable when combined with other information (usernames, password patterns, reset questions, or subsequent observation), and it can help an attacker craft more convincing follow-on social engineering attempts.
Why the other options do not fit:
Dumpster diving (B) involves retrieving sensitive information from trash (printed documents, media, badges, notes), not observing logins in real time.

Impersonation (C) requires actively posing as a trusted person (IT staff, vendor, employee) to persuade someone to disclose information or grant access; the scenario explicitly avoids interaction with staff.
Tailgating (D) is physically following someone through a secure door to gain unauthorized entry; it's about bypassing physical access controls rather than capturing credentials.
Because the technique relies on visual observation of screens and keystrokes to obtain login details, the correct answer is A. Shoulder Surfing.

NEW QUESTION: 31
In Austin, Texas, ethical hacker Michael Reyes is conducting a red team exercise for Horizon Tech, a software development firm. During his assessment, Michael crafts a malicious link that appears to lead to the company's internal project management portal. When an unsuspecting employee clicks the link, it redirects them to a login session that Michael has already initialized with the server. After the employee logs in, Michael uses that session to access the portal in a controlled test, demonstrating a vulnerability to the IT team.
Which session hijacking technique is Michael using in this red team exercise?
A. Session donation attack
B. Session replay attack
C. Session sniffing
D. Session fixation attack
Answer: D (LEAVE A REPLY)
This scenario matches a session fixation attack because Michael sets up a valid session identifier with the application first, then forces the victim to authenticate while using that same pre-established session. In CEH terms, session fixation occurs when an attacker "fixes" or plants a known session ID in the victim's browser, typically via a crafted URL parameter, cookie setting through a subdomain, or a redirect that preserves a session token. If the application does not regenerate the session ID after login, the victim's authentication becomes bound to the attacker-known session. The attacker can then reuse that same session ID to access the application as the victim, exactly as described when Michael "uses that session to access the portal" after the employee logs in.
The other options do not fit the mechanism. Session sniffing relies on capturing session tokens from network traffic, usually when encryption is missing or weak, but the question focuses on a link and a pre-initialized session rather than intercepting traffic. Session replay generally refers to capturing and replaying authentication exchanges or tokens, not pre-setting a session before the victim authenticates. "Session donation" is not the standard CEH label for this behavior and is not the best match to the described flow.
CEH-recommended mitigations include regenerating session IDs immediately after authentication and privilege changes, rejecting session IDs supplied in URLs, setting Secure and HttpOnly cookie flags, enforcing SameSite where appropriate, implementing

short idle timeouts, and adding server-side controls to detect concurrent use or abnormal session binding changes.

NEW QUESTION: 32
You are a security analyst at Sentinel Cyber Group, monitoring the web portal of Aspen Valley Bank in Salt Lake City, Utah. During log review, you notice repeated attempts by attackers to inject malicious strings into the login fields. However, despite these attempts, the application executes queries safely without altering their logic, since user inputs are kept separate from the SQL statements and bound as fixed values before execution. Based on the observed defense mechanism, which SQL injection countermeasure is the application employing?
A. Perform user input validation
B. Restrict database access
C. Encoding the single quote
D. Use parameterized queries or prepared statements
Answer: D (LEAVE A REPLY)
The defense described-keeping user inputs separate from the SQL statement and binding them as fixed values before execution-is the defining characteristic of parameterized queries (prepared statements). This is one of the most effective and widely recommended countermeasures against SQL injection because it prevents attacker input from being interpreted as SQL code.
In a vulnerable application, developers often build SQL statements by concatenating strings, such as
"SELECT ... WHERE user='" + input + "'". In that pattern, malicious payloads can alter the query structure (adding conditions, UNIONs, comments, or stacked queries). With prepared statements, the SQL engine receives the query structure first (the template), and then receives the parameter values separately. The database treats the parameters strictly as data, not executable SQL. As a result, even if an attacker submits quotes, keywords, or operators, those characters remain part of the parameter value and cannot change the query's logic.
The scenario specifically says inputs are "bound as fixed values," which is direct language associated with parameter binding. That makes option D the best answer.

Why the other options are less accurate:
User input validation (A) is helpful but can be bypassed and is not as robust as parameterization; also the described mechanism is not validation but binding separation.
Restrict database access (B) is a defense-in-depth measure (least privilege) that reduces impact, but it does not inherently stop injection from occurring.
Encoding the single quote (C) is a legacy/insufficient approach; encoding or escaping can be error-prone and DBMS-specific, and it does not match the description of parameters being bound separately.
Therefore, the application is using D. Use parameterized queries or prepared statements.

NEW QUESTION: 33
A penetration tester performs a vulnerability scan on a company's network and identifies a critical vulnerability related to an outdated version of a database server. What should the tester prioritize as the next step?
A. Attempt to exploit the vulnerability using publicly available tools or exploits
B. Conduct a brute-force attack on the database login page
C. Ignore the vulnerability and move on to testing other systems
D. Perform a denial-of-service (DoS) attack on the database server
Answer: A (LEAVE A REPLY)
CEH v13 details the standard penetration testing workflow, where confirmed critical vulnerabilities- especially those affecting core systems like database servers-should be prioritized for exploitation only after verification and when explicitly permitted by the rules of engagement. Exploiting a known vulnerability using vetted tools (e.g., Metasploit, CVE-specific exploits) provides evidence of real-world risk and validates the severity rating. Brute-forcing logins (Option B) is inefficient and often outside scope. Ignoring a critical vulnerability (Option C) violates CEH's prioritization guidelines. A DoS attack (Option D) is never appropriate unless the engagement explicitly authorizes destructive testing, which is rare. CEH stresses that high-impact vulnerabilities should be exploited to demonstrate business risk, privilege escalation potential, data exposure, or lateral movement possibilities-making Option A fully aligned with CEH methodology.

NEW QUESTION: 34
In a highly secure online banking environment, customers report unauthorized access to their accounts despite robust authentication controls. Investigation reveals attackers are using advanced session hijacking techniques to perform fraudulent transactions. Which advanced session-hijacking attack, resembling a scenario-based attack, presents the greatest challenge to detect and mitigate?
A. Covert Cross-Site Scripting (XSS) attack injecting malicious scripts into banking pages
B. Man-in-the-Browser (MitB) attack using malicious browser extensions to intercept sessions
C. Session fixation attack manipulating HTTP session identifiers

D. Passive sniffing attack capturing encrypted session tokens over unsecured Wi-Fi
Answer: B (LEAVE A REPLY)
According to the CEH System Hacking and Web Application Security modules, Man-in-the-Browser (MitB) attacks are among the most sophisticated and difficult session-hijacking techniques to detect. In MitB attacks, malware operates inside the victim's browser, allowing attackers to intercept, modify, or inject transactions after authentication has occurred.
CEH documentation highlights that MitB attacks bypass:
Multi-factor authentication
Encrypted cookies
HTTPS/TLS protections
Because the malicious activity occurs at the browser level, security controls perceive transactions as legitimate.
Option B is correct.
Option A (XSS) is detectable via content security policies.
Option C is mitigated by regenerating session IDs.
Option D is ineffective against encrypted sessions.
CEH emphasizes MitB attacks as a critical threat to online banking systems.

NEW QUESTION: 35
During an internal penetration test within a large corporate environment, the red team gains access to an unrestricted network port in a public-facing meeting room. The tester deploys an automated tool that sends thousands of DHCPDISCOVER requests using randomized spoofed MAC addresses. The DHCP server's lease pool becomes fully depleted, preventing legitimate users from obtaining IP addresses. What type of attack did the penetration tester perform?
A. DHCP starvation
B. Rogue DHCP relay injection
C. DNS cache poisoning
D. ARP spoofing
Answer: A (LEAVE A REPLY)
DHCP starvation is a network-level attack in which an attacker sends a massive number of DHCPDISCOVER requests, each appearing to originate from a different MAC address. CEH courseware explains that DHCP servers assign IP leases based on unique MAC addresses, and when the lease pool is exhausted, legitimate clients are unable to obtain valid IP configurations. This disrupts network connectivity and can serve as a precursor to deploying a rogue DHCP server, enabling further attacks such as traffic redirection or credential interception. DHCP starvation is different from ARP spoofing, which manipulates MAC-IP mappings, or DNS poisoning, which corrupts domain resolution. Rogue DHCP relay attacks involve forwarding DHCP packets to unauthorized servers, not depleting leases. The scenario described-rapid MAC address spoofing and exhaustion of DHCP

leases-matches the precise definition of DHCP starvation as documented in CEH materials.

NEW QUESTION: 36
During a penetration test at a financial services company in Denver, ethical hacker Jason demonstrates how employees could be tricked by a rogue DHCP server. To help the client prevent such attacks in the future, Jason shows the administrators how to configure their Cisco switches to reject DHCP responses from untrusted ports. He explains that this global setting must be activated before more granular controls can be applied.
Which switch command should Jason recommend to implement this defense?
A. Switch(config)# ip dhcp snooping
B. Switch(config)# ip arp inspection vlan 10
C. Switch(config)# ip dhcp snooping vlan 10
D. Switch(config-if)# ip dhcp snooping trust
Answer: A (LEAVE A REPLY)
The correct answer is A. Switch(config)# ip dhcp snooping because the question asks for the global setting that must be enabled first, before applying more specific (granular) DHCP Snooping controls. In Cisco switching, DHCP Snooping is the primary Layer 2 security feature used to mitigate rogue DHCP server attacks. Once enabled, the switch can distinguish between trusted ports (where legitimate DHCP server responses are allowed, typically uplinks toward the authorized DHCP server) and untrusted ports (typically access ports to end-user devices), where DHCP server responses (DHCPOFFER/DHCPACK) are filtered to prevent a rogue server from handing out malicious network configuration (gateway/DNS) to clients.
The scenario's defense goal-"reject DHCP responses from untrusted ports"-is exactly what DHCP Snooping enforces after it is enabled and ports are assigned trust states.
Conceptually, the workflow is:
Enable DHCP Snooping globally (feature activation),
Enable it for the relevant VLAN(s), and
Mark the legitimate DHCP-facing interface(s) as trusted so only those ports can send DHCP server responses.
Options C and D are part of the later, granular steps:
C enables DHCP snooping for a specific VLAN, which is necessary but is not the global prerequisite the question highlights.
D is applied under an interface to designate a port as trusted; again, this is granular and only meaningful after DHCP snooping is activated.
Option B is a different feature (Dynamic ARP Inspection) and is used to mitigate ARP spoofing/poisoning rather than rogue DHCP.
Therefore, the global command Jason should recommend first is Switch(config)# ip dhcp snooping.

NEW QUESTION: 37
In Austin, Texas, ethical hacker Liam Carter is hired by Lone Star Healthcare to probe the defenses of their patient data network. During his penetration test, Liam aims to bypass the hospital's firewall protecting a medical records server. To do so, he uses a tool to craft custom network packets, carefully designing their headers to slip past the firewall's filtering rules. His goal is to demonstrate how an attacker could infiltrate the system, exposing vulnerabilities for the security team to address.
Which tool is Liam using to bypass Lone Star Healthcare's firewall during his penetration test?
A. Metasploit
B. Colasoft Packet Builder
C. Nmap
D. Traffic IQ Professional
Answer: (SHOW ANSWER)
Colasoft Packet Builder is specifically designed for creating and editing custom packets, making it the best match for a scenario where the tester "crafts custom network packets" and "carefully designs their headers" to test or evade firewall filtering. In CEH methodology, packet crafting is a common technique used to validate how filtering devices respond to unusual or borderline traffic patterns, including altered TCP flags, manipulated fragmentation behavior, spoofed fields, and protocol edge cases. A packet builder tool enables precise control over Layer 2 through Layer 4 fields and, in many cases, supports building application payloads as well. This supports testing for weaknesses such as overly permissive rules, inconsistent state handling, improper reassembly, and inadequate normalization that could allow malicious traffic to pass.
Metasploit is primarily an exploitation framework used to deliver payloads and run modules after targets and weaknesses are identified. While it can generate traffic, it is not the most direct tool for low-level, manual header crafting as described. Nmap is mainly used for host discovery, port scanning, service detection, and scripting-based enumeration; it can manipulate some packet characteristics, but its core purpose is not interactive custom packet construction. Traffic IQ Professional is typically associated with network analysis and traffic monitoring rather than crafting bespoke packets to probe firewall rule behavior. Therefore, the tool most aligned with CEH-style custom packet creation for firewall evasion testing is Colasoft Packet Builder.

NEW QUESTION: 38
An attacker analyzes how small changes in plaintext input affect ciphertext output to deduce encryption key patterns in a symmetric algorithm. What technique is being used?
A. Differential cryptanalysis
B. Timing attack
C. Chosen-ciphertext attack
D. Brute-force attack

Answer: A (LEAVE A REPLY)
The CEH Cryptanalysis module describes differential cryptanalysis as an attack that studies the relationship between differences in input and resulting differences in output to recover secret keys.
Option A precisely matches this definition.
Option B relies on execution timing.
Option C requires ciphertext manipulation.
Option D exhaustively tests keys.
CEH lists differential cryptanalysis as a foundational theoretical attack.

NEW QUESTION: 39
A penetration tester identifies malware that monitors the activities of a user and secretly collects personal information, such as login credentials and browsing habits. What type of malware is this?
A. Worm
B. Rootkit
C. Spyware
D. Ransomware
Answer: C (LEAVE A REPLY)
CEH defines spyware as malware designed to covertly observe user behavior and transmit sensitive information to attackers without the victim's knowledge. Spyware commonly records keystrokes, browser activity, form submissions, application usage, and other personally identifiable information. CEH highlights that spyware often operates silently and may disguise itself as legitimate software, making detection difficult.
Unlike rootkits-which hide processes and files-or worms that self-replicate, spyware focuses exclusively on monitoring and data exfiltration. It is frequently installed through phishing, drive-by downloads, browser vulnerabilities, or malicious installers. Spyware can serve as a stepping stone for further system compromise by providing attackers with credentials for privilege escalation, lateral movement, or financial theft. CEH emphasizes the need for endpoint hardening, updated anti-malware engines, and behavioral analysis tools to detect such stealthy monitoring programs.

NEW QUESTION: 40
John, a penetration tester at a Los Angeles-based online gaming company, is analyzing the company's cloud infrastructure after a recent security breach caused unexpected downtime and delayed alerts. His investigation reveals that the attackers remained undetected, due to the absence of mechanisms that track function-level activity and capture anomalous events. The backend architecture for matchmaking and in-game purchases is serverless, increasing the importance of robust security measures.
So, which cloud computing threat should John prioritize to prevent similar breaches?
A. Insufficient logging and monitoring

B. Privilege escalation
C. Loss of governance
D. Side-channel attacks
Answer: (SHOW ANSWER)
Insufficient logging and monitoring is the most direct threat highlighted by the scenario. In CEH-aligned cloud security concepts, visibility is foundational: without adequate telemetry, security teams cannot detect, investigate, or respond to malicious activity in time. The question explicitly states attackers "remained undetected" because the organization lacked mechanisms to track function-level activity and capture anomalous events. In a serverless architecture, this visibility gap can be especially damaging because there are no traditional servers for defenders to log into, and many security signals must be collected from cloud-native sources such as function invocation logs, API gateway logs, identity events, and centralized monitoring pipelines.
While privilege escalation is a common cloud threat, the question's root cause is not described as excessive permissions or role abuse; it is the lack of detection capability. Loss of governance refers to weak policies, mismanaged accounts, and lack of control over cloud resources, which may contribute indirectly but is not the immediate failure described. Side-channel attacks are specialized and do not match the evidence of missed alerts and absent operational telemetry.
CEH guidance emphasizes implementing centralized logging, continuous monitoring, alerting, and anomaly detection as core controls. For serverless, this includes capturing detailed function execution logs, tracing, identity and access events, and integrating them into a SIEM/SOAR workflow. Effective monitoring enables rapid detection of abnormal invocation patterns, suspicious API calls, unusual data access, and persistence attempts-reducing dwell time and preventing small compromises from becoming major outages.

NEW QUESTION: 41
A penetration tester submits altered ciphertexts to a web server and pays close attention to how the server responds. When the server produces different error messages for certain inputs, the tester starts to infer which inputs result in valid internal processing. Which cryptanalytic method is being used in this scenario?
A. Exploit padding error feedback to recover data
B. Compare traffic timing to deduce the key
C. Flip bits randomly to scramble the decryption
D. Inspect randomness across multiple sessions
Answer: (SHOW ANSWER)
Padding oracle attacks exploit systems that reveal differences in error responses when incorrectly padded ciphertext is submitted. CEH explains that these variations allow attackers to iteratively determine valid padding bytes and ultimately decrypt or modify encrypted data without knowledge of the key.

NEW QUESTION: 42
You are Riley, an incident responder at NovaEx Crypto in San Antonio, Texas, tasked with investigating a recent double-spend reported by a retail merchant that accepts the exchange's token. Your telemetry shows that a reseller node used by the merchant received blocks only from a small, fixed set of peers for several hours and accepted a conflicting history that later allowed the attacker to reverse a confirmed payment. The attacker appears to have controlled which peers that node communicated with and supplied it a private chain until they were ready to reveal it. Which blockchain attack does this behavior most closely describe?
A. Finney Attack
B. DeFi Sandwich Attack
C. 51% Attack
D. Eclipse Attack
Answer: D (LEAVE A REPLY)
The behavior described most closely matches an Eclipse attack. In an eclipse attack, an adversary isolates a victim node by controlling its peer connections so that the node communicates only with attacker-controlled (or attacker-influenced) peers. Once isolated, the attacker can feed the victim a manipulated view of the blockchain-such as withholding blocks, delaying transactions, or presenting an alternative chain history.
This can enable downstream impacts like double-spending against merchants who rely on that node's view for confirmation.
The scenario's strongest indicators are:
The node "received blocks only from a small, fixed set of peers for several hours," suggesting abnormal peer diversity and potential isolation.
The attacker "controlled which peers that node communicated with," which is essentially the definition of eclipsing a node.
The node "accepted a conflicting history" and the attacker supplied "a private chain until they were ready to reveal it," consistent with feeding the victim a tailored chain view and then releasing/realigning it to profit from reversed payments.
Why the other options are less fitting:
A Finney attack (A) involves a miner pre-mining a block containing a spend, making a payment to a merchant, and then releasing the pre-mined block to invalidate the merchant's transaction-this doesn't require isolating a specific node's peers for hours.
A DeFi sandwich attack (B) is a mempool/MEV tactic on decentralized exchanges involving front-running and back-running, unrelated to isolating node peer connections or feeding a private chain.
A 51% attack (C) involves controlling a majority of network hash power/stake to rewrite history at network scale. The scenario emphasizes isolation of a particular merchant-related node via peer control rather than majority network control.
Therefore, the attack is best identified as D. Eclipse Attack.

NEW QUESTION: 43
Targeted, logic-based credential guessing using prior intel best describes which technique?
A. Strategic pattern-based input using known logic
B. Exhaustive brute-force testing
C. Shoulder surfing
D. Rule-less hybrid attack
Answer: A (LEAVE A REPLY)
This describes a rule-based or logic-based password attack, which CEH v13 classifies as a smart, targeted guessing technique. Attackers use known patterns-such as naming conventions, dates, or personal interests-to reduce the keyspace and increase success rates.
Option A accurately reflects this methodology. Option B is brute force, which is random and exhaustive.
Option C is physical observation. Option D describes hybrid attacks without structured logic.
CEH v13 emphasizes that pattern-based attacks are highly effective when attackers possess prior intelligence.
Therefore, Option A is correct.

NEW QUESTION: 44
In sunny San Diego, California, security consultant Maya Ortiz is engaged by PacificGrid, a regional utilities provider, to analyze suspicious access patterns on their employee portal. While reviewing authentication logs, Maya notices many accounts each receive only a few login attempts before the attacker moves on to other targets; the attempts reuse a very small set of likely credentials across a large number of accounts and are spread out over several days and IP ranges to avoid triggering automated lockouts. Several low-privilege accounts were successfully accessed before the pattern was detected. Maya prepares a forensic timeline to help PacificGrid contain the incident.
Which attack technique is being used?
A. Session Hijacking
B. Password Spraying
C. Cross-Site Request Forgery (CSRF)
D. Brute Force Attack
Answer: B (LEAVE A REPLY)
The correct answer is B. Password Spraying because the pattern described is the defining behavior of a spraying attack: the attacker tries a small set of common or likely passwords (for example, seasonal passwords, default patterns, or organization-themed guesses) across many different user accounts, using only a few attempts per account to avoid account lockout thresholds. The scenario explicitly states that "many accounts each receive only a few login attempts," the attacker "reuses a very small set of likely credentials

across a large number of accounts," and the activity is "spread out over several days and IP ranges to avoid triggering automated lockouts." These are the exact operational traits that distinguish password spraying from traditional brute force.
In CEH-aligned credential attack concepts, brute force is typically characterized by repeated attempts against a single account (or a small set of accounts), often cycling through many password candidates until the correct one is found. That approach is noisy and quickly triggers lockouts and detection. Password spraying flips the strategy: it keeps the per-account attempt count low and distributes attempts widely and slowly, which reduces alerting and lockout events. This is why the attacker was able to successfully access "several low- privilege accounts" before the pattern was noticed-spraying often compromises accounts with weak or reused passwords while staying below detection thresholds.
Why the other options are incorrect: Session hijacking involves stealing or replaying session tokens/cookies after authentication, not repeated login attempts across accounts. CSRF forces a logged-in user's browser to perform unintended actions; it does not produce distributed authentication failures in logs. Brute force is related, but the avoidance of lockouts through minimal attempts per account and broad targeting is the signature of password spraying.
Therefore, the observed behavior most clearly indicates a password spraying attack.

NEW QUESTION: 45
At Liberty Mutual ' s cybersecurity operations center in Boston, network engineer Marcus is troubleshooting a critical issue during peak transaction hours. Multiple VLANs are experiencing intermittent access delays, and several endpoints including those on isolated VLANs are receiving network traffic not intended for them, raising concerns about data exposure. Marcus notices that the issue began after a newly imaged workstation used by an intern named Lisa was connected to a trunk port in the server room. Switch logs indicate abnormal traffic patterns overwhelming the network.
Which sniffing technique is Lisa ' s workstation most likely using to cause this behavior?
A. DNS Cache Poisoning
B. ARP Poisoning
C. MAC Flooding
D. Switch Port Stealing
Answer: C (LEAVE A REPLY)
The symptoms strongly match MAC flooding, a classic Layer 2 sniffing-related attack discussed in CEH under switch-based network attacks. Ethernet switches maintain a CAM table that maps MAC addresses to physical switch ports. This table allows the switch to forward frames only to the correct destination port, preventing other hosts from seeing traffic not intended for them. In a MAC flooding attack, an attacker generates a very large number of frames with spoofed, random source MAC addresses. The goal is to overflow the switch CAM table so it can no longer reliably store legitimate MAC-to-port mappings.

When the CAM table is full or unstable, many switches fail open by flooding frames out of multiple ports, behaving more like a hub for unknown destinations. That leads to exactly what Marcus observes: devices on segments that should be isolated start receiving traffic they normally would not see, and overall performance degrades due to excessive broadcast-like forwarding. The prompt also mentions "abnormal traffic patterns overwhelming the network," which aligns with the high-volume frame injection required to poison or overflow the CAM table.
ARP poisoning would primarily redirect traffic through the attacker by manipulating IP-to-MAC mappings within a VLAN, but it would not typically cause widespread flooding and generalized delays across multiple VLANs. DNS cache poisoning affects name resolution rather than Layer 2 forwarding behavior. Switch port stealing targets a specific victim MAC entry to redirect that host's traffic, but the widespread flooding and overload indicators are more characteristic of MAC flooding. Therefore, MAC flooding is the most likely technique in this scenario.

NEW QUESTION: 46
In a tense red team exercise at a mid-sized university in Austin, Texas, an ethical hacker named Jake targeted a legacy Linux server in the engineering department. Late one afternoon, he discovered TCP port 2049 was open during his first sweep, suggesting hidden file-sharing capabilities. Intrigued, Jake used a standard utility to request a list of remote file systems shared across the network, aiming to map accessible resources. Meanwhile, he idly checked for Telnet access and probed a time-sync service out of routine, but both proved fruitless on this host.
Which enumeration method is actively demonstrated in this scenario?
A. NFS Enumeration
B. SNMP Enumeration
C. NetBIOS Enumeration
D. NTP Enumeration
Answer: (SHOW ANSWER)
NFS Enumeration is the correct choice because the scenario is centered on TCP port 2049 and the use of a standard utility to list exported remote file systems. In CEH-aligned reconnaissance and enumeration, port
2049 is the primary service port for Network File System NFS. When a tester identifies 2049 as open on a Linux or UNIX-like host, a common next step is to enumerate NFS exports to learn which directories are shared and what access rules apply. The "standard utility" described is consistent with tools such as showmount, which queries the target to retrieve a list of exported file systems and, in some cases, the clients allowed to mount them. This directly supports the stated objective of "requesting a list of remote file systems shared across the network" to map accessible resources.
The distractor checks mentioned in the scenario reinforce why the answer is NFS. Telnet enumeration would relate to TCP 23 and interactive plaintext terminal access, not file-

share exports. NTP enumeration aligns to UDP 123 and focuses on time synchronization information and server behavior, not shared directories. SNMP enumeration typically involves UDP 161 and extracts device and system details via community strings and management information bases. NetBIOS enumeration is associated with Windows networking services such as UDP 137 and TCP 139, which are unrelated to NFS on 2049. Therefore, the active enumeration method demonstrated is NFS enumeration through export listing on TCP port 2049.

NEW QUESTION: 47
A penetration tester is evaluating a web application that does not properly validate the authenticity of HTTP requests. The tester suspects the application is vulnerable to Cross-Site Request Forgery (CSRF). Which approach should the tester use to exploit this vulnerability?
A. Execute a directory traversal attack to access restricted server files
B. Create a malicious website that sends a crafted request on behalf of the user when visited
C. Perform a brute-force attack on the application's login page to guess weak credentials
D. Inject a SQL query into the input fields to perform SQL injection
Answer: (SHOW ANSWER)
CSRF occurs when a vulnerable application processes unauthorized state-changing requests because it does not verify whether the request was intentionally initiated by the authenticated user. CEH v13 explains that exploitation involves tricking a logged-in user into unknowingly executing a crafted HTTP request-usually via a malicious webpage, hidden form submission, embedded image tag, or JavaScript trigger. When the victim visits the attacker-controlled page, the browser automatically includes the user's active session cookies, allowing the server to treat the forged request as legitimate. This technique is central to CSRF attacks and is highlighted in the CEH curriculum as the correct exploitation path. Directory traversal, SQL injection, and brute-force attacks target different vulnerabilities and do not exploit missing request authenticity validation. The key requirement for CSRF exploitation is user interaction via a malicious external resource, making option B the correct CEH-aligned method.

NEW QUESTION: 48
A payload drops a database table by injecting ; DROP TABLE users; --. What SQL injection method was used?
A. Piggybacked queries
B. UNION-based SQL injection
C. Boolean-based SQL injection
D. Error-based SQL injection
Answer: (SHOW ANSWER)
This attack is a classic example of Piggybacked SQL Injection, covered in CEH v13 Web Application Hacking. Piggybacked queries allow attackers to append additional malicious SQL commands to an existing query using a delimiter such as a semicolon.
The payload executes the original query followed by a destructive command (DROP TABLE). UNION-based injections retrieve data, Boolean-based injections infer logic, and error-based injections rely on error messages-not destructive execution.
CEH v13 explicitly describes piggybacked queries as capable of data destruction and privilege escalation, making Option A correct.

NEW QUESTION: 49
At a New York-based e-commerce company preparing for Black Friday sales, analyst Sarah evaluates cloud billing practices. She notices that the provider tracks compute hours, storage usage, and bandwidth consumption in detail, enabling the company to pay only for what is consumed while also supporting audits.
Which cloud computing characteristic best explains this feature?
A. Measured service
B. Broad network access
C. On-demand self-service
D. Resource pooling
Answer: A (LEAVE A REPLY)
The correct answer is A. Measured service because the scenario describes a core cloud characteristic where resource usage is metered, monitored, controlled, and reported, enabling pay-as-you-go billing and supporting accountability and auditability. In CEH cloud computing coverage (aligned with standard cloud definitions), measured service refers to the cloud provider's ability to automatically track and quantify consumption of resources such as CPU/compute time, storage capacity, memory, and network bandwidth. This metering is fundamental to cloud economics: customers pay based on actual usage rather than fixed, up-front infrastructure costs.
In the Black Friday context, demand is bursty and unpredictable. Measured service allows the organization to scale resources up during peak shopping hours and scale down afterward, while billing remains tied to what was truly consumed. This is especially important for cost control in e-commerce environments where overprovisioning for peak loads on-premises would be expensive and inefficient. Additionally, because the provider

records usage in detail, the organization can perform chargeback/showback internally, validate invoices, and maintain evidence for audits and compliance reviews-all of which depend on accurate, granular measurement.
Why the other options are not the best fit: Broad network access describes availability over networks and access via standard mechanisms (not usage tracking). On-demand self-service refers to users provisioning resources automatically without human interaction from the provider (not billing metering). Resource pooling refers to multi-tenant pooling of provider resources dynamically assigned and reassigned according to demand (again, not the billing/audit measurement function).
Therefore, the feature of detailed tracking of compute hours, storage usage, and bandwidth consumption that supports pay-per-use and auditing is best explained by measured service.

NEW QUESTION: 50
During a black-box security assessment of a large enterprise network, the penetration tester scans the internal environment and identifies that TCP port 389 is open on a domain controller. Upon further investigation, the tester runs the ldapsearch utility without providing any authentication credentials and successfully retrieves a list of usernames, email addresses, and departmental affiliations from the LDAP directory. The tester notes that this sensitive information was disclosed without triggering any access control mechanisms or requiring login credentials. Based on this behavior, what type of LDAP access mechanism is most likely being exploited?
A. LDAP over SSL (LDAPS)
B. Authenticated LDAP with Kerberos
C. Anonymous LDAP binding
D. LDAP via RADIUS relay
Answer: (SHOW ANSWER)
CEH reconnaissance and enumeration modules explain that LDAP services often support anonymous binding by default unless explicitly disabled. Anonymous bind allows unauthenticated users to query certain directory attributes, which can lead to disclosure of usernames, organizational hierarchy, and email addresses-critical information for password attacks, phishing campaigns, and privilege escalation planning. In the scenario described, the tester obtained directory data without providing any credentials, demonstrating that anonymous bind permissions were enabled. LDAPS requires TLS encryption and authentication, which contradicts the observed access. Kerberos authentication mandates valid credentials. LDAP via RADIUS is used for authentication integration, not for information disclosure. Since the query was successful with no authentication and no access controls triggered, this aligns exactly with CEH's description of anonymous LDAP binding.

NEW QUESTION: 51

During a UDP service enumeration scan, the tester sees that some ports respond with ICMP Type 3 Code 3 (Port Unreachable), while most remain silent. No firewall or IDS is interfering. What can the tester conclude about the non-responsive ports?

A. The ports are likely closed because no ICMP response was received.

B. The system blocked all probes after rate-limiting was detected.

C. They may be open or filtered, requiring retransmission.

D. They may correspond to some services requiring three-way handshakes.

Answer: C (LEAVE A REPLY)

UDP scanning produces reliable "closed" results only when an ICMP Port Unreachable is returned. Silent responses indicate either open ports (no reply expected) or filtered ports (blocks dropping packets). CEH emphasizes that non-responses require retransmission or alternate verification techniques.

NEW QUESTION: 52

During a red team exercise for a global insurance provider in Chicago, ethical hacker Maria tests the effectiveness of the company ' s endpoint defenses. She launches an attack by injecting malicious PowerShell commands into a trusted process without dropping any executables to disk. The code executes entirely in memory, generating abnormal spikes in resource usage. After a reboot, Maria notes that the system returns to normal and traditional antivirus logs show no evidence of infection.

Which type of malware technique did Maria most likely use in this test?

A. Rootkit

B. Trojan

C. Fileless Malware

D. Ransomware

Answer: C (LEAVE A REPLY)

Maria most likely used fileless malware, because the scenario explicitly describes malicious activity that does not write a payload executable to disk and instead executes entirely in memory using PowerShell and process injection. In CEH-aligned malware classifications, fileless malware is characterized by leveraging legitimate system tools (often called "living off the land" utilities) such as PowerShell, WMI, cmd.exe, or scripting engines to execute attacker-controlled code without creating traditional malware files on the filesystem. Since many legacy antivirus solutions depend heavily on signature-based scanning of files on disk, purely memory- resident execution can reduce or eliminate typical AV detections and leave minimal artifacts in standard AV logs.

The description also mentions that after a reboot the system returns to normal, which strongly supports fileless behavior: if the attacker did not establish persistence (for example via registry run keys, scheduled tasks, services, or WMI event subscriptions), then the in-memory code and injected instructions would be cleared when memory is reset. The "abnormal spikes in resource usage" are consistent with malicious scripts running

inside a trusted process context, where attackers may inject or reflectively load code to blend into normal operating activity and evade straightforward monitoring.
Why the other options are incorrect: a rootkit primarily focuses on stealth through deep system-level hiding (often kernel/driver-level) and is commonly associated with persistent concealment rather than "no disk footprint" PowerShell-only execution. A trojan is typically a malicious program masquerading as legitimate software and usually involves a delivered executable or application. Ransomware is defined by encrypting data and extorting payment, which is not described here.
Thus, the technique most consistent with the test is fileless malware executed via PowerShell and memory- only injection.

NEW QUESTION: 53
You suspect a Man-in-the-Middle (MitM) attack inside the network. Which network activity would help confirm this?
A. Sudden increase in traffic
B. Multiple login attempts from one IP
C. IP addresses resolving to multiple MAC addresses
D. Abnormal DNS request volumes
Answer: C (LEAVE A REPLY)
CEH v13 identifies ARP spoofing/poisoning as a primary MitM technique in local networks. In such attacks, a single IP address maps to multiple MAC addresses, indicating ARP table manipulation.
This anomaly allows attackers to intercept traffic between victims and gateways. Increased traffic or DNS activity may occur but are not definitive indicators. Thus, IP-to-MAC inconsistencies are the most reliable confirmation of MitM activity.

NEW QUESTION: 54
You are an ethical hacker at RedOak Cyber Solutions, contracted to perform a penetration test for MetroHealth Hospital in Cleveland, Ohio. While assessing the hospital's appointment booking portal, you craft and submit multiple malicious inputs into the patient search field. One of your payloads successfully manipulates the backend query, returning additional appointment data that was not intended to be displayed.
Based on the observed behavior, which step of the SQL injection methodology are you performing?
A. Identifying Data Entry Paths
B. Launching SQL Injection Attacks
C. Database Enumeration
D. Information Gathering and Vulnerability Detection
Answer: B (LEAVE A REPLY)
The correct answer is B. Launching SQL Injection Attacks because the scenario describes moving beyond merely locating inputs or detecting error behavior and into actively sending

injection payloads that successfully alter query logic and change returned results. In a typical CEH-aligned SQL injection workflow, testers begin by identifying where user-controlled input enters the application (forms, URL parameters, cookies, headers), then perform basic tests to detect whether inputs affect backend SQL processing. Once a suspected injection point is found, the next step is to launch SQL injection attempts using crafted inputs designed to manipulate the query and demonstrate impact.
In this case, you "craft and submit multiple malicious inputs," and one payload "successfully manipulates the backend query," causing the application to return "additional appointment data that was not intended to be displayed." That outcome is a clear indicator that exploitation is underway: the injection is not hypothetical- it is functioning and changing the application's behavior in a way that reveals unauthorized data. This is characteristic of executing an SQL injection attack (in-band exploitation), such as using boolean logic manipulation (e.g., conditions that expand result sets) or other query-altering techniques. The emphasis is on the successful manipulation and unauthorized data exposure, which aligns with the attack execution phase.
Why the other options are less correct: Identifying Data Entry Paths would be earlier, when you locate the patient search field as a candidate parameter. Information Gathering and Vulnerability Detection generally refers to discovering and confirming the presence of weaknesses (often via initial probes, errors, or abnormal responses) rather than a confirmed payload that already returns unauthorized data. Database Enumeration is typically the follow-on step once exploitation is confirmed, where the tester extracts metadata such as database names, tables, columns, users, and versions. Here, you are demonstrating the injection's ability to retrieve extra records, which is the exploitation/attack-launch stage, not full enumeration yet.
Therefore, the step being performed is Launching SQL Injection Attacks.

NEW QUESTION: 55
A penetration tester detects malware on a system that secretly records all keystrokes entered by the user. What type of malware is this?
A. Rootkit
B. Ransomware
C. Keylogger
D. Worm
Answer: C (LEAVE A REPLY)
CEH v13 explains that a keylogger is a type of spyware designed to capture user input covertly, often storing or transmitting captured data-such as passwords, emails, chat messages, and financial information-to an attacker. Keyloggers can be implemented as software, firmware, or hardware, and they operate silently in the background without affecting system performance, making them ideal for credential theft. CEH categorizes keyloggers under spying and monitoring malware frequently used in the System Hacking phase to escalate privileges or move laterally once credentials are harvested. Unlike

rootkits, which hide processes, or ransomware, which encrypts files, a keylogger's main purpose is passive surveillance. CEH emphasizes how attackers deploy keyloggers post-compromise or use phishing/social engineering to trick victims into installing them. Their covert nature and ability to bypass traditional AV solutions by masquerading as legitimate processes make identifying them crucial during forensics and incident response activities.

NEW QUESTION: 56
You are Ava Mitchell, an ethical hacker at Sentinel Cyberworks, hired to test the wireless defenses of Horizon Financial, a bank in Boston, Massachusetts. During a covert night-time assessment, your objective is to simulate an attacker attempting to breach the bank's WPA-protected Wi-Fi network. You deploy a tool that allows you to capture wireless packets, send de-authentication packets to force client reconnections, and attempt to recover the encryption key, all within a single graphical interface. Based on the described functionality, which Wi-Fi security auditing tool are you using?
A. Fern WiFi Cracker
B. RFProtect
C. Cisco Adaptive Wireless IPS
D. WatchGuard Wi-Fi Cloud WIPS
Answer: A (LEAVE A REPLY)
The tool described matches Fern WiFi Cracker because CEH wireless assessment workflows commonly reference GUI-based auditing utilities that combine packet capture, wireless injection support, and key recovery attempts in one interface. The scenario specifically mentions three core capabilities: capturing wireless packets, sending de-authentication frames to trigger client reconnects, and attempting to recover the encryption key. Those steps align with the typical WPA cracking methodology discussed in CEH learning paths: capture the WPA handshake when a client connects, optionally force a reconnection by sending de- authentication frames, then perform an offline attack against the captured handshake using a wordlist or brute- force approach. Fern WiFi Cracker is known for presenting these functions through a graphical interface, making it a common example of an "all-in-one" Wi-Fi auditing tool.
The other options are defensive monitoring and prevention platforms, not offensive auditing tools used to actively deauthenticate clients or attempt key recovery. RFProtect, Cisco Adaptive Wireless IPS, and WatchGuard Wi-Fi Cloud WIPS are Wireless Intrusion Prevention and Monitoring solutions designed to detect rogue access points, identify attacks such as deauthentication floods, enforce wireless security policies, and generate alerts for security teams. They are used to stop or respond to attacks rather than conduct packet capture plus key-recovery attempts as part of an assessment.
Because the question emphasizes a single graphical interface that captures traffic, injects deauth frames, and attempts key recovery, the correct match among the choices is Fern WiFi Cracker.

NEW QUESTION: 57
In the humid air of Houston, Texas, a chemical plant is preparing to deploy a new production automation module. As part of a red team engagement, you, Ethan Brooks, a cybersecurity specialist are tasked with identifying industrial control devices that communicate with SCADA systems. To proactively uncover devices that may expose critical functions, you launch a focused Nmap sweep targeting TCP port 102, known to be associated with industrial controllers used in critical infrastructure. Your scan detects specific PLC models used in the automation process. What OT reconnaissance step are you performing?
A. Scanning Omron PLC devices
B. Scanning Modbus devices
C. Capturing Modbus TCP traffic using Wireshark
D. Scanning Siemens SIMATIC S7 PLCs
Answer: D (LEAVE A REPLY)
TCP port 102 is strongly associated with Siemens S7 communications, commonly referred to as S7comm, which is used by Siemens SIMATIC S7 PLC families and related engineering and HMI components in OT environments. In CEH coverage of ICS and SCADA reconnaissance, identifying industrial protocols by their well-known ports is a standard first step because it quickly narrows down device type, vendor ecosystem, and likely attack surface. When Ethan targets TCP 102 and the scan reveals PLC models used in the automation process, that aligns directly with enumerating Siemens SIMATIC S7 PLCs, since S7comm typically operates over ISO-on-TCP on port 102.
The other options do not match the port-protocol pairing described. Modbus TCP most commonly uses TCP port 502, so "scanning Modbus devices" would be associated with 502 rather than 102. "Capturing Modbus TCP traffic using Wireshark" is passive sniffing and also would focus on Modbus traffic patterns on 502, not an active Nmap sweep on 102. Omron PLCs may use different protocols and ports depending on model and configuration, but TCP 102 is the canonical indicator for Siemens S7 in most defensive and offensive playbooks taught for OT discovery.
From a defensive perspective, CEH-aligned best practices emphasize segmenting OT networks, restricting access to engineering ports like 102, monitoring for scanning behavior, and enforcing allowlisted communications between SCADA, HMIs, and PLCs to reduce the risk of unauthorized enumeration and follow-on manipulation.

NEW QUESTION: 58
At Norwest Freight Services, Simon, a junior analyst, is tasked with running a vulnerability scan on several departmental servers. This time, he is provided with administrator-level credentials to input into the scanner.
The scan takes significantly longer than usual but returns detailed results, including weak registry permissions, outdated patches, and insecure configuration files that would not

have been visible to an outsider. SIEM logs confirm that successful logins occurred during the scanning process.
Which type of vulnerability scan best explains the behavior observed in Simon's assessment?
A. External Scanning
B. Credentialed Scanning
C. Internal Scanning
D. Non-Credentialed Scanning
Answer: B (LEAVE A REPLY)
This is best explained by credentialed scanning because the scanner is given administrator-level credentials, and the SIEM confirms successful logins occurred during the scan. Credentialed scans authenticate to the target systems (via SMB/WMI/WinRM for Windows, SSH for Linux/Unix, APIs for certain platforms) and then perform deeper inspection from an "inside" perspective. That allows the scanner to enumerate details that are not reliably visible from unauthenticated network probing-such as installed patch levels, local security policy settings, registry permissions, configuration files, running services with their exact versions, and misconfigurations that require local access to verify.
The scenario's outcomes strongly match this: the scan takes significantly longer, which is common because authenticated checks involve logging in and performing many local queries; the results include weak registry permissions, outdated patches, and insecure configuration files, all of which typically require authenticated access to assess comprehensively. In addition, credentialed scanning reduces false positives and improves accuracy, because it can confirm vulnerability conditions directly rather than inferring from banners or open ports.
Why the other options are less accurate:
Non-credentialed scanning (D) is performed from an external perspective without logins; it would not normally retrieve detailed registry/config file permission findings, and SIEM logs would not show successful authentication events caused by the scanner.
External scanning (A) describes the scan's network location (outside the organization) rather than the authentication mode. You can do external credentialed scans, but the defining feature here is authenticated logins and deep host checks.
Internal scanning (C) also refers to where the scan originates. While the scan might be internal, the question's key differentiator is that admin credentials were used to log in and gather detailed local information.
Therefore, the scan type is B. Credentialed Scanning.

NEW QUESTION: 59
At a Miami-based cryptocurrency exchange, investigator Jake uncovers that attackers exploited exposed API keys to issue unauthorized cloud commands, leading to resource abuse and lateral movement inside the cloud environment. Which cloud hacking technique is most directly demonstrated in this incident?

A. Cryptojacking
B. Enumerating S3 buckets
C. Wrapping attack
D. Compromising secrets
Answer: (SHOW ANSWER)
The most direct technique demonstrated is D. Compromising secrets, because the attackers abused exposed API keys to authenticate to the cloud provider and execute unauthorized cloud commands. In CEH-aligned cloud attack paths, "secrets" commonly include API keys, access tokens, secret keys, passwords, certificates, and service account credentials. When these secrets are exposed (for example, hard-coded in source code, leaked in public repositories, stored insecurely in endpoints, or logged accidentally), an attacker can use them to gain the same privileges as the legitimate account or service identity.
Once valid API keys are obtained, attackers typically perform actions consistent with the compromised identity's permissions: spinning up compute, modifying IAM policies, accessing storage, disabling logging, creating new credentials, and pivoting across services. The incident description mentions both resource abuse and lateral movement. Resource abuse is a frequent consequence of stolen cloud credentials because attackers can provision infrastructure on the victim's account (often for botnets, staging, or other activities). Lateral movement inside the cloud environment can happen when the compromised keys grant access to additional services or when the attacker uses the initial foothold to discover and access other roles, instances, or secrets (for example, by querying metadata services, reading configuration stores, or enumerating IAM privileges).
Why the other options are less accurate: Cryptojacking specifically refers to illicit cryptocurrency mining using hijacked resources; while "resource abuse" could include mining, the key distinguishing factor in the question is the use of exposed API keys to issue commands, which is fundamentally credential/secret compromise. Enumerating S3 buckets is a reconnaissance activity focused on object storage discovery and misconfigurations, not the central mechanism here. A wrapping attack relates to specific cloud/identity token wrapping scenarios and is not indicated by exposed API keys.
Therefore, the incident most clearly demonstrates compromising secrets (exposed API keys).

NEW QUESTION: 60
Which approach should an ethical hacker avoid to maintain passive reconnaissance?
A. Direct interaction with the threat actor
B. WHOIS and DNS lookups
C. Anonymous browsing via Tor
D. Using the Wayback Machine
Answer: A (LEAVE A REPLY)

CEH v13 defines passive reconnaissance as information gathering without interacting directly with the target or alerting them. The goal is to remain undetected while collecting intelligence from publicly available sources.
Directly interacting with a threat actor on forums-even under a pseudonym-constitutes active engagement
. CEH v13 warns that such interaction risks exposure, attribution, and legal complications. It can alert the adversary, cause them to alter behavior, or even retaliate.
WHOIS lookups, DNS queries, archived web content, and anonymous browsing are all passive techniques endorsed in CEH v13. These methods do not notify the target and leave minimal trace.
Thus, Option A should be avoided to maintain a low profile.

NEW QUESTION: 61
You are an ethical hacker at Apex Security Consulting, hired by Riverfront Media, a digital marketing firm in Boston, Massachusetts, to assess the security of their customer relationship management CRM web application. While evaluating the application's search feature, you input a long string of single quote characters into the search bar. The application responds with an error message suggesting that it cannot handle the length or structure of the input in the current SQL context. Based on the observed behavior, which SQL injection vulnerability detection technique are you employing?
A. Detecting SQL Modification
B. Fuzz Testing
C. Function Testing
D. Error Message Analysis
Answer: D (LEAVE A REPLY)
The technique being used is Error Message Analysis, because the tester is intentionally supplying a special character payload and then interpreting the application's returned database or SQL parsing error to infer the presence of an injection point. In CEH-aligned SQL injection methodology, one of the earliest indicators of SQL injection is when crafted input causes the application to generate a database error, such as syntax errors, unclosed quotation marks, type conversion failures, or context-related messages that reveal how the input is being embedded into a query. A long series of single quotes is a classic trigger: if user input is concatenated into a SQL statement without proper sanitization or parameterization, the quotes can break the query structure and force the database engine or ORM layer to throw an error that exposes the query context.
The scenario explicitly states the response is an error message indicating the application cannot handle the input "in the current SQL context." That means the application is leaking information through error responses, which CEH highlights as both a detection opportunity for testers and a security weakness because detailed errors can guide attackers toward successful payload construction.

This is not primarily "Detecting SQL Modification," which focuses on confirming changes in query logic or results, often using boolean-based techniques. It is not "Function Testing," which validates application functions rather than probing input handling at the SQL layer. While the input resembles fuzzing, fuzz testing is broader and does not specifically depend on interpreting SQL error messages as the detection signal. Here, the decisive evidence is the SQL-context error returned, making Error Message Analysis the correct technique.

NEW QUESTION: 62
Customer data in a cloud environment was exposed due to an unknown vulnerability. What is the most likely cause?
A. Misconfigured security groups
B. Brute force attack
C. DoS attack
D. Side-channel attack
Answer: A (LEAVE A REPLY)
CEH v13 identifies misconfigured cloud security groups as the leading cause of cloud data exposure. Open ports, public storage buckets, and overly permissive firewall rules frequently expose sensitive data.
Brute force and DoS do not directly expose stored data, and side-channel attacks are rare and advanced.

NEW QUESTION: 63
At a Chicago-based healthcare provider, security engineer Emily reviews the migration of critical applications to a cloud service. During her evaluation, she notes that administrators can provision new servers, increase storage, and expand compute power instantly through a web dashboard without any manual involvement from the cloud provider. Which NIST-defined characteristic of cloud computing best explains this capability?
A. On-demand self-service
B. Measured service
C. Resource pooling
D. Broad network access
Answer: (SHOW ANSWER)

The capability described-administrators instantly provisioning servers, storage, and compute through a web portal without needing the provider to manually intervene-is the NIST cloud characteristic called on-demand self-service. In NIST's cloud computing model, on-demand self-service means a consumer can unilaterally provision computing capabilities (such as server time and network storage) as needed automatically, without requiring human interaction with each service provider.
The scenario explicitly highlights that the admins can scale resources "instantly" through a dashboard and that there is "no manual involvement from the cloud provider." That is exactly what on-demand self-service captures: rapid provisioning driven by the customer through automated orchestration and APIs/portals.
Why the other options are not the best match:
Broad network access (D) means cloud capabilities are available over the network and accessed through standard mechanisms by heterogeneous platforms (mobile, laptops, workstations). While the dashboard is accessed over the network, broad access is about reachability and standard access mechanisms, not the self- provisioning behavior.
Resource pooling (C) refers to the provider's multi-tenant model where physical/virtual resources are pooled and dynamically assigned; it explains how the provider can offer elasticity, but the user-facing "provision it yourself" aspect is on-demand self-service.
Measured service (B) refers to metering and monitoring resource usage for billing/optimization; it doesn't explain instant self-provisioning.
Therefore, the characteristic is A. On-demand self-service.

NEW QUESTION: 64
A penetration tester alters the "file" parameter in a web application (e.g., view?
file=report.txt) to ../../../../etc
/passwd and successfully accesses restricted system files. What attack method does this scenario illustrate?
A. Conduct a brute-force attack to obtain administrative credentials
B. Use directory traversal sequences in URL parameters to retrieve unauthorized system content
C. Inject malicious scripts into web pages to manipulate content via XSS vulnerabilities
D. Exploit buffer overflow issues by injecting oversized data in HTTP request headers
Answer: B (LEAVE A REPLY)
CEH v13 explains that directory traversal (also called path traversal) occurs when an application improperly handles user-supplied input used for file path generation. Attackers exploit this by inserting traversal sequences such as ../ beyond the intended directories, gaining access to sensitive files like /etc/passwd, configuration data, or source code. The vulnerability arises from missing input validation and failure to restrict file access to safe directories. CEH stresses that directory traversal is common in file handling functions such as view, download, or include operations. Brute-forcing credentials (Option A) is unrelated.

XSS (Option C) targets script injection into web pages, not file access. Buffer overflow (Option D) manipulates memory, not file paths. Therefore, the scenario represents classic directory traversal exploitation.

NEW QUESTION: 65
A penetration tester needs to map open ports on a target network without triggering the organization's intrusion detection systems (IDS), which are configured to detect standard scanning patterns and abnormal traffic volumes. To achieve this, the tester decides to use a method that leverages a third-party host to obscure the origin of the scan. Which scanning technique should be employed to accomplish this stealthily?
A. Conduct a TCP FIN scan with randomized port sequences
B. Perform a TCP SYN scan using slow-timing options
C. Execute a UDP scan with packet fragmentation
D. Use an Idle scan by exploiting a "zombie" host
Answer: D (LEAVE A REPLY)
CEH v13 identifies the Idle Scan as one of the most stealthy and advanced reconnaissance techniques due to its ability to avoid generating any traffic directly between the attacker and the target. Using a "zombie host," which has predictable IP ID sequencing, the attacker forges packets so that all scan traffic appears to originate from the zombie. The IDS sees communication only between the zombie and the target, not the attacker. This allows evasion of network monitoring tools, traffic correlation systems, and intrusion detection signatures.
CEH highlights Idle Scanning as a core technique for bypassing sophisticated detection controls because it leaves no direct fingerprint of the attacker. Options A and B still originate from the attacker's IP. Option C can evade some filters but remains detectable due to packet anomalies. Only Idle Scanning provides full origin obfuscation, making it the most appropriate method for stealth port enumeration.

NEW QUESTION: 66
A biotech research firm in Boston, Massachusetts, migrates its laboratory management platform to the cloud.
The vendor provides an environment where developers can deploy and test custom applications without managing the underlying servers, operating systems, or storage. The firm controls the application logic but not the runtime infrastructure.
Which cloud service model is the company using?
A. Infrastructure as a Service (IaaS)
B. Platform as a Service (PaaS)
C. Software as a Service (SaaS)
D. Anything as a Service (XaaS)
Answer: (SHOW ANSWER)

This scenario describes Platform as a Service (PaaS) because the provider delivers a managed platform where developers can deploy and run custom applications while the provider manages the underlying infrastructure components-servers, operating systems, storage, and often middleware/runtime components. The customer is responsible for application code and logic (and usually data and application configuration), but not for provisioning or maintaining the base compute and OS layers.
The key phrasing is: "developers can deploy and test custom applications without managing the underlying servers, operating systems, or storage," and "the firm controls the application logic but not the runtime infrastructure." That is the hallmark responsibility split of PaaS: the provider handles infrastructure and platform operations, enabling rapid development and deployment through managed runtimes, build/deploy pipelines, and scalable services.
Why the other models don't fit:
IaaS (A) would require the customer to manage the OS and many platform components (patching, runtime configuration, middleware), even though the provider supplies the virtualized infrastructure. The scenario explicitly says they do not manage OS or servers.
SaaS (C) provides a complete finished application that the customer uses; customers typically cannot deploy their own custom application logic onto it in the way described.
XaaS (D) is a broad umbrella term, not the specific NIST-style service model classification being asked.
Therefore, the correct answer is B. Platform as a Service (PaaS).

NEW QUESTION: 67
Javier Ruiz from CyberFortress Solutions is tasked with auditing the mobile security practices of Apex Financial Services, a financial firm in Houston, Texas. During a covert penetration test, Javier targets employees' personal smartphones used to access corporate financial systems. He exploits a vulnerability by installing a malicious app that bypasses access controls, granting him unauthorized entry to sensitive financial data because the devices lack a specific security measure to restrict app access. Based on this vulnerability, which BYOD security guideline is most likely missing in Apex Financial Services' policy?
A. Review permissions requested by apps before installing them
B. Set passwords for apps to restrict others from accessing them
C. Enforce automatic device locking or implement biometric authentication
D. Use encryption mechanisms to store data
Answer: A (LEAVE A REPLY)
The most likely missing BYOD guideline is reviewing application permissions before installation. In CEH mobile security guidance, a major risk in BYOD environments is the introduction of untrusted or malicious applications that abuse the mobile permission model to access corporate data, intercept authentication tokens, read storage, capture keystrokes via accessibility services, or communicate externally. When users install apps without

scrutinizing requested permissions, they may unknowingly grant excessive privileges that enable data theft or access-control bypass, especially if the app leverages OS weaknesses or misconfigurations.
The scenario states Javier "installs a malicious app that bypasses access controls" and gains access to sensitive financial data because devices "lack a specific security measure to restrict app access." This maps directly to a policy gap around controlling and validating apps and their permission requests. CEH emphasizes that organizations should reduce attack surface by limiting app privileges, avoiding sideloading from untrusted sources, and enforcing least privilege through user awareness and enterprise controls such as MDM application allowlisting and permission governance. Reviewing permissions is the user-facing guideline that prevents employees from granting dangerous access (for example, SMS, storage, contacts, accessibility, device admin, or VPN configuration permissions) that can enable credential theft or unauthorized data access.
Option B adds an extra layer for local access but does not stop a malicious app with granted permissions from accessing corporate data. Option C helps if a device is physically stolen, but it does not prevent malicious apps already running under the user context. Option D protects data at rest, yet a malicious app can still exfiltrate data once it is decrypted and accessed by the user session. Therefore, permission review is the most directly relevant missing BYOD guideline.

NEW QUESTION: 68
An attacker exploits legacy protocols to perform advanced sniffing. Which technique is the most difficult to detect and neutralize?
A. HTTP header overflow extraction
B. SMTP steganographic payloads
C. Covert channel via Modbus protocol manipulation
D. X.25 packet fragmentation
Answer: (SHOW ANSWER)
CEH v13 identifies covert channels in legacy industrial protocols as among the hardest sniffing techniques to detect. Modbus, widely used in OT and ICS environments, lacks authentication and encryption, making it ideal for covert communication.
Attackers can manipulate function codes and payload timing to exfiltrate data without triggering traditional IDS signatures. CEH v13 highlights that OT protocols often bypass deep inspection tools, making covert channels extremely stealthy.
Other options are less realistic or less persistent in modern enterprise environments.

NEW QUESTION: 69
In Denver, Colorado, ethical hacker Sophia Nguyen is hired by Rocky Mountain Insurance to assess the effectiveness of their network security controls. During her penetration test, she attempts to evade the company's firewall by fragmenting malicious packets to avoid detection. The IT team, aware of such techniques, has implemented a security measure to

analyze packet contents beyond standard headers. Sophia's efforts are thwarted as the system identifies and blocks her fragmented packets.
Which security measure is the IT team most likely using to counter Sophia's firewall evasion attempt?
A. Deep Packet Inspection
B. Anomaly-Based Detection
C. Signature-Based Detection
D. Stateful Packet Inspection
Answer: D (LEAVE A REPLY)
Fragmentation is a well-known firewall and IDS evasion technique covered in CEH materials. The attacker breaks a malicious packet into smaller IP fragments so that simple filtering devices, especially those relying mainly on basic header checks or stateless rules, may fail to reconstruct the original payload and therefore miss the malicious content. To counter this, defenses must track packet state and perform reassembly or validation of fragmented traffic so the security control can evaluate the complete communication stream rather than isolated fragments.
Stateful Packet Inspection is the control most aligned with this requirement. A stateful inspection firewall maintains a state table of active connections and monitors traffic as part of an ongoing session. Because it tracks session context, it can handle fragmented packets more effectively by correlating fragments to the original flow and applying policy after reconstructing or normalizing traffic. In CEH-aligned descriptions, this directly reduces the effectiveness of fragmentation-based evasion, overlapping with the concept of traffic normalization that removes ambiguity attackers try to exploit.
Deep Packet Inspection examines payload beyond headers, but the key success factor in stopping fragmentation evasion is state tracking and reassembly, which is characteristic of stateful inspection and state- aware security devices. Signature-based and anomaly-based detection can help detect malicious patterns or unusual behavior, but without reliable reassembly and session context, fragmented payloads may not match signatures and may appear benign in isolation. Therefore, the most likely measure used to identify and block fragmented packets in this scenario is Stateful Packet Inspection.

NEW QUESTION: 70
During a red team exercise at Apex Logistics in Denver, ethical hacker Rachel launches controlled packet injection attacks to simulate session hijacking attempts. The client ' s IT team wants a way to automatically detect such abnormal behaviors across the network in real time, instead of relying on manual analysis. They decide to deploy a monitoring system capable of flagging suspicious session activity based on predefined rules and traffic signatures.
Which detection method best fits the IT team ' s requirement?
A. Check for predictable session tokens
B. Perform manual packet analysis using sniffing tools

C. Monitor for ACK storms
D. Use an Intrusion Detection System (IDS)
Answer: (SHOW ANSWER)
The IT team's requirement is automatic, real-time detection of abnormal session activity using predefined rules and traffic signatures. That description aligns most directly with an Intrusion Detection System (IDS), particularly a network IDS (NIDS) that monitors traffic, compares it to known patterns (signatures) and/or behavioral rules, and generates alerts when suspicious activity is detected. Session hijacking attempts often produce recognizable anomalies-unexpected packet sequences, suspicious flags, unusual injection patterns, resets, or protocol misuse-that IDS rules can be designed to detect across many hosts and segments without requiring an analyst to manually inspect each capture.
The scenario explicitly contrasts this desired capability with "manual analysis," which rules out option B.
Tools like packet sniffers are valuable for investigation and confirmation, but they do not provide organization-wide automated alerting by themselves. An IDS is built for continuous monitoring and alert generation, making it appropriate for detecting red-team-simulated packet injection and session manipulation attempts.
Why the other options are less suitable:
Checking for predictable session tokens (A) is an application-layer defensive review (and a good hardening practice), but it does not automatically detect packet injection behaviors occurring on the network in real time.
Monitoring for ACK storms (C) can be one specific indicator in some TCP manipulation or desynchronization scenarios, but it is too narrow and does not represent a general detection system. The requirement is broader: a monitoring system that flags suspicious session activity using rules and signatures-an IDS fits that role.
Manual packet analysis (B) is explicitly what they want to avoid.
Therefore, the correct answer is D. Use an Intrusion Detection System (IDS).

NEW QUESTION: 71
Lily, a network security analyst at a regional healthcare provider, is preparing defenses ahead of a scheduled external vulnerability assessment. During internal simulation drills, she observes that scanners are successfully identifying open ports and service banners across critical systems. Tasked with reducing exposure to such reconnaissance efforts, Lily is instructed to apply measures that specifically hinder port scanning activity without disrupting legitimate traffic.
Which of the following actions should Lily implement?
A. Block unwanted services running on the ports and update the service versions
B. CConfiguring firewall and IDS rules to detect and block probes is the most direct and CEH-aligned countermeasure for hindering port scanning while preserving legitimate traffic. Port scans typically generate recognizable patterns such as many connection attempts across multiple ports in a short time window, repeated SYN packets, abnormal

TCP flag combinations, or sequential targeting of hosts and ports. An IDS or IPS can detect these behaviors using thresholds and signatures and then alert or actively block the scanning source through shunning, dynamic ACL updates, or automated firewall integration. This approach focuses on stopping the reconnaissance activity itself, rather than only addressing the symptoms after exposure has already occurred.Option B is partially valid because blocking unwanted ports at the firewall reduces the attack surface, but it is primarily hardening and exposure reduction. It does not necessarily hinder scanning behavior, and overly broad filtering can unintentionally block legitimate services if not carefully scoped. Option A improves security by removing unnecessary services and patching, but scanning can still occur and banners may still be collected from required services. Option D is not appropriate because blocking ICMP type 3 unreachable messages can interfere with normal network operations, troubleshooting, and path MTU discovery, and it does not reliably stop modern scanning techniques that use TCP-based probing.
Therefore, the best action specifically aimed at disrupting port scanning activity with minimal impact on legitimate traffic is tuning firewall and IDS controls to detect and block scan probes.
C. Configure firewall and IDS rules to detect and block probes
D. Use a custom rule set to lock down the network, block unwanted ports at the firewall, and filter specific ports
E. Block inbound ICMP message types and all outbound ICMP type 3 unreachable messages
Answer: A,B,C,D,E (LEAVE A REPLY)

NEW QUESTION: 72
Which technique is least useful during passive reconnaissance?
A. WHOIS lookup
B. Search engines
C. Social media monitoring
D. Nmap scanning
Answer: D (LEAVE A REPLY)
Passive reconnaissance involves gathering information without directly interacting with the target. WHOIS, search engines, and social media are all passive techniques highlighted in CEH v13 Reconnaissance.
Nmap scanning, however, actively probes target systems and generates traffic that can be logged and detected.
This makes it an active reconnaissance technique.
Therefore, Option D is least useful in a passive phase.

NEW QUESTION: 73

In Atlanta, Georgia, ethical hacker James Patel is hired by Southern Retail, a major e-commerce chain, to test the security of their online shopping platform. During his penetration test, James aims to simulate a session hijacking attack by setting up a proxy to intercept HTTP traffic between customers and the platform, log the requests, and perform advanced searches on the captured data to identify session tokens. He needs a lightweight tool specifically designed for security research that can handle these tasks in a controlled environment to demonstrate vulnerabilities to the company ' s security team.
Which tool should James use to perform this session hijacking simulation?
A. Caido
B. Hetty
C. Bettercap
D. Wireshark
Answer: A (LEAVE A REPLY)
The best choice is Caido because the scenario describes a web-focused interception proxy workflow:
intercepting HTTP traffic, logging requests, and performing advanced searches to identify session tokens. In CEH-aligned web application testing methodology, session hijacking simulations commonly rely on an intercepting proxy to observe and manipulate application-layer requests and responses, extract session identifiers from cookies or headers, and demonstrate how weak session management can lead to account compromise. A lightweight security research proxy that captures traffic and supports fast filtering and searching across requests fits this exact need. Caido is designed as a modern web security toolkit centered around an interception proxy, allowing testers to capture browser-to-server traffic, inspect headers and cookies, and quickly search through recorded traffic for patterns such as session IDs, authentication cookies, bearer tokens, or predictable parameters.
The other tools are less aligned with the described requirements. Wireshark is a powerful packet analyzer, but it operates primarily at the packet level and is not optimized for web-app testing workflows such as organized request history, token-focused searching, and convenient HTTP manipulation. Bettercap is primarily a network MITM and exploitation framework; while it can intercept traffic, it is not the typical choice for controlled web proxy testing and detailed HTTP request analysis in the way described. Hetty is an HTTP toolkit, but the question's emphasis on a lightweight, security-research proxy with strong captured-data searching and request logging aligns more closely with Caido's purpose-built approach for web application assessments and session token discovery.
'

NEW QUESTION: 74
In a security assessment conducted in New York, Sarah, an ethical hacker, is evaluating a corporate network to enhance its protection against potential threats. She aims to gather essential data about available access points to guide her analysis. Which scanning

technique should Sarah apply to meet this objective while adhering to the organization's ethical guidelines?

A. Vulnerability Scanning

B. Port Scanning

C. Topology Mapping

D. Network Scanning

Answer: B (LEAVE A REPLY)

Port scanning is the CEH-aligned technique used to identify available access points into systems, where

"access points" refers to open TCP and UDP ports and the services listening on them. In the reconnaissance and scanning phases described in CEH methodology, testers first enumerate live hosts and then perform port scanning to discover which network services are reachable, such as HTTP on 80 or 443, SSH on 22, RDP on

3389, DNS on 53, and many others. This information directly guides the next steps of analysis by revealing the attack surface: what services are exposed, which systems are running them, and which ports may permit remote interaction.

Vulnerability scanning is different because it attempts to identify known weaknesses or misconfigurations and typically requires service detection, versioning, and signature or configuration checks. It is usually performed after ports and services are discovered, not as the first method for finding "available access points." Topology mapping focuses on understanding how the network is structured, including routing paths, device relationships, and segmentation boundaries. Network scanning is a broader term that can include host discovery and other probes, but it is less precise than port scanning for identifying the specific entry points that an attacker could use to connect.

Under ethical guidelines, port scanning is conducted with proper authorization, scoped targets, controlled timing to avoid disruption, and clear reporting of open ports, detected services, and risk implications so defenders can reduce exposure by closing unnecessary ports and hardening required services.

NEW QUESTION: 75

During a penetration test at IntelliCore Systems in Raleigh, North Carolina, ethical hacker Javier directs a wave of repetitive web requests against the company ' s portal that overloads backend scripts which process search queries and form submissions. As a result, legitimate customers experience long delays and occasional timeouts while attempting to log in or complete transactions.

Which DoS/DDoS technique is Javier most likely demonstrating?

A. Slowloris

B. UDP Flood

C. Peer-to-Peer Attack

D. HTTP GET/POST Attack

Answer: D (LEAVE A REPLY)

The scenario describes a Layer 7 (application-layer) denial-of-service pattern: Javier sends a wave of repetitive web requests that specifically overload backend scripts responsible for search queries and form submissions. This is characteristic of an HTTP GET/POST attack, where the attacker floods a web application with large volumes of HTTP requests- commonly GET requests for pages/resources and POST requests that trigger server-side processing (login, checkout, searches, form handlers). Because these requests can be syntactically valid and target costly operations, they can quickly exhaust CPU, memory, threads, database connections, or application worker pools, resulting in slow responses and timeouts for legitimate users- exactly what the customers experience here.
Why the other options don't fit as well:
Slowloris (A) is also an application-layer technique, but it works differently: it holds many connections open by sending partial HTTP headers very slowly, aiming to exhaust the server's concurrent connection capacity.
The question emphasizes repetitive requests overloading backend scripts, not slow, incomplete requests holding sockets open.
UDP Flood (B) is a network/transport-layer volumetric attack that sends massive UDP packets to random or targeted ports, consuming bandwidth and host resources. It doesn't specifically target web scripts handling search/forms.
Peer-to-Peer Attack (C) typically involves abusing P2P networks or reflection/amplification through distributed peers; it's not described as direct repetitive web requests to application endpoints.
The key indicators are: (1) web requests (2) targeting script-driven functions like search and form submissions, and (3) resulting in user-facing slowness/timeouts due to overwhelmed application processing.
These align most directly with D. HTTP GET/POST Attack.

NEW QUESTION: 76
A malware analyst finds JavaScript and /OpenAction keywords in a suspicious PDF using pdfid. What should be the next step to assess the potential impact?
A. Upload the file to VirusTotal
B. Extract and analyze stream objects using PDFStreamDumper
C. Compute file hashes for signature matching
Answer: (SHOW ANSWER)
CEH's Malware Analysis module outlines a structured approach:
* Identify suspicious indicators (e.g., JavaScript, OpenAction)
* Extract and analyze embedded objects
* Determine behavior and exploit logic
PDFStreamDumper allows analysts to extract JavaScript code and embedded objects for detailed inspection.
Option B is correct.
Option A is useful but insufficient for deep analysis.

Option C only aids identification, not behavior understanding.

NEW QUESTION: 77
Multiple internal workstations and IoT devices are compromised and transmitting large volumes of traffic to numerous external targets under botnet control. Which type of denial-of-service attack best describes this situation?
A. An attack where compromised internal devices participate in a botnet and flood external targets
B. An attack relying on spoofed IP addresses to trick external servers
C. A direct botnet flood without spoofing intermediary services
D. An internal amplification attack using spoofed DNS responses
Answer: (SHOW ANSWER)
This scenario represents a Botnet-Based Distributed Denial-of-Service (DDoS) attack, as described in CEH v13 Network Attacks. Compromised internal devices become part of a botnet and are used to launch attacks against external targets.
CEH v13 notes that botnets frequently include IoT devices and employee workstations, making insider- originated DDoS activity a serious concern.

NEW QUESTION: 78
In the rainy streets of Portland, Oregon, ethical hacker Ethan Brooks delves into the security layers of ShopSwift, a US-based e-commerce platform reeling from a recent data breach. Tasked with uncovering the method behind unauthorized account takeovers, Ethan examines login patterns across the platform's user base.
His investigation reveals a surge of automated login activity across multiple accounts, with a suspiciously high success rate. Determined to trace the root cause, Ethan compiles a detailed log to assist ShopSwift's security team in restoring trust.
Which attack method is Ethan most likely uncovering in ShopSwift's authentication system?
A. Password Spraying
B. Brute Force Attack
C. Credential Stuffing
D. Phishing Attacks

Answer: (SHOW ANSWER)
Credential stuffing is the best match because the scenario highlights automated login attempts across many accounts with an unusually high success rate, occurring in the aftermath of a breach. In CEH-aligned system hacking concepts, credential stuffing is the automated testing of known username and password pairs- typically harvested from prior breaches-against a different service. Because many users reuse passwords across sites, attackers often achieve a higher-than-normal success rate compared to guessing-based attacks.
This "high success rate" across numerous accounts is a key indicator that the attacker is not randomly guessing, but replaying valid credentials at scale using bots or automation frameworks.
Password spraying differs in that the attacker tries a small set of common passwords (or one password) across many accounts to avoid lockouts. Spraying generally yields a lower success rate and is driven by guessing rather than replaying known credential pairs. A brute force attack is even noisier and typically involves repeated guessing for a single account or small set of accounts; it is both slower and far less likely to produce a high success rate across many users in a short period. Phishing attacks can lead to account takeovers, but the pattern described would more often show targeted victims and varied sources rather than broad, automated, multi-account authentication bursts with consistently successful logins.
CEH defensive guidance emphasizes layered controls: enforce MFA, monitor for abnormal login velocity and credential reuse indicators, deploy bot detection and rate limiting, use breached-password checks, implement adaptive authentication, and tune lockout and detection policies to disrupt automated credential replay without enabling denial-of-service against legitimate users.

NEW QUESTION: 79
During a security assessment of an internal network, a penetration tester discovers that UDP port 123 is open, indicating that the NTP service is active. The tester wants to enumerate NTP peers, check synchronization status, offset, and stratum levels. Which command should the tester use?
A. ntpdc
B. ntpq
C. ntptrace
D. ntpdate
Answer: B (LEAVE A REPLY)
The ntpq utility provides detailed NTP peer information, synchronization states, offsets, delays, and strata.
CEH specifically lists ntpq as the tool for querying NTP daemon status and enumerating peer relationships, making it essential for reconnaissance and lateral movement mapping.

NEW QUESTION: 80
During a red team assessment at a university in Chicago, Jake, a penetration tester, scans a group of older Windows workstations in the administration department. On several hosts, he notices traffic on UDP ports
137 and 138 as well as an open TCP port 139. Curious, he uses a utility to query the name table and session services. Within moments, he collects information including machine names, logged-in usernames, and available shared folders without authentication.
Which enumeration method is being demonstrated in this scenario?
A. NFS Enumeration
B. NetBIOS Enumeration
C. SMB Enumeration
D. SNMP Enumeration
Answer: B (LEAVE A REPLY)
The correct answer is B. NetBIOS Enumeration because the ports and services described map directly to NetBIOS over TCP/IP (NBT) and the actions align with querying NetBIOS name table and session services.
In Windows networking (especially older systems), NetBIOS provides naming and session-layer services that can reveal valuable host and user information. Specifically, UDP 137 is used for the NetBIOS Name Service (NBNS), UDP 138 for NetBIOS Datagram Service, and TCP 139 for NetBIOS Session Service. Observing activity on UDP 137/138 and an open TCP 139 strongly indicates that NetBIOS services are reachable and can be interrogated.
The scenario states Jake "uses a utility to query the name table and session services," which is a hallmark of NetBIOS enumeration. NetBIOS name table queries can disclose machine names, domain/workgroup names, and sometimes logged-in usernames (depending on configuration and what names are registered). Session
/service enumeration can reveal information about active sessions and available resources. The fact that Jake obtains machine names, usernames, and shared folders without authentication is consistent with weakly configured legacy Windows networking where NetBIOS/SMB information disclosure is possible through null
/unauthenticated queries.
Why not the other options: NFS enumeration targets UNIX/Linux file sharing and is unrelated to ports 137-
139. SNMP enumeration uses UDP 161/162 and relies on SNMP communities, not NetBIOS naming/session queries. SMB enumeration is closely related and often overlaps operationally, but the question emphasizes
"query the name table and session services" and explicitly references the classic NetBIOS port set (137/138
/139), making NetBIOS enumeration the most precise classification for this behavior.

In practice, defenders mitigate this exposure by disabling NetBIOS where unnecessary, restricting these ports at network boundaries, enforcing SMB hardening, and limiting anonymous/null session information disclosure.

NEW QUESTION: 81
Ethical hacker Ryan Brooks, a skilled penetration tester from Austin, Texas, was hired by Skyline Aeronautics, a leading aerospace firm in Denver, to conduct a security assessment. One stormy morning, Ryan noticed an unexpected lag in the routine system update process while running his tests, sparking his curiosity. During a late-night session, he observed a junior analyst, Chris Miller, cautiously modifying a legacy server's configuration, including a scheduled task set to a specific date. The lead developer, Jessica Hayes, casually mentioned receiving an odd email from an unfamiliar source, which she ignored as clutter. As Ryan probed deeper, he detected a faint increase in network activity only after the scheduled date passed, and a systems admin, Mark Thompson, quickly pointed out some unusual code traces on a dormant workstation.
Which type of threat best characterizes this attack?
A. Logic Bomb
B. Fileless Malware
C. Advanced Persistent Threat APT
D. Ransomware
Answer: A (LEAVE A REPLY)
A logic bomb is malware or malicious code that is deliberately planted within a system and configured to execute when a specific condition is met, such as a particular date and time, a user action, or the presence or absence of a file. CEH materials describe logic bombs as condition-based triggers that can remain dormant for extended periods, producing minimal indicators until the trigger occurs. The most decisive clue in this scenario is the "scheduled task set to a specific date," followed by abnormal behavior that appears only after that date passes. This is a textbook trigger mechanism used to activate malicious actions while avoiding early detection.
The "odd email from an unfamiliar source" suggests an initial delivery or social engineering vector, but the core behavior is the delayed activation. The later "faint increase in network activity only after the scheduled date passed" aligns with a logic bomb executing a payload such as beaconing, data exfiltration, or enabling remote access. The "unusual code traces on a dormant workstation" further supports the idea of implanted code that was inactive until triggered.
Fileless malware emphasizes execution in memory using legitimate tools such as PowerShell or WMI and is defined more by its living-off-the-land technique than by a date-based trigger. An APT describes a broader campaign style involving long-term, multi-stage intrusion, not a single defining trigger artifact. Ransomware is characterized by encryption and extortion behavior, which is not described. Therefore, the threat is best characterized as a logic bomb.

NEW QUESTION: 82
During a penetration test at Windy City Enterprises in Chicago, ethical hacker Mia Torres targets the company ' s public-facing site. By exploiting an unpatched vulnerability in the web server, she manages to alter visible content on the homepage, replacing it with unauthorized messages. Mia explains to the IT team that this kind of attack can damage the company ' s reputation and erode customer trust, even if sensitive data is not directly stolen.
Which type of web server attack is Mia most likely demonstrating?
A. DNS Hijacking
B. Frontjacking
C. File Upload Exploits
D. Website Defacement
Answer: D (LEAVE A REPLY)
The attack described is website defacement, which occurs when an attacker gains the ability to modify the content of a website-often the homepage-to display unauthorized messages, propaganda, or vandalism.
The scenario explicitly says Mia "alter[s] visible content on the homepage, replacing it with unauthorized messages," and emphasizes the reputational harm even without data theft. That reputational impact is a hallmark of defacement: it undermines customer trust, signals weak security, and can create regulatory/brand consequences even if no confidential information is exfiltrated.
The stated entry point-"exploiting an unpatched vulnerability in the web server"-is also consistent with defacement. Attackers frequently leverage web server or web application weaknesses (misconfigurations, known CVEs, weak credentials, vulnerable plugins, or insecure file permissions) to gain write access to web content or templates. Once write access is achieved, the attacker can replace HTML pages, alter templates, inject malicious scripts, or modify assets so that visitors see the attacker's message.
Why the other options are less appropriate:
DNS hijacking (A) redirects users by changing DNS resolution so that the domain points to an attacker- controlled server. That can lead to a fake site, but it's not the same as modifying the real server's homepage content.
Frontjacking (B) typically involves UI deception-overlaying or framing content to trick users-rather than server-side modification of the homepage.
File upload exploits (C) are a method that can be used to gain code execution or place malicious files on a server, but the question asks for the type of web server attack being demonstrated. The visible outcome described-unauthorized homepage changes-is best categorized as defacement.
Therefore, Mia is most likely demonstrating D. Website Defacement.

NEW QUESTION: 83

You are investigating unauthorized access to a web application using token-based authentication. Tokens expire after 30 minutes. Server logs show multiple failed login attempts using expired tokens within a short window, followed by successful access with a valid token. What is the most likely attack scenario?

A. The attacker captured a valid token before expiration and reused it

B. The attacker brute-forced the token generation algorithm

C. The attacker exploited a race condition allowing expired tokens to be validated

D. The attacker performed a token replay attack that confused the server

Answer: C (LEAVE A REPLY)

The CEH Web Application Security module explains that race conditions occur when systems improperly handle simultaneous requests, leading to unexpected behavior. In token-based authentication systems, poor synchronization between token expiration checks and validation logic can allow attackers to exploit timing gaps.

The observed pattern-failed attempts with expired tokens followed by successful access-suggests the attacker exploited a race condition where the application inconsistently validated token state.

Option C is correct.

Option A would not involve expired tokens.

Option B is highly impractical given secure token entropy.

Option D typically succeeds without repeated failures.

CEH highlights race conditions as subtle but dangerous logic flaws.

NEW QUESTION: 84

During a late-night shift at IronWave Logistics in Seattle, cybersecurity analyst Marcus Chen notices a pattern of high-port outbound traffic from over a dozen internal machines to a previously unseen external IP. Each system had recently received a disguised shipping report, which, when opened, initiated a process that spread autonomously to other workstations using shared folders and stolen credentials. Upon investigation, Marcus discovers that the machines now contain hidden executables that silently accept remote instructions and occasionally trigger coordinated background tasks. The compromised endpoints are behaving like zombies, and malware analysts confirm that the payload used worm-like propagation to deliver a backdoor component across the network.

Which is the most likely objective behind this attack?

A. To exfiltrate sensitive information and tracking data

B. To execute a ransomware payload and encrypt all data

C. To establish a botnet for remote command and control

D. To deploy a Remote Access Trojan (RAT) for stealthy surveillance

Answer: C (LEAVE A REPLY)

The strongest indicator in this scenario is that multiple compromised hosts are "behaving like zombies," communicating outbound to a single unfamiliar external IP over high ports, and "silently accept remote instructions" while performing "coordinated background tasks."

In CEH-aligned malware terminology, these are hallmark characteristics of a botnet: a collection of infected endpoints (bots/zombies) under centralized or semi-centralized command-and-control. Worm-like propagation explains how the compromise rapidly expanded across the internal network-using shared folders and stolen credentials for lateral spread-while the "backdoor component" provides persistent remote control functionality once a system is infected. The observed coordination across many hosts strongly suggests the attacker's goal is not merely individual surveillance of a single machine, but scalable remote control of many machines at once.
Option A, data exfiltration, is plausible in many intrusions, but the question emphasizes orchestration and remote tasking across many endpoints rather than targeted theft from specific repositories. Option B is inconsistent because there is no mention of encryption, ransom notes, or disruption-focused behavior. Option D, a RAT, typically describes remote control of a host, but the scenario's defining feature is the creation of many "zombies" with coordinated behavior-this aligns more precisely with building a botnet for command and control, which can later be used for data theft, DDoS, spam, or further intrusion operations.
CEH defensive guidance includes monitoring egress traffic anomalies, detecting C2 patterns, segmenting networks to limit worm spread, disabling unnecessary shares, enforcing strong credential hygiene, and using EDR to identify backdoors and lateral movement behaviors.

NEW QUESTION: 85
You are Sofia Patel, an ethical hacker at Nexus Security Labs, hired to test the mobile device security of Bayview University in San Francisco, California. During your assessment, you are given an Android 11-based Samsung Galaxy Tab S6 with USB debugging disabled and OEM unlock restrictions in place. To simulate an attacker attempting to gain privileged access, you install a mobile application that exploits a system vulnerability to gain root access directly on the device without requiring a PC. This allows you to bypass OS restrictions and retrieve sensitive research data. Based on this method, which Android rooting tool are you using?
A. Magisk Manager
B. One Click Root
C. KingoRoot
D. RootMaster
Answer: C (LEAVE A REPLY)
The scenario describes an on-device, app-based rooting approach that does not rely on a PC connection, USB debugging, or a bootloader unlock workflow. In CEH mobile platform coverage, this aligns with "one-click" rooting tools that package exploits to elevate privileges directly from user space to root on the device. These tools typically target known vulnerabilities in the Android OS, vendor kernels, or system services to obtain root privileges and then install a management component to maintain elevated access.

KingoRoot is commonly cited in ethical hacking training contexts as a popular one-click rooting solution that can run as an Android application and attempt to root a device without a computer, depending on the device model, Android version, and patch level. This directly matches the prompt: Sofia installs a mobile application, it "exploits a system vulnerability," and it achieves root "without requiring a PC." The constraints given, USB debugging disabled and OEM unlock restrictions, make PC-assisted ADB workflows or bootloader-based rooting less feasible, which further supports an exploit-driven, on-device rooting tool. Magisk Manager is primarily a root management and systemless modification framework and typically assumes the device is already rooted or that the user can patch the boot image and flash it, often requiring bootloader unlock steps that OEM restrictions would block. "One Click Root" is a generic label rather than a specific tool in many CEH-style question banks. RootMaster is another one-click tool, but KingoRoot is the most widely recognized and frequently referenced for direct APK-based rooting in this context.

NEW QUESTION: 86
As a newly appointed network security analyst, you are tasked with ensuring that the organization's network can detect and prevent evasion techniques used by attackers. One commonly used evasion technique is packet fragmentation, which is designed to bypass intrusion detection systems (IDS). Which IDS configuration should be implemented to effectively counter this technique?
A. Implementing an anomaly-based IDS that can detect irregular traffic patterns caused by packet fragmentation.
B. Adjusting the IDS to recognize regular intervals at which fragmented packets are sent.
C. Configuring the IDS to reject all fragmented packets to eliminate the risk.
D. Employing a signature-based IDS that recognizes the specific signature of fragmented packets.
Answer: A (LEAVE A REPLY)
According to the Certified Ethical Hacker (CEH) IDS/IPS and Evasion Techniques module, packet fragmentation is a technique attackers use to split malicious payloads into smaller fragments so that signature-based IDS sensors may fail to reassemble and inspect the complete packet.
CEH explains that anomaly-based IDS systems are more effective against fragmentation evasion because they analyze behavioral deviations rather than relying solely on known signatures. Fragmented traffic often deviates from baseline network behavior in terms of packet size, sequencing, and reassembly anomalies.
Option A is correct because anomaly-based detection can identify abnormal fragmentation behavior even if the payload itself does not match known signatures.
Option B is unreliable, as attackers do not use consistent intervals.
Option C is impractical, since legitimate traffic may be fragmented.
Option D is less effective because signature-based IDS systems can be bypassed by fragmentation techniques.

CEH recommends packet normalization and anomaly-based detection as effective countermeasures.

NEW QUESTION: 87
During a security review for a healthcare provider in Denver, Colorado, Ava examines the header of a suspicious message to map the sender's outbound email infrastructure. Her goal is to identify which specific system on the sender's side processed the message so the team can understand where the transmission originated within that environment. Which detail from the email header should she examine to determine this?
A. Date and time of message sent
B. Sender's mail server
C. Sender's IP address
D. Authentication system used by sender's mail server
Answer: B (LEAVE A REPLY)
To determine which specific system on the sender's side processed the message, the most relevant email- header detail is the sender's mail server, typically revealed in the chain of Received: headers. Each mail transfer agent (MTA) that handles the message adds a Received line indicating the system that passed the message along and the system that received it. By reviewing these headers from bottom to top (earliest hop upward), analysts can identify the originating outbound infrastructure used by the sender-such as the initial submission server, outbound relay, or gateway that first accepted the email for delivery.
The scenario's goal is to "map the sender's outbound email infrastructure" and identify "which specific system on the sender's side processed the message." That maps more directly to identifying the mail server hostnames involved (the MTAs), because those are the processing systems that relayed the email. While an IP address can help locate a host, the question emphasizes the "specific system" responsible for processing, which is typically expressed as the mail server identity (hostname/domain) shown in header traces. In practice, investigators correlate the sender mail server information with IPs, TLS details, and authentication results, but the primary header clue for the processing system is the server identified in Received lines.
Why the other options are less suitable:
Date and time (A) helps with timeline analysis, not identification of the processing system.
Sender's IP address (C) can indicate a source network, but the message may traverse NAT, relays, or cloud email services; it doesn't always name the processing system.
Authentication system used (D) (e.g., SPF/DKIM/DMARC results) indicates validation outcomes, not which server processed the message.
Therefore, the correct choice is B. Sender's mail server.

NEW QUESTION: 88

A web server was compromised through DNS hijacking. What would most effectively prevent this in the future?

A. Changing IP addresses

B. Regular patching

C. Implementing DNSSEC

D. Using LAMP architecture

Answer: C (LEAVE A REPLY)

DNS hijacking occurs when attackers manipulate DNS responses to redirect traffic to malicious servers. CEH v13 clearly identifies DNSSEC (Domain Name System Security Extensions) as the primary defense against such attacks.

DNSSEC adds cryptographic signatures to DNS records, enabling clients to verify authenticity and integrity of DNS responses. Without DNSSEC, attackers can spoof DNS responses even if servers are fully patched.

Changing IP addresses and using LAMP do not address DNS trust. Patching is essential but does not prevent DNS spoofing.

CEH v13 explicitly recommends DNSSEC for preventing cache poisoning and DNS hijacking attacks, making Option C the correct answer.

NEW QUESTION: 89

In the hushed offices of Pinecrest Solutions in Denver, network security analyst Lisa Nguyen began a covert review of a recent spike in network access issues reported by the sales team. The trouble surfaced during a low-traffic period when agents couldn't reach their CRM system, prompting Lisa to examine the subnet logs.

She spotted irregular IP assignment attempts linked to an unfamiliar device. Acting quickly, Lisa entered a series of commands on the Cisco switches and later confirmed that connectivity issues had ceased without any new devices appearing in the logs.

Which command did Lisa most likely use to address the issue?

A. Switch(config)# ip dhcp snooping vlan 10

B. Switch(config)# ip arp inspection vlan 10

C. Switch(config)# ip dhcp snooping

D. Switch(config-if)# switchport port-security

Answer: A (LEAVE A REPLY)

The symptoms point to a rogue DHCP scenario, which CEH materials commonly describe as a method attackers use to disrupt networks or perform man-in-the-middle attacks. If an unauthorized device begins answering DHCP requests faster than the legitimate DHCP server, endpoints may receive incorrect IP settings such as a fake default gateway or DNS server. This causes loss of connectivity to internal applications like a CRM system and can silently redirect traffic through an attacker-controlled host. The question explicitly mentions "irregular IP assignment attempts" tied to an unfamiliar device, which aligns strongly with rogue DHCP behavior rather than ARP-only manipulation or simple MAC-limit violations.

DHCP snooping is a Layer 2 security feature on Cisco switches that filters untrusted DHCP messages and allows only authorized DHCP servers on trusted ports. When enabled for the affected VLAN, the switch will drop DHCP offers and acknowledgments arriving on untrusted access ports, stopping the rogue device from leasing addresses. Option A, ip dhcp snooping vlan 10, is the command that applies DHCP snooping protection to the specific VLAN experiencing the issue, which matches the "subnet logs" and the localized impact described.
Option B, Dynamic ARP Inspection, primarily mitigates ARP spoofing and relies on DHCP snooping bindings, but it does not directly stop rogue DHCP leasing. Option D, port security, can limit MAC addresses but does not specifically block DHCP server behavior. Option C enables the feature globally but does not target the VLAN; the VLAN-specific activation in A best matches the scenario and the immediate restoration of correct addressing and connectivity.

NEW QUESTION: 90
During a security compliance audit at Nexus Tech Solutions in Boston, Massachusetts, the ethical hacking team launches a controlled social engineering exercise to assess help desk vulnerabilities. Ethical hacker Rachel Kim calls the company ' s help desk, posing as a stressed employee named Laura Bennett from the marketing department. Rachel claims her laptop is running slowly and offers to share her login credentials if the help desk can provide a quick fix to meet a tight project deadline. The call is designed to test whether help desk staff follow proper verification protocols or fall for the offer of credentials in exchange for assistance.
What social engineering technique is Rachel employing in this exercise?
A. Shoulder Surfing
B. Vishing
C. Impersonation
D. Quid Pro Quo
Answer: C (LEAVE A REPLY)
This scenario best illustrates impersonation. In CEH-aligned social engineering concepts, impersonation occurs when an attacker assumes the identity of a legitimate person, such as an employee, contractor, executive, or vendor, to exploit trust and bypass established procedures. Rachel explicitly "poses as a stressed employee named Laura Bennett" and uses a believable workplace pretext such as a slow laptop and a tight deadline. This is a classic pressure-and-urgency tactic used to lower skepticism and push the target into breaking policy, such as skipping identity verification or accepting unsafe troubleshooting steps.
Although the interaction happens over the phone, the defining technique being tested is not merely the communication channel but the identity deception. Vishing is phone-based phishing, and while the call could be described as vishing in a broad sense, the prompt emphasizes the assumed identity and the help desk's verification controls, which is the

hallmark of impersonation. Quid pro quo typically involves offering a benefit or service in exchange for information; here, the core mechanic is Rachel's false identity and her attempt to get the help desk to accept credential sharing as part of support. Shoulder surfing is unrelated because it involves physically observing someone's screen or keystrokes.
CEH best practices to mitigate impersonation include strict caller verification, callback procedures to known numbers, ticket validation, prohibiting password sharing, requiring multi-factor authentication resets via approved workflows, and training help desk staff to recognize urgency-based manipulation and escalate suspicious requests.

NEW QUESTION: 91
During an ethical hacking exercise, a security analyst is testing a web application that manages confidential information and suspects it may be vulnerable to SQL injection. Which payload would most likely reveal whether the application is vulnerable to time-based blind SQL injection?
A. UNION SELECT NULL, NULL, NULL--
B. ' OR '1'='1'--
C. ' OR IF(1=1,SLEEP(5),0)--
D. AND UNION ALL SELECT 'admin','admin'--
Answer: C (LEAVE A REPLY)
CEH's SQL Injection coverage distinguishes between classic (error-based), union-based, boolean-based blind, and time-based blind SQL injection. Time-based blind SQL injection is used when the application does not return database errors or query results to the attacker (no visible output), but the attacker can infer execution behavior by measuring response delays.
A time-based payload intentionally triggers a database delay function (for example, SLEEP(), WAITFOR DELAY, pg_sleep() depending on DBMS). If the injection is successful, the page response time increases predictably, confirming that attacker-controlled SQL is being executed.
Option C is the correct time-based blind probe because it uses conditional logic (IF(1=1, SLEEP(5), 0)) to cause a measurable delay only when the injected condition evaluates true. CEH teaches that this technique is particularly effective against hardened applications that suppress errors and sanitize outputs, because timing becomes the side-channel for confirmation.
Option A and Option D are UNION-based payload patterns intended to extract data via returned result sets, which time-based blind scenarios typically do not provide. Option B is a classic authentication-bypass
/boolean test; it can indicate injection but does not specifically validate time-based blind behavior when output is not observable.

CEH mitigation guidance includes parameterized queries, strict input validation, least-privilege DB accounts, WAF tuning, and centralized logging to detect anomalous query timing patterns.

NEW QUESTION: 92
During a cryptographic audit of a legacy system, a security analyst observes that an outdated block cipher is leaking key-related information when analyzing large sets of plaintext-ciphertext pairs. What approach might an attacker exploit here?
A. Launch a key replay through IV duplication
B. Use linear approximations to infer secret bits
C. Modify the padding to obtain plaintext
D. Attack the hash algorithm for collisions
Answer: B (LEAVE A REPLY)
CEH covers classical cryptanalytic attacks, including linear cryptanalysis, which uses statistical correlations between plaintext and ciphertext to infer bits of the secret key. If a cipher leaks structural patterns across many data samples, linear approximations can be computed to break the cipher.

NEW QUESTION: 93
Working as an Information Security Analyst at a technology firm, you are designing training material for employees about the dangers of session hijacking. As part of the training, you want to explain how attackers could use sidejacking to compromise user accounts. Which of the following scenarios most accurately describes a sidejacking attack?
A. An attacker exploits a vulnerability in the company's network firewall to gain unauthorized access to internal systems.
B. An attacker intercepts network traffic, captures unencrypted session cookies, and uses them to impersonate the user.
C. An attacker uses social engineering techniques to trick an employee into revealing their password.
D. An attacker convinces an employee to visit a malicious website that injects a harmful script into their browser.
Answer: B (LEAVE A REPLY)

According to the Certified Ethical Hacker (CEH) System Hacking and Session Hijacking module, sidejacking is a form of session hijacking where an attacker passively intercepts network traffic to capture unencrypted session cookies. These cookies are then reused to impersonate the authenticated user without needing credentials.
CEH documentation explains that sidejacking commonly occurs on unencrypted HTTP connections, public Wi-Fi networks, or improperly secured internal networks. Once the session cookie is stolen, the attacker can replay it to gain access to the victim's active session.
Option B correctly describes this mechanism and directly matches CEH's definition of sidejacking.
Option A refers to perimeter exploitation, not session hijacking.
Option C describes social engineering, which is unrelated to sidejacking.
Option D is an example of cross-site scripting (XSS), not sidejacking.
CEH emphasizes HTTPS enforcement and secure cookie attributes as key countermeasures.

NEW QUESTION: 94
Infected systems receive external instructions over HTTP and DNS, with fileless payloads modifying system components. What is the most effective action to detect and disrupt this malware?
A. Update antivirus signatures regularly
B. Allow only encrypted traffic via proxies
C. Block common malware ports
D. Use behavioral analytics to monitor abnormal outbound behavior
Answer: D (LEAVE A REPLY)
This scenario describes fileless malware using covert command-and-control (C2) channels over commonly allowed protocols such as HTTP and DNS, a technique heavily emphasized in CEH v13 Malware Threats.
Such malware avoids writing files to disk and instead leverages memory, legitimate system tools, and trusted protocols to evade traditional defenses.
Signature-based antivirus updates (Option A) are ineffective against fileless malware because there are no static artifacts to match. Blocking known malware ports (Option C) is also ineffective, as the malware intentionally uses ports 80 and 53, which must remain open for normal business operations. Restricting plain HTTP (Option B) may reduce visibility but does not stop DNS tunneling or encrypted malicious traffic.
CEH v13 identifies behavioral analytics as the most effective countermeasure against advanced malware.
Behavioral solutions establish a baseline of normal system and network activity, then detect anomalies such as:
Unusual outbound DNS query patterns
Abnormal HTTP beaconing intervals

Legitimate applications behaving suspiciously
PowerShell or system tools generating network traffic unexpectedly
By monitoring how systems behave rather than what files exist, behavioral analytics can identify stealthy C2 communications and disrupt them early. Therefore, Option D is the most effective and CEH-aligned response.

NEW QUESTION: 95
Which advanced evasion technique poses the greatest challenge to detect and mitigate?
A. Covert channel communication using IP header fields
B. Honeypot spoofing
C. Polymorphic malware
D. Packet fragmentation evasion
Answer: A (LEAVE A REPLY)
Covert channel communication is one of the most sophisticated evasion techniques described in CEH v13 Evasion Techniques. By embedding malicious data within unused or rarely inspected protocol fields (such as IP headers), attackers can bypass firewalls, IDS, and IPS systems entirely.
Unlike polymorphic malware (Option C), which can still be detected using behavior analysis, covert channels blend seamlessly into legitimate traffic. Packet fragmentation (Option D) is well-known and often mitigated.
Honeypot spoofing (Option B) is rare and defensive in nature.
CEH v13 emphasizes that covert channels are difficult because:
* They do not violate protocol specifications
* They evade signature-based and stateful inspection
* They appear as normal traffic
Detecting covert channels often requires deep protocol analysis and statistical traffic inspection, making them extremely challenging to mitigate.
Thus, Option A is the correct answer.

NEW QUESTION: 96
An ethical hacker is conducting a penetration test on a company's network with full knowledge and permission from the organization. What is this type of hacking called?
A. Blue Hat Hacking
B. Grey Hat Hacking
C. Black Hat Hacking
D. White Hat Hacking
Answer: (SHOW ANSWER)
White-hat hackers perform security assessments with authorization. CEH defines ethical hacking as legal, structured testing of network defenses with the goal of improving security rather than causing harm.

NEW QUESTION: 97
A penetration tester is evaluating a secure web application that uses HTTPS, secure cookie flags, and regenerates session IDs only during specific user actions. To hijack a legitimate user's session without triggering security alerts, which advanced session hijacking technique should the tester employ?
A. Perform a man-in-the-middle attack by exploiting certificate vulnerabilities
B. Use a session fixation attack by setting a known session ID before the user logs in
C. Conduct a session token prediction attack by analyzing session ID patterns
D. Implement a Cross-Site Scripting (XSS) attack to steal session tokens
Answer: C (LEAVE A REPLY)
CEH v13 emphasizes that well-secured applications use HTTPS, secure cookies, and session regeneration to defend against common session hijacking techniques. In such hardened environments, traditional attacks like session fixation or simple XSS-based token theft often fail because session IDs change at login and secure flags prevent exposure. The remaining viable approach is session token prediction, an advanced attack that analyzes statistical patterns, entropy weaknesses, or timing issues in session ID generation algorithms. CEH discusses that weak pseudorandom number generators (PRNGs) or predictable sequences can allow attackers to compute a valid session ID without intercepting traffic. This method bypasses cookie security and does not rely on manipulating user input, making it suitable for environments with strong defenses. MITM attacks (Option A) require certificate compromise, which is impractical. Session fixation (Option B) fails because the application regenerates tokens. XSS (Option D) is ineffective when secure flags prevent JavaScript access to cookies. Thus, token prediction is the correct answer.

NEW QUESTION: 98
At a cybersecurity consultancy firm in Boston, senior analyst Amanda Liu is called in to assess a malware outbreak affecting a regional healthcare provider. Despite using updated antivirus tools, the security team notices inconsistent detection across infected endpoints. Amanda discovers that while the malicious behavior is consistent, system file tampering and suspicious outbound traffic, each malware sample has a slightly different code structure and fails traditional hash-based comparison. Static analysis reveals that the underlying logic remains unchanged, but the code patterns vary unpredictably across infections. What type of virus is most likely responsible for this behavior?
A. Cavity virus
B. Macro virus
C. Polymorphic virus
D. Stealth virus
Answer: C (LEAVE A REPLY)
A polymorphic virus is specifically designed to change its code appearance while keeping the same underlying functionality, which aligns exactly with the scenario. In CEH terms,

polymorphism allows malware to mutate its decryptor routine, instruction ordering, register usage, junk code insertion, and other syntactic elements every time it propagates or executes. This causes each instance to look different at the binary level, producing different hashes and signatures, even though the malicious payload and behavior remain the same. That is why the security team sees inconsistent antivirus detection and why "traditional hash- based comparison" fails. The key indicator is that static analysis shows the "underlying logic remains unchanged," but "code patterns vary unpredictably," which is the hallmark of polymorphism: behavior stays consistent, signature changes.
The other options do not fit as well. A cavity virus typically hides by inserting itself into unused spaces within legitimate executable files to avoid changing the overall file size, but it does not inherently generate unpredictable code variants per infection. A macro virus primarily targets macro-enabled documents and spreads through document templates and user actions, which is not suggested here. A stealth virus focuses on evading detection by intercepting system calls and hiding its presence, such as returning "clean" file reads, but it does not necessarily produce many structurally different binaries that break hash matching. Therefore, the most likely cause of the described outbreak is a polymorphic virus.

NEW QUESTION: 99
Javier Ruiz from CyberFortress Solutions is tasked with auditing the mobile security practices of Apex Financial Services, a financial firm in Houston, Texas. During a covert penetration test, Javier targets employees' personal smartphones used to access corporate financial systems. He exploits a vulnerability by installing a malicious app that bypasses access controls, granting him unauthorized entry to sensitive financial data because the devices lack a specific security measure to restrict app access. Based on this vulnerability, which BYOD security guideline is most likely missing in Apex Financial Services' policy?
A. Review permissions requested by apps before installing them
B. Set passwords for apps to restrict others from accessing them
C. Enforce automatic device locking or implement biometric authentication
D. Use encryption mechanisms to store data
Answer: A (LEAVE A REPLY)
The most likely missing BYOD guideline is reviewing application permissions before installation. In CEH mobile security guidance, a major risk in BYOD environments is the introduction of untrusted or malicious applications that abuse the mobile permission model to access corporate data, intercept authentication tokens, read storage, capture keystrokes via accessibility services, or communicate externally. When users install apps without scrutinizing requested permissions, they may unknowingly grant excessive privileges that enable data theft or access-control bypass, especially if the app leverages OS weaknesses or misconfigurations.

The scenario states Javier "installs a malicious app that bypasses access controls" and gains access to sensitive financial data because devices "lack a specific security measure to restrict app access." This maps directly to a policy gap around controlling and validating apps and their permission requests. CEH emphasizes that organizations should reduce attack surface by limiting app privileges, avoiding sideloading from untrusted sources, and enforcing least privilege through user awareness and enterprise controls such as MDM application allowlisting and permission governance. Reviewing permissions is the user-facing guideline that prevents employees from granting dangerous access (for example, SMS, storage, contacts, accessibility, device admin, or VPN configuration permissions) that can enable credential theft or unauthorized data access.
Option B adds an extra layer for local access but does not stop a malicious app with granted permissions from accessing corporate data. Option C helps if a device is physically stolen, but it does not prevent malicious apps already running under the user context. Option D protects data at rest, yet a malicious app can still exfiltrate data once it is decrypted and accessed by the user session. Therefore, permission review is the most directly relevant missing BYOD guideline.

NEW QUESTION: 100
Which tool is best for sniffing plaintext HTTP traffic?
A. Nessus
B. Nmap
C. Netcat
D. Wireshark
Answer: (SHOW ANSWER)
Wireshark is the primary packet-sniffing tool covered in CEH v13 Network Sniffing. It captures and analyzes live traffic, allowing analysts to view plaintext HTTP packets. Nessus is a vulnerability scanner, Nmap is for scanning, Netcat is a networking utility. None provide protocol- level inspection like Wireshark.
Thus, Option D is correct.

NEW QUESTION: 101
A penetration tester must enumerate user accounts and network resources in a highly secured Windows environment where SMB null sessions are blocked. Which technique should be used to gather this information discreetly?
A. Utilize NetBIOS over TCP/IP to list shared resources anonymously
B. Exploit a misconfigured LDAP service to perform anonymous searches
C. Leverage Active Directory Web Services for unauthorized queries
D. Conduct a zone transfer by querying the organization's DNS servers
Answer: B (LEAVE A REPLY)
CEH v13 explains that when traditional enumeration techniques-such as SMB null sessions-are disabled, attackers often pivot to misconfigured LDAP services that still allow

anonymous binding. LDAP anonymous bind, when not properly restricted, exposes directory information such as usernames, organizational units, group memberships, and other metadata. This aligns directly with the scenario, where the tester must avoid triggering alarms while still gathering internal data. LDAP queries generate minimal noise, often blending with normal authentication-related traffic, making them ideal for covert enumeration. Options A and C would require authentication or violate access restrictions, and DNS zone transfers (Option D) rarely succeed because modern DNS servers disable AXFR requests from unauthorized clients. CEH repeatedly stresses the importance of detecting and securing LDAP anonymous bind due to its potential for silent information leakage-making Option B the correct choice.

NEW QUESTION: 102
In a vertical privilege escalation scenario, the attacker attempts to gain access to a user account with higher privileges than their current level. Which of the following examples describes vertical privilege escalation?
A. An attacker exploits weak access controls to access and steal sensitive information from another user's account with alike privileges.
B. An attacker leverages a lack of session management controls to switch accounts and access resources assigned to another user with the same permissions.
C. An attacker uses an unquoted service path vulnerability to gain unauthorized access to another user's data with equivalent privileges.
D. An attacker escalates from a regular user to an administrator by exploiting administrative functions.
Answer: D (LEAVE A REPLY)
CEH v13 distinguishes between vertical and horizontal privilege escalation. Vertical escalation occurs when an attacker moves upward in the hierarchy of privileges-such as from a regular user to an administrator or root-by exploiting vulnerabilities, misconfigurations, or insecure privilege boundaries. This allows the attacker to perform tasks that were previously restricted, such as modifying system settings, accessing sensitive data, installing malware, or controlling the entire environment. Horizontal escalation, on the other hand, involves accessing another user's resources at the same privilege level, which the other options describe. Exploiting unquoted service paths or weak access controls may facilitate privilege abuse, but they do not inherently elevate the user to a higher privilege tier unless they specifically lead to administrative execution. The scenario that aligns perfectly with the CEH definition of vertical privilege escalation is the escalation from regular user to administrator.

NEW QUESTION: 103
A future-focused security audit discusses risks where attackers collect encrypted data today, anticipating they will be able to decrypt it later using quantum computers. What is this threat commonly known as?

A. Saving data today for future quantum decryption
B. Breaking RSA using quantum algorithms
C. Flipping qubit values to corrupt output
D. Replaying intercepted quantum messages
Answer: A (LEAVE A REPLY)
The Certified Ethical Hacker (CEH) Cryptography and Quantum Computing section introduces the concept known as "Harvest Now, Decrypt Later". This threat model describes adversaries capturing encrypted data today, even if they cannot decrypt it immediately, with the expectation that future quantum computers will be able to break currently secure public-key algorithms such as RSA and ECC.
Option A accurately reflects this concept.
Option B describes a method (Shor's algorithm) but not the threat model itself.
Option C is unrelated to cryptographic attacks.
Option D refers to quantum communication attacks, not classical encrypted data harvesting.
CEH emphasizes post-quantum cryptography as a mitigation strategy.

NEW QUESTION: 104
A Nessus scan reveals a critical SSH vulnerability (CVSS 9.0) allowing potential remote code execution on a Linux server. What action should be immediately prioritized?
A. Redirect SSH traffic to another server
B. Treat the finding as a possible false positive
C. Immediately apply vendor patches and reboot during scheduled downtime
D. Temporarily isolate the affected server, conduct a forensic audit, and then patch
Answer: (SHOW ANSWER)
According to the CEH Vulnerability Assessment and Incident Response modules, vulnerabilities with high CVSS scores and potential RCE must be treated as active threats.
CEH best practices recommend:
* Immediate containment (network isolation)
* Investigation and impact analysis
* Patch application
* Recovery
Option D follows the CEH incident response lifecycle precisely.
Option C is incomplete without containment.
Options A and B are unsafe.
CEH emphasizes containment before remediation.

NEW QUESTION: 105
A cybersecurity analyst wants to monitor competitors' web content updates. What key element is missing from the plan?
A. Hacking competitor databases

B. Google Alerts for content monitoring
C. Engaging in blog discussions
D. Using a VPN
Answer: B (LEAVE A REPLY)
In CEH v13 Reconnaissance Techniques, passive monitoring of competitors' online presence is a legitimate and effective intelligence-gathering activity. One of the most efficient tools for this purpose is Google Alerts.
Google Alerts allow analysts to receive automated notifications when new content containing specific keywords-such as company names, products, or executives-is indexed online. This enables continuous, passive surveillance without repeatedly visiting websites manually.
Option B directly addresses the analyst's goal of staying updated efficiently.
Option A is illegal and unethical.
Option C involves direct interaction, which may reveal the analyst's presence.
Option D provides anonymity but does not actively monitor changes.
CEH v13 strongly encourages automation in reconnaissance to reduce noise, effort, and detection risk.
Therefore, Option B is the correct and CEH-aligned answer.

NEW QUESTION: 106
During a reconnaissance engagement at a law firm in Houston, Texas, you are tasked with analyzing the physical movement of employees through their publicly shared media. By examining geotagged images and mapping them to specific locations, you aim to evaluate whether staff are unintentionally disclosing sensitive information about office routines.
Which tool from the reconnaissance toolkit would best support this task?
A. Creepy
B. Social Searcher
C. Sherlock
D. Maltego
Answer: A (LEAVE A REPLY)
The correct answer is A. Creepy because the task is specifically about extracting and analyzing geolocation information (geotags) from publicly shared media and mapping that data to real-world locations to infer employee movement patterns. In CEH-aligned reconnaissance/OSINT workflows, geolocation intelligence is a common element of footprinting because it can reveal sensitive operational details such as office locations, travel routines, meeting venues, home addresses, and patterns of presence/absence.
Tools designed for geolocation OSINT help testers identify whether staff are unintentionally exposing location metadata through social media posts, uploaded photos, or other public sources.
Creepy is purpose-built for geolocation reconnaissance: it collects location metadata associated with content and presents results in a way that supports mapping and timeline-

style analysis, helping analysts correlate people, posts, and coordinates. This directly supports the goal of evaluating whether employees are disclosing sensitive information about office routines by publishing geotagged images. When used in an authorized assessment, such tooling helps demonstrate risk in a measurable way-for example, showing clusters of posts around a specific building, repeated visits at predictable times, or regular travel routes that could support surveillance, targeted social engineering, or physical intrusion planning.
Why the other options are less suitable: Social Searcher is primarily used for monitoring and searching social media content by keywords, usernames, hashtags, and mentions; it is useful for broad OSINT collection but is not specifically focused on geotag extraction and movement mapping. Sherlock is designed to find a username across many platforms, helping link identities, but it does not specialize in geolocation mapping.
Maltego is a powerful link-analysis platform that can correlate entities (people, domains, emails, social profiles) and can support OSINT investigations, but for the narrow requirement of extracting and mapping geotagged location data from media, Creepy is the most direct and purpose-specific tool.
Therefore, the best tool for this geotagged image movement analysis task is Creepy.

NEW QUESTION: 107
Which technique is commonly used by attackers to evade firewall detection?
A. Spoofing source IP addresses to appear trusted
B. Using open-source operating systems
C. Using encrypted communication channels
D. Social engineering employees
Answer: C (LEAVE A REPLY)
CEH v13 identifies encrypted communication channels as one of the most common and effective firewall evasion techniques. Firewalls that rely on packet inspection or signature-based filtering often cannot inspect encrypted payloads without SSL/TLS interception capabilities.
By encrypting malicious traffic-using HTTPS, VPN tunnels, or encrypted C2 channels-attackers can bypass firewall rules that inspect packet contents. CEH v13 emphasizes that

this technique is widely used in malware communication, data exfiltration, and command-and-control operations.
IP spoofing (Option A) is limited by ingress and egress filtering and is less effective against modern firewalls.
Open-source operating systems (Option B) do not inherently evade firewalls. Social engineering (Option D) targets users, not firewalls.
Therefore, Option C is the correct and CEH-aligned answer.

NEW QUESTION: 108
During a security assessment of a cloud-hosted application using SOAP-based web services, a red team operator intercepts a valid SOAP request, duplicates the signed message body, inserts it into the same envelope, and forwards it. Due to improper validation, the server accepts the duplicated body and executes unauthorized code. What type of attack does this represent?
A. Cloud snooper attack
B. Cryptanalysis attack
C. Wrapping attack
D. IMDS abuse
Answer: C (LEAVE A REPLY)
Comprehensive Explanation from CEH v13 Courseware:
CEH v13 identifies XML Signature Wrapping (XSW) attacks, also known simply as Wrapping attacks, as a major threat against SOAP-based web services. These attacks exploit weak XML parsing and insufficient validation of signed message components. SOAP messages often include digitally signed sections, but if the server validates the signature without confirming the correct position or structure of the signed elements, attackers can duplicate, move, or wrap signed content inside a modified XML envelope. This allows an attacker to inject malicious payloads while still presenting a valid signature. CEH details how this can lead to unauthorized execution, privilege escalation, or bypassing authentication controls in SOAP APIs. Cloud snooping, cryptanalysis, and IMDS abuse do not involve message duplication or signature misplacement. The scenario precisely matches CEH's definition of a Wrapping Attack in SOAP/XML security.

NEW QUESTION: 109
An ethical hacker needs to gather detailed information about a company's internal network without initiating any direct interaction that could be logged or raise suspicion. Which approach should be used to obtain this information covertly?
A. Analyze the company's SSL certificates for internal details
B. Examine email headers from past communications with the company
C. Inspect public WHOIS records for hidden network data
D. Utilize network scanning tools to map the company's IP range
Answer: B (LEAVE A REPLY)

Passive reconnaissance focuses on collecting information without directly touching or interacting with the target's systems. CEH materials stress that any action that sends network traffic to the target-such as scanning, probing, fingerprinting, or enumeration-creates logs and increases the risk of detection. Email headers, however, are considered an excellent source of passive intelligence because they reveal internal IP structures, routing paths, mail server hostnames, internal domain formats, and technology stacks without requiring interaction with the target environment. Since these headers are already in the possession of the ethical hacker through legitimate communication records, examining them does not generate traffic or trigger monitoring systems. SSL certificates and WHOIS data provide valuable external information, but they rarely disclose internal addressing schemes. Active scanning tools, such as Nmap, would immediately violate the requirement to avoid detection. Therefore, analyzing previously received email headers is the most effective and covert method for extracting internal network details during the reconnaissance phase.

NEW QUESTION: 110
A penetration tester discovers that a web application is using outdated SSL/TLS protocols (TLS 1.0) to secure communication. What is the most effective way to exploit this vulnerability?
A. Conduct a Cross-Site Scripting (XSS) attack on the application
B. Use a man-in-the-middle (MitM) attack to intercept and decrypt traffic
C. Perform a brute-force attack on the SSL/TLS handshake
D. Execute a SQL injection attack on the application's backend
Answer: B (LEAVE A REPLY)
Outdated encryption protocols such as SSL 3.0 and TLS 1.0 contain numerous cryptographic weaknesses, making them susceptible to downgrade attacks, cipher-suite vulnerabilities, and interception. CEH explains that weak SSL/TLS configurations expose encrypted traffic to man-in-the-middle attacks because attackers can exploit vulnerabilities such as BEAST, POODLE, or weak ciphers to decrypt or manipulate data in transit. These flaws compromise confidentiality and integrity, allowing attackers to observe login credentials, session identifiers, or sensitive information. XSS and SQL injection exploit entirely different web vulnerabilities unrelated to encryption strength. Brute-forcing SSL handshakes is computationally infeasible and not relevant. Therefore, a MitM attack targeting the outdated protocol is the most effective exploitation method.

NEW QUESTION: 111
During a penetration test at a healthcare facility in Baltimore, Maryland, an ethical hacker demonstrates how attackers are mapping active hosts and open ports using ICMP-based techniques. To reduce the organization's exposure, the security team decides to implement a countermeasure that specifically disrupts ICMP discovery traffic by preventing error messages from being returned. Which action should they take?

A. Use a custom rule set to lock down the network, block unwanted ports at the firewall, and filter specific ports
B. Configure firewall and IDS rules to detect and block probes
C. Block unwanted services running on the ports and update the service versions
D. Block inbound ICMP message types and all outbound ICMP type 3 (Destination Unreachable) messages
Answer: D (LEAVE A REPLY)
The correct choice is D because the question is specifically about disrupting ICMP-based discovery by preventing error messages from being returned. In ICMP reconnaissance, attackers often rely not only on ICMP Echo (ping) but also on ICMP error messages to infer host availability, filtering behavior, and port reachability. A key ICMP error category is ICMP Type 3: Destination Unreachable, which includes several codes (for example, "port unreachable" and "communication administratively prohibited") that can reveal whether a host exists, whether a firewall is filtering traffic, and whether specific ports are reachable or blocked. When these ICMP Type 3 messages are allowed to leave the network, they provide valuable feedback that helps attackers map the environment accurately.
By blocking inbound ICMP message types (to reduce direct ICMP probing) and blocking outbound ICMP Type 3 unreachable messages, the organization reduces the "informational signals" that external scanners can use to distinguish between live hosts, filtered hosts, and closed ports. This directly aligns with the requirement in the prompt: stopping ICMP discovery by preventing error messages from being returned.
Why the other choices are less precise:
A and C focus on general hardening (port/service reduction), which is good practice but does not directly address ICMP error-message feedback.
B (firewall/IDS detection) is helpful, but the prompt asks for an action that specifically disrupts ICMP discovery traffic by suppressing error responses, which is more directly achieved via ICMP filtering rules.
Operational note: while blocking ICMP Type 3 can reduce reconnaissance visibility, organizations should apply this carefully because some ICMP is important for normal network operations and troubleshooting.

NEW QUESTION: 112
On a busy Monday morning at Horizon Financial Services in Chicago, accounts assistant Clara Nguyen receives an email that appears to come from the company's IT department. The email, addressed specifically to Clara and mentioning her role in the accounts team, warns of a critical system vulnerability requiring immediate action. It includes a link to a login page resembling the company's internal portal, urging her to update her credentials to prevent account suspension. The email's sender address looks legitimate, but Clara notices a slight misspelling in the domain name.
What social engineering technique is being attempted against Clara?
A. Spear Phishing

B. Impersonation
C. Quid Pro Quo
D. Vishing
Answer: A (LEAVE A REPLY)
The attack described is spear phishing because it is a targeted phishing attempt crafted for a specific individual using personal and organizational context. In CEH social engineering coverage, spear phishing differs from generic phishing by its customization: the attacker addresses the victim by name, references the victim's job function, and tailors the message to create credibility and urgency. Here, the email is addressed specifically to Clara and mentions her role in the accounts team, which increases the likelihood she will trust the message and comply.
The message uses classic phishing psychological triggers emphasized in CEH materials: urgency and fear. By claiming a "critical system vulnerability" and threatening account suspension, the attacker pressures Clara to act quickly and ignore verification steps. The inclusion of a link to a login page that "resembles the company' s internal portal" indicates credential harvesting, where the attacker's goal is to capture usernames and passwords or other authentication tokens. The subtle misspelling in the sender's domain is a common indicator of lookalike or typosquatting domains used to mimic legitimate corporate email addresses and bypass casual inspection.
The other options do not match as well. Impersonation is a broader category, but spear phishing is the specific technique using an email lure with personalization. Quid pro quo involves offering a benefit or service in exchange for information, which is not present. Vishing is voice-based phishing via phone calls, not email.
Recommended defenses in CEH guidance include verifying sender domains, using out-of-band confirmation with IT, enabling email security controls like SPF, DKIM, and DMARC, and enforcing phishing awareness training and MFA to reduce credential theft impact.

NEW QUESTION: 113
A serverless application was compromised through an insecure third-party API used by a function. What is the most effective countermeasure?
A. Deploy a cloud-native security platform
B. Enforce function-level least privilege permissions
C. Use a CASB for third-party services
D. Regularly update serverless functions
Answer: B (LEAVE A REPLY)
In CEH v13 Cloud Computing, serverless architectures introduce unique security challenges, particularly around Function-as-a-Service (FaaS) permissions. When a serverless function is compromised through an insecure third-party API, the damage depends largely on what the function is allowed to do.
Implementing function-level permission models and enforcing the principle of least privilege ensures that even if a function is exploited, its ability to execute malicious actions

is strictly limited. CEH v13 strongly emphasizes granular IAM controls in serverless environments.
While cloud-native security platforms (Option A) and CASBs (Option C) provide visibility and governance, they do not directly prevent excessive permissions. Regular patching (Option D) is important but does not mitigate permission abuse.
CEH v13 identifies least privilege as the single most critical control in preventing serverless abuse and privilege escalation. Therefore, Option B is the correct answer.

NEW QUESTION: 114
Which advanced session hijacking technique is the most difficult to detect and mitigate?
A. Credential stuffing
B. Clickjacking
C. CSRF
D. Session replay attack
Answer: (SHOW ANSWER)
Session Replay Attacks are highlighted in CEH v13 Web Application Hacking as one of the most sophisticated and difficult-to-detect session hijacking techniques. In this attack, adversaries capture valid session tokens or encrypted session identifiers and replay them to impersonate legitimate users.
Unlike credential stuffing, which relies on login attempts and can be detected through authentication anomalies, session replay occurs after authentication, using legitimate session artifacts. Clickjacking and CSRF manipulate user interactions but do not directly hijack session tokens.
CEH v13 explains that session replay attacks are especially dangerous in environments where session tokens are predictable, long-lived, or improperly bound to client attributes such as IP address or device fingerprint.
Because the attacker reuses valid session data, traditional detection mechanisms often fail.
The replayed session appears legitimate to the server, making fraud detection extremely difficult without advanced behavioral analytics. This makes session replay attacks particularly effective in online retail environments where transactions are frequent and time-sensitive.
Thus, Option D correctly identifies the most challenging attack.

NEW QUESTION: 115
A penetration tester is assessing an organization's cloud infrastructure and discovers misconfigured IAM policies on storage buckets. The IAM settings grant read and write permissions to any authenticated user.
What is the most effective way to exploit this misconfiguration?
A. Use leaked API keys to access the cloud storage buckets and exfiltrate data

B. Execute a SQL injection attack on the organization's website to retrieve sensitive information
C. Create a personal cloud account to authenticate and access the misconfigured storage buckets
D. Perform a Cross-Site Scripting (XSS) attack on the cloud management portal to gain access
Answer: (SHOW ANSWER)
CEH notes that cloud IAM misconfigurations can unintentionally grant broad access. If any authenticated cloud account is permitted read/write access, attackers can simply authenticate with their own cloud identity and directly interact with the misconfigured storage buckets, enabling data exfiltration or manipulation.

NEW QUESTION: 116
An attacker exploits medical imaging protocols to intercept patient data. Which sniffing technique is most challenging?
A. MRI firmware interception
B. Ultrasound malware
C. Covert channel within administrative messages
D. Embedding data inside CT scan images
Answer: D (LEAVE A REPLY)
This scenario describes steganographic sniffing, a highly sophisticated technique covered in CEH v13 Network Sniffing and Steganography. By embedding sensitive data inside legitimate image files-such as CT scans-attackers can intercept or exfiltrate patient information while avoiding detection.
Option D represents a steganography-based covert channel, which is extremely difficult to identify because:
* The file appears legitimate
* Standard encryption and IDS tools do not flag it
* Medical images naturally contain large data volumes
Options A and B involve malware, which is more detectable. Option C involves text-based covert channels, which are easier to analyze than binary image embedding.
CEH v13 identifies steganography as one of the hardest data-hiding techniques to detect, making Option D correct.

NEW QUESTION: 117
While evaluating a smart card implementation, a security analyst observes that an attacker is measuring fluctuations in power consumption and timing variations during encryption operations on the chip. The attacker uses this information to infer secret keys used within the device. What type of exploitation is being carried out?
A. Disrupt control flow to modify instructions
B. Observe hardware signals to deduce secrets

C. Crack hashes using statistical collisions
D. Force session resets through input flooding
Answer: B (LEAVE A REPLY)
CEH v13 explains that Side-Channel Attacks exploit physical characteristics of cryptographic devices-such as power consumption, timing variations, electromagnetic leakage, or acoustic emissions-to infer confidential data like encryption keys. These attacks do not break the cryptographic algorithm itself but instead analyze unintended signals produced during computation. The scenario describes a classic power analysis and timing analysis attack, where the attacker monitors fluctuations during encryption operations on a smart card. CEH details how Differential Power Analysis (DPA) and Simple Power Analysis (SPA) allow attackers to extract secret keys by statistically correlating measured power traces to cryptographic operations.
This type of attack is extremely dangerous because it bypasses mathematical strength and targets hardware implementation flaws. Options A, C, and D do not relate to side-channel exploitation. CEH specifically categorizes this method as observing hardware emissions to deduce secrets, making Option B the most accurate match.

NEW QUESTION: 118
An ethical hacker conducts testing with full knowledge and permission. What type of hacking is this?
A. Blue Hat
B. Grey Hat
C. White Hat
D. Black Hat
Answer: C (LEAVE A REPLY)
White Hat Hacking is defined in CEH v13 as ethical hacking performed with explicit authorization to identify and remediate vulnerabilities. White hat hackers operate within legal frameworks and contractual agreements.
Grey hats act without permission but without malicious intent. Black hats conduct illegal attacks. Blue hats are external testers invited to find bugs before product release.
Thus, Option C is correct.

NEW QUESTION: 119
A cybersecurity team identifies suspicious outbound network traffic. Investigation reveals malware utilizing the Background Intelligent Transfer Service (BITS) to evade firewall detection. Why would attackers use this service to conceal malicious activities?
A. Because BITS packets appear identical to normal Windows Update traffic.
B. Because BITS operates exclusively through HTTP tunneling.
C. Because BITS utilizes IP fragmentation to evade intrusion detection systems.
D. Because BITS traffic uses encrypted DNS packets.
Answer: A (LEAVE A REPLY)

The Certified Ethical Hacker (CEH) Malware Threats module explains that attackers often abuse legitimate system services to blend malicious traffic with normal system behavior. Background Intelligent Transfer Service (BITS) is a Windows service designed to transfer files in the background using idle network bandwidth.
Attackers leverage BITS because its traffic closely resembles legitimate Windows Update traffic, which is commonly allowed through firewalls and proxy servers. CEH documentation states that BITS-based malware can download payloads, upload stolen data, and maintain persistence without triggering security alerts.
Option A is correct because BITS traffic appears legitimate and trusted, making it difficult for security devices to distinguish malicious usage.
Option B is incorrect because BITS does not operate exclusively through HTTP tunneling; it primarily uses HTTP/HTTPS in a legitimate manner.
Option C is incorrect because IP fragmentation is not a core feature of BITS.
Option D is incorrect because BITS does not rely on encrypted DNS traffic.
CEH emphasizes that living-off-the-land (LotL) techniques-using native tools like BITS-are increasingly favored by attackers due to their stealth and reliability.

NEW QUESTION: 120
Bluetooth devices are suspected of being targeted by a Bluesnarfing attack. What is the most effective countermeasure?
A. Disable discoverable mode
B. Update firmware regularly
C. Increase Bluetooth PIN complexity
D. Encrypt Bluetooth traffic
Answer: (SHOW ANSWER)
Bluesnarfing is a Bluetooth attack described in CEH v13 Wireless Network Hacking, where attackers exploit misconfigured Bluetooth devices to access sensitive data such as contacts, messages, and files-often without user interaction.
One of the most critical enablers of Bluesnarfing is Bluetooth discoverable mode. When devices are discoverable, attackers can easily identify them and attempt unauthorized connections or exploit vulnerabilities in Bluetooth services.
Disabling discoverable mode significantly reduces the attack surface by preventing unauthorized devices from locating Bluetooth-enabled systems. CEH v13 explicitly recommends setting Bluetooth devices to non- discoverable mode when not pairing.
While firmware updates (Option B) are important, they do not immediately prevent discoverability-based attacks. Stronger PINs (Option C) help against pairing attacks but do not stop unauthorized queries. Network- level encryption (Option D) is inherent in Bluetooth protocols and does not mitigate discovery abuse.
CEH v13 highlights that visibility control is the most immediate and effective defense against Bluesnarfing.
Therefore, Option A is the correct answer.

NEW QUESTION: 121
A large chemical plant uses operational technology (OT) networks to control its industrial processes.
Recently, abnormal behavior is observed from PLCs, suggesting a stealthy compromise via malicious firmware. Which action should the team take FIRST to verify and neutralize the issue?
A. Immediately isolate suspicious devices
B. Perform detailed inspections of device software for unauthorized modifications
C. Implement enhanced IDS rules
D. Restrict remote administrative access
Answer: B (LEAVE A REPLY)
In CEH v13 Mobile, IoT, and OT Hacking, firmware-level attacks on Programmable Logic Controllers (PLCs) are categorized as high-impact and stealth-oriented threats, often designed to evade traditional network-based defenses. Malicious firmware compromises the integrity of the device itself, allowing attackers persistent and covert control over industrial processes.
The first and most critical step is to verify the integrity of the firmware and software running on the PLCs.
CEH v13 emphasizes that before containment or mitigation actions are applied, accurate identification and confirmation of compromise must occur. Firmware inspection enables analysts to detect unauthorized code injections, modified logic blocks, altered checksums, or tampered boot loaders-hallmarks of OT malware such as Stuxnet-like attacks.
Immediate isolation (Option A) may be necessary later, but premature isolation can disrupt industrial operations and destroy volatile forensic evidence. IDS enhancements (Option C) focus on traffic patterns and are ineffective against firmware-resident malware. Restricting remote access (Option D) is preventative but does not validate or remove an existing firmware compromise.
CEH v13 stresses that OT environments require forensic verification at the device level, especially when abnormal behavior originates from controllers themselves. Firmware validation using vendor-approved tools and hash verification is the correct first step to confirm compromise and plan remediation without risking operational safety.

NEW QUESTION: 122
A penetration tester performs a vulnerability scan on a company's web server and identifies several medium- risk vulnerabilities related to misconfigured settings. What should the tester do to verify the vulnerabilities?
A. Use publicly available tools to exploit the vulnerabilities and confirm their impact
B. Ignore the vulnerabilities since they are medium-risk
C. Perform a brute-force attack on the web server's login page
D. Conduct a denial-of-service (DoS) attack to test the server's resilience
Answer: A (LEAVE A REPLY)
CEH v13 emphasizes that after identifying vulnerabilities during scanning, testers must validate findings to determine real impact and eliminate false positives. This requires safe, controlled exploitation using approved tools such as Metasploit, Nikto, or custom proof-of-concept scripts. Misconfigurations labeled as medium-risk may still provide privilege escalation, data exposure, or footholds for further attacks. CEH methodology reinforces that exploitation should always follow the scope and rules of engagement and should avoid disruptive activities like brute-forcing or DoS attacks unless explicitly authorized. Ignoring the vulnerabilities is never acceptable in a professional assessment. Verifying the issue helps the organization prioritize remediation using evidence-based results. Therefore, the correct next step is to verify the vulnerability through controlled exploitation.

NEW QUESTION: 123
During security awareness training, which scenario best describes a tailgating social engineering attack?
A. An attacker impersonates a customer to recover account credentials
B. An attacker leaves a malicious USB labeled "Employee Bonus List"
C. A person gains access to a secure building by following an authorized employee through a locked door
D. An email urges employees to enter credentials for an urgent system update
Answer: C (LEAVE A REPLY)
The Certified Ethical Hacker (CEH) Social Engineering module defines tailgating as a physical social engineering attack where an unauthorized person follows an authorized individual into a restricted area.
Option C precisely matches CEH's definition.
Option A is pretexting.
Option B is baiting.
Option D is phishing.
CEH stresses physical security awareness as critical as cyber defenses.

NEW QUESTION: 124
A cyber adversary wants to enumerate firewall rules while minimizing noise and mimicking normal traffic behavior. Which reconnaissance technique enables mapping of firewall filtering behavior using TTL- manipulated packets?
A. Sending ICMP Echo requests to the network's broadcast address
B. Passive DNS monitoring to observe domain-to-IP relationships
C. Conducting full SYN scans on all ports for each discovered IP
D. Firewalking with manipulated TTL values to analyze ACL responses
Answer: D (LEAVE A REPLY)
Comprehensive Explanation from CEH v13 Courseware:
CEH v13 describes Firewalking as a reconnaissance technique designed to determine which layer-4 protocols and ports a firewall allows. The attacker sends packets with carefully adjusted TTL values so that the packet expires just beyond the firewall. If the next hop generates ICMP Time Exceeded responses, the attacker can infer which ports the firewall permits. This method mimics normal TTL behavior, making it stealthier than full SYN scans or high-noise probing. Firewalking is expressly highlighted in CEH as a low-profile way to map firewall ACLs without triggering alarms. Broadcast pings are noisy and detectable, passive DNS monitoring does not reveal firewall rule sets, and full SYN scans are easily flagged by IDS systems.
Firewalking's reliance on TTL behavior, combined with protocol-specific probes, makes it the correct and CEH-aligned technique for quietly discovering open ports and firewall filtering rules.

NEW QUESTION: 125
During a quarterly vulnerability management review at RedCore Motors, Priya finalizes the deployment of Nessus Essentials across the company's IT infrastructure. The solution is selected for its ability to support diverse technologies including operating systems, databases, web servers, and virtual environments. While preparing a training session for junior analysts, Priya asks them to identify a capability that Nessus Essentials is specifically designed to provide as part of its scanning process.
Which capability is Nessus Essentials specifically designed to provide?
A. Patch management for operating systems and third-party applications
B. High-speed asset discovery
C. Checks for outdated versions across a wide range of server and service technologies
D. Agent-based detection
Answer: (SHOW ANSWER)
The correct choice is C because Nessus Essentials is fundamentally a vulnerability assessment scanner. Its core purpose is to identify security weaknesses by checking systems and services against a large vulnerability knowledge base, which includes detecting outdated or vulnerable versions of operating systems, server software, databases, web servers, and common network services. In practical scanning, Nessus

performs remote checks such as banner/version identification, configuration and patch-level assessment (where possible), and vulnerability plugin checks to flag software releases that are known to be insecure or end-of- life. This directly matches the scenario emphasis: supporting "diverse technologies including operating systems, databases, web servers, and virtual environments," and asking for a capability it provides "as part of its scanning process." Why the other options are incorrect:
A (Patch management) is not what Nessus Essentials is designed to do. Nessus identifies missing patches and vulnerabilities, but it does not serve as an operating system and third-party application patch deployment platform.
B (High-speed asset discovery) is more characteristic of dedicated asset discovery/attack surface tools or broader platform features; while Nessus can discover hosts during scans, "high-speed asset discovery" is not the defining, primary capability being tested here.
D (Agent-based detection) refers to endpoint agents running locally for continuous monitoring. Nessus Essentials is primarily used for scanner-driven vulnerability assessment; agent-based functionality is a separate approach/tooling concept and not the main Essentials scanning capability being targeted in this question.
Therefore, the best answer is C: Nessus Essentials is designed to scan and identify vulnerabilities, including detecting outdated/vulnerable versions across many server and service technologies.

NEW QUESTION: 126
At a financial headquarters in Denver, Colorado, ethical hacker Jordan Lee moves beyond cataloging IoT devices and begins testing them for weaknesses. He runs specialized tools against smart lighting and HVAC systems to check for outdated firmware, default passwords, and open service ports. Which step of the IoT hacking methodology is Jordan carrying out?
A. Vulnerability scanning
B. Gain remote access
C. Information gathering
D. Launch attacks
Answer: A (LEAVE A REPLY)
Jordan is in the vulnerability scanning step because he has already moved past identification/cataloging (information gathering) and is now actively testing IoT devices for weaknesses such as outdated firmware, default credentials, and exposed/open service ports. In IoT hacking methodology, information gathering focuses on discovering devices, mapping the environment, identifying device types, interfaces, protocols, and versions, and understanding how data flows between endpoints, gateways, mobile apps, and cloud services.
Once that baseline inventory exists, the next step is to assess the devices and their ecosystem components for known and observable security gaps.

The specific checks described are classic vulnerability scanning targets in IoT environments:
Outdated firmware can indicate known vulnerabilities, missing security fixes, and unpatched components.
Default passwords are a common IoT weakness and can enable trivial compromise when not changed.
Open service ports reveal exposed management interfaces or unnecessary services that can be enumerated or exploited.
Running "specialized tools" to systematically evaluate these elements is consistent with vulnerability scanning because it is structured assessment aimed at finding exploitable conditions, but it stops short of actually exploiting or establishing persistence.
Why the other options do not fit:
Information gathering (C) would focus on identifying devices and collecting details, not actively checking them for outdated firmware/default passwords/open ports as vulnerabilities.
Gain remote access (B) implies exploitation or obtaining unauthorized control/access, which the scenario does not indicate-he is checking and assessing.
Launch attacks (D) implies executing exploitation, disruption, or compromise steps. The question explicitly frames this as testing for weaknesses, not carrying out attacks.
Therefore, Jordan is performing A. Vulnerability scanning.

NEW QUESTION: 127
Alice, a software developer, digitally signs an email contract and sends it to Bob. Later, a dispute arises and Alice claims she never sent the agreement. However, Bob produces the email with Alice's unique digital signature, which unequivocally links the message to her. In information security terms, what principle is illustrated by Bob's ability to prove Alice's authorship of the email?
A. Confidentiality
B. Integrity
C. Non-Repudiation
D. Availability
Answer: (SHOW ANSWER)
Non-repudiation is the security principle that prevents a sender from denying having performed a specific action, such as sending a message or approving a transaction. In CEH-aligned cryptography, non-repudiation is most commonly achieved using digital signatures backed by public key cryptography and, in many real- world deployments, supported by digital certificates and a trusted certificate authority. When Alice digitally signs the email contract, she uses her private key to create a signature that is mathematically tied to both her identity and the exact content of the message. Bob can then use Alice's corresponding public key to verify the signature. If verification succeeds, it

provides strong evidence that the message originated from the holder of Alice's private key and that the content has not been altered since it was signed.
This is different from confidentiality, which is about preventing unauthorized disclosure of message contents through encryption. It is also distinct from integrity alone: integrity ensures the message was not modified, but non-repudiation adds accountability by binding the action to a specific signer in a way that can be demonstrated to a third party.
Availability is unrelated here, as it concerns ensuring systems and data are accessible when needed.
CEH materials emphasize that non-repudiation depends on proper key management and trust infrastructure. If Alice's private key is compromised, the evidentiary value is weakened. Therefore, protecting private keys with secure storage, access controls, and revocation mechanisms is essential to preserve non-repudiation.

NEW QUESTION: 128
Which advanced session-hijacking technique is hardest to detect and mitigate?
A. Covert XSS attack
B. Man-in-the-Browser (MitB) attack
C. Passive sniffing on Wi-Fi
D. Session fixation
Answer: B (LEAVE A REPLY)
CEH v13 identifies Man-in-the-Browser (MitB) attacks as one of the most dangerous and difficult-to-detect session hijacking techniques, especially in online banking environments. In MitB attacks, malware operates inside the user's browser, intercepting and manipulating transactions in real time.
Unlike XSS or session fixation attacks, MitB bypasses server-side security controls entirely. Even strong encryption, multi-factor authentication, and secure cookies are ineffective because the attack occurs after authentication, within a trusted session.
Passive sniffing is limited by encryption, and session fixation relies on poor session management. Covert XSS requires injection points and is more easily mitigated.
CEH v13 emphasizes that MitB attacks can modify transaction details without user awareness, making detection extremely difficult. Therefore, Option B is correct.

NEW QUESTION: 129
A senior executive receives a personalized email titled "Annual Performance Review 2024." The email includes a malicious PDF that installs a backdoor when opened. The message appears to originate from the CEO and uses official company branding. Which phishing technique does this scenario best illustrate?
A. Email clone attack with altered attachments
B. Broad phishing sent to all employees
C. Pharming using DNS poisoning
D. Whaling attack targeting high-ranking personnel

Answer: D (LEAVE A REPLY)
The Certified Ethical Hacker (CEH) Social Engineering module defines whaling as a highly targeted phishing attack aimed specifically at senior executives or high-ranking personnel. This scenario exhibits all whaling characteristics: personalization, impersonation of leadership, business- themed content, and tailored malware delivery.
Option D is correct.
Option A involves copying legitimate emails, but does not necessarily target executives.
Option B lacks targeting.
Option C is unrelated to email-based attacks.
CEH stresses executive awareness training to counter whaling attacks.

NEW QUESTION: 130
During a red team operation on a segmented enterprise network, the testers discover that the organization's perimeter devices deeply inspect only connection-initiation packets (such as TCP SYN and HTTP requests).
Response packets and ACK packets within established sessions, however, are minimally inspected. The red team needs to covertly transmit payloads to an internal compromised host by blending into normal session traffic. Which approach should they take to bypass these defensive mechanisms?
A. Port knocking
B. SYN scanning
C. ICMP flooding
D. ACK tunneling
Answer: D (LEAVE A REPLY)
CEH teaches that certain advanced intrusion evasion techniques rely on understanding how firewalls differentiate between new connections and established traffic. Most perimeter firewalls scrutinize SYN packets and initial HTTP requests but allow ACK packets from established sessions to pass with minimal filtering. ACK tunneling leverages this behavior by embedding malicious payloads inside ACK packets, which appear to be part of a legitimate, pre-established session. Because ACK packets are often considered "safe," they bypass deep inspection engines, intrusion detection systems, and application-layer gateways. This method allows attackers to move data or commands covertly between compromised internal systems and external hosts. CEH references such evasion strategies when discussing bypassing stateful firewalls and making malicious traffic appear legitimate. Port knocking and SYN scans would initiate new connections- precisely what the firewall is heavily inspecting. ICMP flooding is noisy and easily detected. ACK tunneling is specifically designed for stealth and is aligned with red team tradecraft for avoiding packet-level inspection mechanisms.

NEW QUESTION: 131

An attacker uses many plaintext-ciphertext pairs and applies statistical analysis to XOR combinations of specific bits. Which technique is being used?

A. Brute-force attack

B. Differential cryptanalysis

C. Linear cryptanalysis

D. Side-channel attack

Answer: C (LEAVE A REPLY)

This scenario describes Linear Cryptanalysis, a technique detailed in CEH v13 Cryptography. Linear cryptanalysis involves finding linear approximations that relate plaintext bits, ciphertext bits, and key bits using XOR operations. By analyzing a large number of known plaintext-ciphertext pairs, attackers can identify statistical biases that reveal information about the secret key.

CEH v13 explains that linear cryptanalysis differs from differential cryptanalysis in its approach. While differential cryptanalysis studies how differences in plaintext affect differences in ciphertext, linear cryptanalysis focuses on linear relationships and probability distributions.

The mention of XOR combinations and statistical analysis of plaintext-ciphertext pairs directly aligns with linear cryptanalysis. Brute-force attacks attempt all keys without analysis. Differential cryptanalysis focuses on input differences, not linear equations. Side-channel attacks exploit physical characteristics such as power consumption or timing.

Modern block ciphers like AES are designed to resist linear cryptanalysis by ensuring that linear approximations occur with probabilities close to random. CEH v13 highlights linear cryptanalysis as a foundational attack method used to evaluate cipher strength.

Therefore, Option C is correct.

NEW QUESTION: 132

As part of a quarterly security review at EvoTrans Logistics, a global freight optimization firm, you have been brought in as a senior cybersecurity analyst to audit perimeter firewall configurations across cloud-hosted application clusters. During your investigation, you notice that TCP port 1433 is open on a virtual machine tagged as svc-node-east-14, which was provisioned by a now-defunct third-party vendor. The node is not referenced in any current infrastructure diagrams, yet live traffic logs suggest it is still handling requests during peak hours. No documentation exists regarding its service role, but you are tasked with flagging misconfigurations that may violate policy or expose critical services unnecessarily. Based on your understanding of standard port assignments, you must determine what service this port likely represents and whether its exposure warrants escalation.

Which of the following services is most likely running on this port and requires immediate review?

A. sqlsrv

B. SqlNet

C. ms-sql-s
D. ms-sql-m
Answer: C (LEAVE A REPLY)
TCP port 1433 is the well-known default port for Microsoft SQL Server, formally registered as ms-sql-s. In CEH network and perimeter security coverage, identifying services by their default port assignments is a critical reconnaissance and defensive skill. When reviewing firewall rules and exposed services, analysts correlate open ports with their associated protocols to determine risk exposure. Port 1433 is widely recognized as the primary listening port for Microsoft SQL Server instances configured with default settings.
The presence of an undocumented virtual machine actively handling traffic on port 1433 is particularly concerning because database services often store sensitive operational or customer data. If exposed unnecessarily, SQL Server can be targeted for brute-force authentication attacks, SQL injection exploitation, misconfiguration abuse, or exploitation of unpatched vulnerabilities. CEH materials emphasize that database services should not be directly exposed to the internet unless absolutely necessary and must be protected by strict access controls, segmentation, encryption, and monitoring.
Option B, SqlNet, typically refers to Oracle database communication over port 1521. Option D, ms-sql-m, is associated with SQL Server Browser service over UDP 1434, not TCP 1433. Option A, sqlsrv, is not the formal IANA-registered service name for port 1433. Because ms-sql-s is the standard designation for Microsoft SQL Server on TCP port 1433, and given the risk of exposing database services, this finding warrants immediate escalation and review.

NEW QUESTION: 133
An attacker performs DNS cache snooping using dig +norecurse. The DNS server returns NOERROR but no answer. What does this indicate?
A. The domain has expired
B. The record was cached and returned
C. The DNS server failed
D. No recent client from that network accessed the domain
Answer: D (LEAVE A REPLY)
In CEH v13 DNS Enumeration, DNS cache snooping determines whether a DNS resolver has a record cached. When +norecurse is used and the response is NOERROR with no answer, it means the server is authoritative but does not have the record cached.
CEH v13 explains that this suggests no internal client has recently queried the domain, making option D correct.

NEW QUESTION: 134
A penetration tester evaluates the security of an iOS mobile application that handles sensitive user information. The tester discovers that the application is vulnerable to insecure data transmission. What is the most effective method to exploit this vulnerability?

A. Execute a SQL injection attack to retrieve data from the backend server
B. Perform a man-in-the-middle attack to intercept unencrypted data transmitted over the network
C. Conduct a brute-force attack on the app's authentication system
D. Use a Cross-Site Request Forgery (CSRF) attack to steal user session tokens
Answer: B (LEAVE A REPLY)
The CEH v13 courseware states that insecure communication occurs when mobile applications transmit sensitive data over unencrypted or weakly encrypted channels, exposing information to interception. When an application uses plain HTTP or does not properly validate certificates, attackers can place themselves between the client and server using a man-in-the-middle (MitM) attack. This allows them to read session tokens, credentials, API keys, or personal user data as it travels across the network. CEH materials emphasize that MitM attacks are the primary exploitation technique for insecure data transmission because they exploit weaknesses in transport-layer security rather than weaknesses in backend code or authentication mechanisms.
SQL injection and CSRF attacks target web application logic, not transport encryption. Brute-force attacks target authentication mechanisms and are unrelated to how data is transmitted. Therefore, the most effective exploitation method is intercepting traffic via MitM to capture or manipulate unencrypted communications.

NEW QUESTION: 135
You are an ethical hacker at Apex Cyber Defense contracted to audit Coastal Healthcare's wireless estate in Miami, Florida. During a network sweep, your logs show a previously unknown access point physically connected to the hospital's internal switch and issuing IP addresses to devices on the corporate VLAN - it was neither provisioned by IT nor listed in the asset inventory. The device is relaying internal traffic and providing remote connectivity back to an external host. Based on the observed behavior, which wireless threat has the attacker most likely introduced?
A. Misconfigured AP
B. Rogue AP
C. Honeypot AP
D. Evil Twin AP
Answer: B (LEAVE A REPLY)
The correct answer is B. Rogue AP because the scenario describes an unauthorized access point that has been physically connected to the internal wired network and is providing network access on the corporate VLAN without approval or inventory records. In CEH-aligned wireless security concepts, a rogue access point is any AP that is installed on an organization's network without authorization, creating an unmanaged entry point that bypasses standard security controls. The key indicators here are: it is "previously unknown," "neither provisioned by IT nor listed in the asset inventory," and it is "physically connected to the hospital's internal switch." The fact that the device is issuing IP addresses

suggests it may be running a DHCP service or bridging into the internal network in a way that places clients directly onto the corporate VLAN. This can allow attackers to gain internal access from nearby wireless range and can also cause network instability if its DHCP responses conflict with the legitimate DHCP infrastructure. Additionally, the device "relaying internal traffic and providing remote connectivity back to an external host" points to an attacker using it as a covert foothold- effectively an unauthorized wireless bridge into the internal network and a channel for command-and-control or remote access.
Why not the other options: a misconfigured AP implies a legitimate AP deployed by IT but configured insecurely (weak encryption, default credentials, poor segmentation). A honeypot AP is typically deployed deliberately (often by defenders) to attract attackers for detection and research, not stealthy backhaul to an external host. An evil twin AP is a spoofed wireless AP that impersonates a legitimate SSID to lure victims; it does not necessarily require being physically plugged into the internal switch, and the defining trait is impersonation of a real AP/SSID. The defining trait here is unauthorized installation on the wired network, which is most directly a rogue access point.

NEW QUESTION: 136
At a smart retail outlet in San Diego, California, ethical hacker Sophia Bennett assesses IoT-based inventory sensors that synchronize with a cloud dashboard. She discovers that sensitive business records are sent across the network without encryption and are also stored in a retrievable format on the provider ' s cloud platform.
Which IoT attack surface area is most directly demonstrated in this finding?
A. Insecure ecosystem interfaces
B. Insecure data transfer and storage
C. Insecure network services
D. Insecure default settings
Answer: B (LEAVE A REPLY)
The finding most directly demonstrates insecure data transfer and storage. The scenario includes two explicit problems: (1) sensitive business records are transmitted "across the network without encryption," and (2) the same records are "stored in a retrievable format" in the cloud platform. Those two conditions map exactly to data-in-transit and data-at-rest weaknesses. When IoT devices transmit sensitive data without encryption (e.g., plain HTTP, unprotected MQTT, insecure proprietary protocols), attackers who gain network visibility can intercept, read, and potentially modify that data. Similarly, when cloud-stored data is kept in an easily retrievable or improperly protected form (e.g., weak access controls, lack of encryption at rest, overly permissive storage buckets, exposed APIs), attackers can access business records long after transmission.
In IoT ecosystems, data typically flows from sensors to gateways, then to cloud dashboards and analytics services. If encryption and strong access control are not consistently applied across these hops, confidentiality and integrity are at risk. This can lead to competitive harm (exposed inventory/business records), privacy impact (if customer

data is included), and operational disruption (tampered records leading to wrong decisions). The scenario is not about the IoT device exposing services like Telnet/FTP (network services), nor about default passwords; it is specifically about how data is transported and stored.
Why the other options are less accurate:
Insecure ecosystem interfaces (A) focuses on APIs, web/mobile apps, and cloud interfaces; while cloud storage access might involve interfaces, the core weakness described is lack of encryption and retrievable storage, which is more directly the data transfer/storage category.
Insecure network services (C) refers to exposed services/ports on IoT devices, not data confidentiality across the pipeline.
Insecure default settings (D) relates to factory defaults (passwords, open ports, insecure configs), not specifically unencrypted transport and weak storage protection.
Therefore, the correct answer is B. Insecure data transfer and storage.

NEW QUESTION: 137
Who are "script kiddies" in the context of ethical hacking?
A. Highly skilled hackers who write custom scripts
B. Novices who use scripts developed by others
C. Ethical hackers using scripts for penetration testing
D. Hackers specializing in scripting languages
Answer: (SHOW ANSWER)
In CEH v13 Information Security and Ethical Hacking Overview, script kiddies are defined as individuals with limited technical knowledge who rely on pre-written tools, scripts, and exploits created by others to carry out attacks. They typically lack a deep understanding of how the underlying exploits work.
CEH v13 categorizes attackers based on skill level and intent. Script kiddies sit at the lower end of the skill spectrum. They often download exploit kits, automated scanners, or attack frameworks and run them with minimal customization. While their attacks may be unsophisticated, they can still cause damage due to the availability of powerful tools.
Option B accurately reflects this definition. Options A and D describe skilled attackers or programmers, which contradicts the CEH classification. Option C is incorrect because

ethical hackers use tools responsibly with authorization and possess a strong understanding of security principles.
CEH v13 emphasizes that although script kiddies are less skilled, they pose a risk because automation allows them to exploit known vulnerabilities at scale. This is why organizations must patch systems promptly and implement baseline security controls.
Thus, Option B is the correct answer.

NEW QUESTION: 138
A penetration tester is assessing an IoT thermostat used in a smart home system. The device communicates with a cloud server for updates and commands. The tester discovers that communication between the device and the cloud server is not encrypted. What is the most effective way to exploit this vulnerability?
A. Conduct a Cross-Site Scripting (XSS) attack on the thermostat's web interface
B. Perform a brute-force attack on the thermostat's local admin login
C. Execute a SQL injection attack on the cloud server ' s login page
D. Use a man-in-the-middle (MitM) attack to intercept and manipulate unencrypted communication
Answer: D (LEAVE A REPLY)
IoT devices that transmit data without encryption expose all communication to interception. CEH explains that attackers can position themselves between the IoT device and cloud service to manipulate or capture traffic. A MitM attack enables interception of commands, credentials, and firmware data due to the absence of TLS protections.

NEW QUESTION: 139
During a cloud security assessment, you discover a former employee still has access to critical cloud resources months after leaving. Which practice would most effectively prevent this?
A. Real-time traffic analysis
B. Regular penetration testing
C. Enforcing timely user de-provisioning
D. Multi-cloud deployment
Answer: C (LEAVE A REPLY)
The CEH Cloud Security module highlights identity and access management (IAM) failures as a major source of cloud breaches. Ensuring timely de-provisioning of user accounts when employees leave is a core security control.
Option C is correct.
Options A and B detect issues but don't prevent access persistence.
Option D is unrelated to access control.
CEH stresses joiner-mover-leaver (JML) processes.

NEW QUESTION: 140

You discover a Web API integrated with webhooks and an existing administrative web shell. Your objective is to compromise the system while leaving minimal traces. Which technique is most effective?

A. SSRF to perform unauthorized API calls

B. IDOR exploitation

C. Upload malicious scripts via the web shell

D. Manipulate the webhook for unintended data transfer

Answer: A (LEAVE A REPLY)

Server-Side Request Forgery (SSRF) is emphasized in CEH v13 Web Application Hacking as a stealthy and powerful attack. SSRF allows attackers to make requests from the trusted server itself, bypassing firewalls, authentication, and logging controls.

Compared to web shells or webhook abuse, SSRF leaves fewer forensic artifacts and enables internal API access, metadata exposure, and lateral movement.

NEW QUESTION: 141

During a penetration test at Cascade Financial in Raleigh, ethical hacker Ethan Brooks evaluates the security of the company ' s authentication system. He observes that the application accepts a high volume of repeated credential submissions without introducing any additional challenge, allowing automated scripts to cycle rapidly through large password lists. Ethan advises the IT team to deploy a control that forces interaction steps designed to disrupt automation.

Which countermeasure should the IT team adopt in this scenario?

A. Use strong hashing algorithms

B. Implement 2FA/MFA

C. Use CAPTCHA challenges on login and registration pages

D. Force periodic password changes

Answer: C (LEAVE A REPLY)

The scenario describes an authentication endpoint that allows a high volume of repeated login attempts with no additional friction, enabling automated scripts to rapidly try large password lists. This is typical of online password guessing and credential stuffing/brute-force style automation. The countermeasure being requested is explicitly one that "forces interaction steps designed to disrupt automation," which best matches CAPTCHA.

CAPTCHA mechanisms introduce a challenge-response test intended to distinguish humans from automated bots, thereby reducing the effectiveness of scripted, high-rate credential attempts.

CAPTCHA is commonly deployed on login and registration pages (and sometimes on password reset flows) to slow down or block automated abuse. When triggered-often after a threshold of failed attempts or suspicious behavior-it forces the requester to complete an interactive step (image selection, puzzle, checkbox with behavioral analysis, etc.). This breaks fully automated attack loops and increases the attacker's cost, especially when

combined with additional controls such as account lockout thresholds, IP reputation, device fingerprinting, and rate limiting.
Why the other options are less aligned to the "disrupt automation" requirement:
Strong hashing algorithms (A) protect stored passwords at rest (e.g., if a database is compromised). They do not directly stop online automated login attempts.
2FA/MFA (B) is excellent for reducing account takeover impact, but it does not inherently prevent high- volume credential submissions; it adds a second factor after correct credentials are provided. Also, the question's wording strongly points to a bot-disruption interaction step.
Forced periodic password changes (D) is not a primary control for stopping automated login attempts and can introduce usability issues; it does not directly add friction to repeated submissions.
Therefore, the most appropriate countermeasure described is C. Use CAPTCHA challenges on login and registration pages.

NEW QUESTION: 142
While simulating a reconnaissance phase against a cloud-hosted retail application, your team attempts to gather DNS records to map the infrastructure. You avoid brute-forcing subdomains and instead aim to collect specific details such as the domain's mail server, authoritative name servers, and potential administrative information like serial number and refresh interval.
Given these goals, which DNS record type should you query to extract both administrative and technical metadata about the target zone?
A. MX
B. SOA
C. TXT
D. NS
Answer: B (LEAVE A REPLY)
The correct choice is the SOA record because it uniquely provides authoritative administrative and operational metadata about a DNS zone. In CEH reconnaissance techniques, DNS enumeration is a high-value passive and semi-passive method to learn about an organization's infrastructure without actively attacking hosts. The Start of Authority record defines core parameters of the zone and identifies the primary authoritative name server for that domain. Most importantly for this question, the SOA record contains fields that directly match "serial number and refresh interval," which are classic SOA elements used for zone replication and synchronization behavior between primary and secondary DNS servers.
An SOA record typically includes the primary name server, the responsible party field often formatted like an email address for the zone administrator, the zone serial number, and timing values such as refresh, retry, expire, and minimum TTL. These details can reveal

change frequency, operational practices, and sometimes administrative contact clues, all of which are relevant in reconnaissance and reporting.
The other record types do not meet the requirement. MX records identify mail exchangers for the domain but do not include serial or refresh parameters. NS records list authoritative name servers but lack administrative timing metadata. TXT records store arbitrary text such as SPF, DKIM, DMARC, or verification strings and are useful for email security posture analysis, but they do not provide the zone control fields the question references. Since the question explicitly calls out serial and refresh interval, the SOA record is the only option that fits completely.

NEW QUESTION: 143
At a Los Angeles-based online gaming company, penetration tester John investigates a recent cloud breach that caused downtime and delayed alerts. He finds that the root issue was management's lack of defined responsibilities for monitoring, auditing, and securing serverless services, which left critical functions unmanaged. Which cloud computing threat does this scenario best illustrate?
A. Insufficient logging and monitoring
B. Loss of governance
C. Privilege escalation
D. Side-channel attacks
Answer: B (LEAVE A REPLY)
The scenario best illustrates loss of governance because the core problem is not a specific technical exploit but a failure in management oversight, accountability, and control assignment for cloud/serverless security responsibilities. The question describes "lack of defined responsibilities for monitoring, auditing, and securing serverless services," resulting in critical functions being "unmanaged," which led to downtime and delayed alerts. That is a governance failure: the organization did not establish clear ownership, policies, and operational processes to ensure cloud workloads-specifically serverless functions-were properly monitored, audited, and secured.
In cloud environments, governance includes defining roles and responsibilities (shared responsibility model understanding), establishing security baselines, ensuring logging/monitoring coverage, enforcing configuration management, and maintaining compliance oversight. When governance is weak, services may be deployed without consistent security controls, alerts may be misconfigured or ignored, and incident response can be delayed because no team is clearly accountable. Serverless increases this risk because it can be rapidly adopted by developers, spun up quickly, and overlooked by traditional infrastructure processes if the organization's governance framework doesn't explicitly include it.
While "insufficient logging and monitoring" (A) is closely related, the scenario frames the root cause as management's lack of defined responsibilities, which is broader than missing logs. It's about the absence of governance structures that ensure logging/monitoring are

implemented and owned. Privilege escalation and side-channel attacks are technical attack categories not suggested by the description.
Therefore, the cloud threat illustrated is B. Loss of governance.

NEW QUESTION: 144
During a penetration test, you perform extensive DNS interrogation to gather intelligence about a target organization. Considering the inherent limitations of DNS-based reconnaissance, which of the following pieces of information cannot be directly obtained through DNS interrogation?
A. The specific usernames and passwords used by the organization's employees.
B. The estimated geographical location of the organization's servers derived from IP addresses.
C. The subdomains associated with the organization's primary internet domain.
D. The IP addresses associated with the organization's mail servers.
Answer: A (LEAVE A REPLY)
The CEH Footprinting and Reconnaissance module describes DNS interrogation as a valuable technique for extracting publicly available infrastructure information such as A records, MX records, NS records, and subdomains.
DNS can reveal:
Subdomains (via zone transfers, brute forcing, or enumeration)
Mail server IP addresses (MX records)
Server locations inferred from IP geolocation
However, DNS does not store authentication credentials. Usernames and passwords are protected within authentication systems and directories, not DNS records.
Therefore, option A is correct.
CEH clearly states that DNS reconnaissance is limited to infrastructure metadata, not sensitive user credentials.

NEW QUESTION: 145
In the neon-lit sprawl of Las Vegas, Nevada, a luxury hotel's smart room control system suffered a breach, allowing an intruder to manipulate guest room settings. The incident investigation revealed that the IoT devices lacked any mechanism to verify the integrity or authenticity of software prior to execution, allowing tampered instructions to run unchecked. As Emna Ruza, a cybersecurity consultant brought in to assess the breach, you recommend a solution that ensures only authorized, validated code is executed on the devices.
Which secure development practice are you advising the hotel to implement?
A. Allow code signing
B. Ensure secure boot
C. Secure firmware or software updates
D. Utilize secure communication protocols

Answer: A (LEAVE A REPLY)
The core weakness described is that the IoT devices "lack any mechanism to verify the integrity or authenticity of software prior to execution," which directly maps to the need for code signing. In CEH-aligned IoT security guidance, code signing ensures that firmware and software images are cryptographically signed by a trusted authority and verified on the device before they are installed or executed. This verification confirms two critical properties: integrity, meaning the code has not been altered or tampered with, and authenticity, meaning the code genuinely originated from an authorized publisher. If an attacker attempts to introduce modified binaries or malicious instructions, signature verification fails and the device can reject execution, preventing unauthorized code from running.
While secure boot is closely related, it is specifically a boot-time chain-of-trust mechanism that verifies the bootloader and early-stage firmware during startup. The question, however, emphasizes a general lack of verification "prior to execution," which is broader than boot only and is most directly addressed by code signing as a secure development and release practice. Secure firmware or software updates is also important, but secure updates typically rely on code signing as the fundamental control that makes updates trustworthy.
Secure communication protocols protect data in transit, but they do not stop tampered code already on the device from executing.
Therefore, the most appropriate secure development practice to ensure only authorized, validated code runs on the devices is to implement code signing with mandatory signature verification.

NEW QUESTION: 146
A security analyst is investigating a network compromise where malware communicates externally using common protocols such as HTTP and DNS. The malware operates stealthily, modifies system components, and avoids writing payloads to disk. What is the most effective action to detect and disrupt this type of malware communication?
A. Blocking commonly known malware ports such as 6667 and 12345.
B. Relying solely on frequent antivirus signature updates.
C. Using behavioral analytics to monitor abnormal outbound traffic and application behavior.
D. Blocking all unencrypted HTTP traffic at the proxy level.
Answer: (SHOW ANSWER)
The Certified Ethical Hacker (CEH) Malware Threats module explains that modern malware increasingly uses fileless techniques and living-off-the-land strategies, communicating over legitimate protocols like HTTP and DNS to evade detection. Because this traffic blends with normal activity, port-based blocking and signature-based antivirus are often ineffective. CEH highlights behavioral analytics and network traffic analysis as the most reliable detection mechanisms for identifying anomalies such as:

Unusual outbound DNS queries
Abnormal HTTP beaconing patterns
Suspicious process behavior
Option C is correct because it focuses on detecting behavioral anomalies, which CEH identifies as essential for combating advanced malware and command-and-control (C2) channels.
Option D may disrupt business operations and does not address DNS-based C2.
Option A is outdated.
Option B cannot detect unknown or fileless malware.
CEH strongly recommends anomaly detection and behavioral monitoring for advanced threats.

NEW QUESTION: 147
In your role as a cybersecurity analyst at a large e-commerce company, you have been tasked with reinforcing the firm's defenses against potential Denial-of-Service (DoS) attacks. During a recent review, you noticed several IP addresses generating excessive traffic, causing an unusually high server load. Inspection of packets revealed that the TCP three-way handshake was never completed, leaving multiple connections in a SYN_RECEIVED state. The intent appears to be saturating server resources without completing connections.
Which type of DoS attack is most likely being executed?
A. SYN Flood
B. Smurf Attack
C. Ping of Death
D. UDP Flood
Answer: A (LEAVE A REPLY)
This scenario clearly indicates a SYN Flood attack, a classic Denial-of-Service technique discussed in CEH v13 Network and Perimeter Hacking. In a normal TCP three-way handshake, a client sends a SYN, the server responds with SYN-ACK, and the client completes the connection with an ACK. In a SYN flood, attackers send a massive number of SYN packets but never complete the handshake.
As described in CEH v13, the server allocates memory and resources for each half-open connection, placing them in the SYN_RECEIVED state. When these connections are not finalized, the server's connection table becomes saturated, preventing legitimate users from establishing new sessions.
Other options are incorrect:
Smurf attacks rely on ICMP amplification, not TCP handshakes.
Ping of Death uses malformed ICMP packets.
UDP Floods overwhelm ports using UDP, not TCP session states.
CEH v13 emphasizes SYN floods as one of the most common Layer 4 DoS attacks due to their simplicity and effectiveness.

NEW QUESTION: 148
You are performing a security audit for a regional hospital in Dallas, Texas. While monitoring the network, you discover that an unknown actor has been silently capturing clear-text credentials and analyzing unencrypted traffic flowing across the internal Wi-Fi network. No modifications have been made to the data, and the attack remained undetected until your assessment. Based on this activity, what type of attack is most likely being conducted?
A. Passive attack
B. Distribution attack
C. Close-in attack
D. Insider attack
Answer: (SHOW ANSWER)
The correct answer is A. Passive attack because the activity described involves monitoring and capturing information without altering data, system resources, or communications. In CEH-aligned information security concepts, passive attacks are defined by the attacker's goal of eavesdropping-observing traffic to collect intelligence such as usernames/passwords, session identifiers, network patterns, or sensitive content-while making minimal changes that would trigger detection. The scenario explicitly states that the actor is "silently capturing clear-text credentials" and "analyzing unencrypted traffic," and that "no modifications have been made to the data." These are signature indicators of passive attacks such as packet sniffing and traffic analysis.
On an internal Wi-Fi network, passive attacks are particularly effective when encryption is weak or absent, or when users access services that transmit credentials in clear text. An attacker can capture packets and reconstruct sensitive information, especially where legacy protocols or misconfigurations exist. Because passive attackers do not need to inject or modify packets, they often avoid generating anomalies such as retransmissions, spoofed responses, or unexpected routing changes-helping them remain undetected, consistent with the prompt.
Why the other options do not fit: Distribution attack is not the standard classification for this behavior and does not specifically describe silent observation of traffic. Close-in attack refers to attacks that depend on physical proximity (e.g., shoulder surfing, physical tapping, local interception near the target). While Wi-Fi sniffing can require proximity, the defining characteristic in the question is the non-invasive observation with no data modification-i.e., passive attack. Insider attack relates to the attacker's identity/role (a trusted internal person), which is not established here; the scenario only describes behavior, not who the actor is.
Therefore, the described credential capture and traffic analysis without modification most clearly indicates a passive attack.

NEW QUESTION: 149

In Seattle, Washington, ethical hacker Mia Chen is hired by Pacific Trust Bank to test the security of their corporate network, which stores sensitive customer financial data. During her penetration test, Mia conducts a thorough reconnaissance, targeting a server that appears to host a critical database of transaction records. As she interacts with the server, she notices it responds promptly to her queries but occasionally returns error messages that seem inconsistent with a production system's behavior, such as unexpected protocol responses.
Suspicious that this server might be a decoy designed to monitor her actions, Mia applies a technique to detect inconsistencies that may reveal the system as a honeypot.
Which technique is Mia most likely using to determine if the server at Pacific Trust Bank is a honeypot?
A. Analyzing Response Time
B. Analyzing MAC Address
C. Fingerprinting the Running Service
D. Analyzing System Configuration and Metadata
Answer: C (LEAVE A REPLY)
Fingerprinting the running service is the most appropriate technique because the strongest indicator in the scenario is inconsistent protocol behavior and error responses that do not match a legitimate production database service. In CEH reconnaissance guidance, honeypots and decoy systems often emulate common services but may implement only partial protocol stacks or simplified responses. This can lead to anomalies such as incorrect banner strings, malformed or generic error messages, unsupported command handling, unusual protocol negotiation, or responses that do not align with the claimed software version. By fingerprinting, Mia compares observed behavior against expected behavior for the genuine service, including version-specific quirks, command sets, response codes, and timing patterns for particular requests.
In practice, service fingerprinting involves interacting with the service using legitimate and edge-case requests, validating banners and headers, and correlating results with known signatures from real implementations. If the server claims to be a specific database or application service but reacts in ways that real deployments would not, it suggests emulation, instrumentation, or deception typical of honeypots designed to log attacker activity.
Analyzing response time can help, because some honeypots respond too quickly or with uniform timing, but timing alone is less definitive than protocol inconsistencies. MAC address analysis is not reliable for identifying honeypots and is often not visible beyond the local segment. Analyzing system configuration and metadata usually requires deeper access than reconnaissance and is not the primary method when the clue is protocol-level mismatch. Therefore, fingerprinting the running service best fits the observed symptoms.

NEW QUESTION: 150

You perform a network scan using ICMP Echo Requests and observe that certain IP addresses do not return Echo Replies, while other network services remain functional. How should this situation be interpreted?

A. The scanned IPs are unused and available for expansion

B. The lack of replies indicates a major breach

C. A firewall or security control is blocking ICMP Echo Requests

D. The non-responsive IPs indicate severe congestion

Answer: (SHOW ANSWER)

According to CEH v13 Network Scanning and Enumeration, ICMP Echo Requests (ping) are commonly filtered by firewalls and intrusion prevention systems to reduce network reconnaissance exposure. When ICMP Echo Replies are not returned but other services remain operational, the most likely explanation is ICMP filtering rather than host unavailability or compromise.

CEH v13 explicitly states that many organizations configure firewalls to block ICMP Echo Requests while allowing other ICMP types or higher-layer protocols. This practice helps prevent attackers from easily mapping live hosts during the reconnaissance phase.

The other options are incorrect because:

Unused IPs would not necessarily have active services.

A breach would typically present additional symptoms.

Network congestion would affect multiple protocols, not just ICMP.

Thus, blocked ICMP is the correct interpretation.

NEW QUESTION: 151

Self-replicating malware causes redundant traffic, crashes, and spreads autonomously. What malware type is responsible, and how should it be handled?

A. Worm - isolate systems, scan network, update OS

B. Ransomware - disconnect, back up data, decrypt

C. Trojan - scan systems and patch

D. Rootkit - reboot and deploy scanner

Answer: A (LEAVE A REPLY)

This scenario describes a worm infection, as defined in CEH v13 Malware Threats. Worms are self- replicating malware that spread autonomously across networks without user interaction. Their propagation often results in excessive network traffic, system crashes, and resource exhaustion, which aligns with the symptoms described.

CEH v13 differentiates worms from other malware:

Ransomware encrypts data but does not self-propagate aggressively.

Trojans require user execution.

Rootkits focus on stealth and persistence rather than replication.

The appropriate response prioritizes containment and eradication. Quarantining affected systems prevents further spread. A network-wide antivirus sweep with updated signatures removes known worm variants.

Updating operating systems closes vulnerabilities that worms exploit for propagation. CEH v13 stresses rapid isolation and patching as critical measures to control worm outbreaks and restore network stability. Therefore, Option A is correct.

NEW QUESTION: 152
During a stealth assessment, an attacker exploits intermittent delays in ARP responses from a target system.
By injecting fake ARP replies before legitimate ones, the attacker temporarily redirects traffic to their own device, allowing intermittent packet capture. What type of sniffing attack is occurring?
A. Passive sniffing on a switched network
B. Duplicate IP conflict resolution attack
C. Switch port stealing via timing-based ARP spoofing
D. ARP poisoning for MiTM interception
Answer: (SHOW ANSWER)
CEH teaches that ARP-based attacks vary in sophistication from basic poisoning to more specialized techniques such as switch port stealing. In environments where ARP poisoning defenses or inspection tools limit traditional attacks, attackers may exploit timing vulnerabilities in ARP reply behavior. Switch port stealing works by sending spoofed ARP replies at precisely the right moment-before the legitimate ARP response from the target host-causing the switch's CAM table to update temporarily and associate the target' s IP address with the attacker's MAC address. CEH emphasizes that switches trust the latest ARP update, so even brief timing windows enable partial packet interception. This is different from fully persistent ARP poisoning, which continuously overwrites ARP tables, and from passive sniffing, which cannot capture unicast traffic on a switched network. This attack is particularly useful when ARP spoofing is mitigated because it relies on opportunistic timing rather than full table poisoning. The intermittent nature of intercepted packets matches CEH's description of switch port stealing behavior.

NEW QUESTION: 153

As an IT security analyst, you perform network scanning using ICMP Echo Requests. During the scan, several IP addresses do not return Echo Replies, yet other network services remain operational. How should this situation be interpreted?

A. The non-responsive IP addresses indicate severe network congestion.

B. A firewall or security control is likely blocking ICMP Echo Requests.

C. The lack of Echo Replies indicates an active security breach.

D. The IP addresses are unused and available for reassignment.

Answer: B (LEAVE A REPLY)

The CEH Network Scanning module explains that ICMP Echo Requests are often filtered or blocked by firewalls, routers, or host-based security controls as a defensive measure to reduce reconnaissance exposure.

When systems fail to respond to ICMP Echo Requests but continue to function normally for other services, CEH indicates that this behavior typically means ICMP traffic is being blocked, not that the host is offline or compromised.

Option B is correct.

Option A would affect all services.

Option C lacks supporting indicators.

Option D is speculative and unreliable.

CEH emphasizes that ICMP filtering is common in hardened networks.

NEW QUESTION: 154

Which best describes the role of a penetration tester?

A. Unauthorized malicious hacker

B. Malware distributor

C. Authorized security professional who exploits vulnerabilities

D. Malicious code developer

Answer: C (LEAVE A REPLY)

In CEH v13 Information Security and Ethical Hacking Overview, a penetration tester is defined as a trusted, authorized security professional hired to simulate real-world attacks in order to identify and exploit vulnerabilities with explicit permission.

The primary objectives of a penetration tester are:

Identify weaknesses in systems, networks, and applications

Demonstrate real-world impact of vulnerabilities

Help organizations improve their security posture

Unlike malicious hackers (Option A) or malware authors (Options B and D), penetration testers operate under strict legal and ethical guidelines, following scopes of engagement and reporting findings responsibly.

CEH v13 emphasizes that penetration testing is proactive defense, not crime. Therefore, Option C accurately defines the role.

NEW QUESTION: 155

A penetration tester is testing a web application's product search feature, which takes user input and queries the database. The tester suspects inadequate input sanitization. What is the best approach to confirm the presence of SQL injection?
A. Inject a script to test for Cross-Site Scripting (XSS)
B. Input DROP TABLE products; -- to see if the table is deleted
C. Enter 1' OR '1'='1 to check if all products are returned
D. Use directory traversal syntax to access restricted files on the server
Answer: C (LEAVE A REPLY)
Tautology-based SQL injection tests, such as using ' OR '1'='1, are safe and effective methods to verify whether SQL queries are being manipulated by user input. CEH emphasizes avoiding destructive queries and using logical expressions that return all rows if injection is successful.

NEW QUESTION: 156
You must map open ports and services while remaining stealthy and avoiding IDS detection. Which scanning technique is best?
A. FIN Scan
B. TCP Connect Scan
C. ACK Scan
D. Stealth Scan (SYN Scan)
Answer: D (LEAVE A REPLY)
The TCP SYN scan, also known as a Stealth Scan, is emphasized in CEH v13 Network Scanning as the most effective balance between accuracy and stealth. It sends a SYN packet and analyzes the response without completing the TCP handshake.
Because the connection is never fully established, SYN scans are less likely to be logged by applications and are harder for IDS systems to detect compared to TCP Connect scans. FIN and ACK scans are used for firewall rule mapping and evasion, but they do not reliably enumerate services. TCP Connect scans are noisy and easily detected. Therefore, Stealth (SYN) Scan is the best choice.

NEW QUESTION: 157
A tester evaluates a login form that builds SQL queries using unsanitized input. By submitting a single quote ('), the tester bypasses authentication and logs in. What type of SQL injection occurred?
A. UNION-based SQL injection
B. Error-based SQL injection
C. Time-based blind SQL injection
D. Tautology-based SQL injection
Answer: (SHOW ANSWER)

The CEH Web Application Attacks module explains tautology-based SQL injection as an attack where input alters a conditional statement to always evaluate as TRUE (e.g., ' OR '1'='1').
Submitting a single quote often breaks query logic and allows attackers to manipulate authentication conditions.
Option D is correct.
Option A extracts data.
Option B relies on error messages.
Option C uses timing delays.
CEH identifies tautology attacks as one of the earliest and most common SQL injection techniques.

NEW QUESTION: 158
Which WPA vulnerability allowed packet injection and decryption attacks?
A. Lack of AES encryption
B. Predictable GTK
C. Weak Initialization Vectors (IVs)
D. Weak passwords
Answer: C (LEAVE A REPLY)
WPA with TKIP suffers from vulnerabilities inherited from WEP, particularly the use of weak Initialization Vectors (IVs). CEH v13 explains that these weaknesses allow attackers to perform packet injection and partial decryption attacks.
Although WPA improved upon WEP, TKIP was designed as a temporary solution and still relies on predictable IV behavior. This makes Option C correct.
Lack of AES (Option A) explains why WPA is weaker than WPA2 but does not directly describe the exploit mechanism. Weak passwords (Option D) affect authentication, not packet injection. GTK predictability (Option B) is relevant but not the primary cause here.
CEH v13 explicitly states that IV reuse and predictability in TKIP enable practical attacks. Therefore, Option C is correct.

NEW QUESTION: 159
A penetration tester evaluates a secure web application using HTTPS, secure cookies, and multi-factor authentication. To hijack a legitimate user's session without triggering alerts, which technique should be used?
A. Exploit a browser zero-day vulnerability to inject malicious scripts
B. Implement a man-in-the-middle attack by compromising a trusted network device
C. Perform a Cross-Site Request Forgery (CSRF) attack to manipulate session tokens
D. Utilize a session token replay attack by capturing encrypted tokens
Answer: C (LEAVE A REPLY)
CEH v13 describes Cross-Site Request Forgery (CSRF) as a technique that forces authenticated users to unknowingly execute actions within a web application without their

intent. Unlike session hijacking methods that require stealing or replaying session cookies, CSRF exploits the trust relationship that the server has with a user's browser. Even with HTTPS, secure cookies, and MFA, once a user is authenticated, the browser automatically sends session cookies with each request. If the attacker convinces the victim to load a maliciously crafted webpage or URL, the browser sends a forged request to the target application, executing actions under the user's authenticated session. CEH notes that secure cookies and MFA do not stop CSRF because no credentials are stolen-only forced actions occur. This technique is sophisticated because it leaves minimal traces, avoids direct cookie manipulation, bypasses robust authentication mechanisms, and leverages design weaknesses rather than technical misconfigurations. Protection typically requires anti-CSRF tokens and proper origin validation.

NEW QUESTION: 160
A penetration tester intercepts HTTP requests between a user and a vulnerable web server. The tester observes that the session ID is embedded in the URL, and the web application does not regenerate the session upon login. Which session hijacking technique is most likely to succeed in this scenario?
A. Injecting JavaScript to steal session cookies via cross-site scripting
B. DNS cache poisoning to redirect users to fake sites
C. Session fixation by pre-setting the token in a URL
D. Cross-site request forgery exploiting user trust in websites
Answer: C (LEAVE A REPLY)
This scenario demonstrates a classic case of Session Fixation, a session hijacking technique explicitly covered under the CEH v13 Web Application Hacking module. Session fixation occurs when an attacker sets or predicts a valid session identifier and forces a victim to authenticate using that same session ID.
In the given question, two critical vulnerabilities are highlighted:
* The session ID is embedded in the URL
* The application does not regenerate the session ID after login
According to CEH v13, secure applications must regenerate session identifiers after successful authentication to prevent fixation attacks. If this does not occur, an attacker can craft a URL containing a known session ID and trick the victim into clicking it. Once the victim logs in, the attacker reuses the same session ID to gain unauthorized access.
CEH documentation states that session fixation is particularly effective when:
* Session IDs are passed via URL parameters
* Sessions persist across authentication
* Secure cookie attributes are not enforced
Other options are incorrect because:
* XSS-based cookie theft requires client-side script injection.
* DNS cache poisoning is unrelated to session management.
* CSRF exploits user trust but does not directly hijack sessions.

Thus, Session Fixation by pre-setting the token in a URL is the most effective attack in this case.

NEW QUESTION: 161
A penetration tester gains access to a target system through a vulnerability in a third-party software application. What is the most effective next step to take to gain full control over the system?
A. Conduct a denial-of-service (DoS) attack to disrupt the system's services
B. Execute a Cross-Site Request Forgery (CSRF) attack to steal session data
C. Perform a brute-force attack on the system's root password
D. Use a privilege escalation exploit to gain administrative privileges on the system
Answer: D (LEAVE A REPLY)
According to the CEH attack methodology, once an attacker obtains initial access-whether through exploitation, misconfiguration, or credential compromise-the next critical phase is privilege escalation.
Gaining system-level or administrative control is essential for maintaining persistence, accessing protected data, modifying system configurations, and pivoting further into the network. Privilege escalation exploits target kernel flaws, misconfigured services, improper permission settings, or vulnerable drivers. CEH emphasizes that performing a DoS attack disrupts the engagement and provides no strategic advantage.
Similarly, CSRF targets web applications rather than operating systems, and brute-force password attempts are inefficient, noisy, and often ineffective once local access has already been established. By leveraging privilege escalation techniques, the tester converts limited user access into full system control, enabling comprehensive post-exploitation activities aligned with CEH system hacking procedures.

NEW QUESTION: 162
A major financial institution is experiencing persistent DoS attacks against online banking, disrupting transactions. Which sophisticated DoS technique poses the greatest challenge to detect and mitigate effectively, potentially jeopardizing service availability?
A. A synchronized Layer 3 Smurf attack flooding routers with ICMP echo requests
B. A distributed SQL injection attack against online banking database servers causing resource exhaustion
C. A zero-day buffer overflow exploit against the web server causing service unavailability via RCE
D. A coordinated UDP flood targeting authoritative DNS servers to disrupt domain resolution
Answer: (SHOW ANSWER)
CEH emphasizes that application-layer DoS attacks are often the most difficult to detect and mitigate because they can mimic legitimate user behavior while exhausting backend resources. A distributed SQL injection- driven DoS (Option B) can be especially

challenging: attackers send requests that appear valid at the HTTP level, but the injected or crafted parameters force the application/database to execute expensive queries (heavy joins, sleep/delay functions, or costly operations). When distributed across many sources, the traffic can look like normal customer usage-successful TCP handshakes, valid HTTP requests, and realistic user- agent patterns-while still causing database connection pool exhaustion, CPU spikes, lock contention, and degraded response times.
Option A (Smurf) and Option D (UDP/DNS flooding) are more volumetric/network-layer patterns and are typically mitigated with upstream DDoS scrubbing, rate limiting, and filtering, and are more readily detectable via traffic anomalies. Option C (zero-day RCE) is severe, but it is not primarily a "DoS technique" in CEH classification; it's an exploitation scenario that may lead to service outage, but the detection
/mitigation path centers on exploit prevention, EDR, patching, and containment rather than DoS controls. In CEH terms, Option B aligns best with a sophisticated, scenario-like DoS that blends into normal app activity.
CEH mitigation approaches for application-layer DoS include WAF rules, input validation/parameterization (preventing SQLi), query cost controls, rate limiting by behavior, caching, database hardening, and anomaly detection at the application and database tiers.

NEW QUESTION: 163
A senior executive receives a personalized email with the subject line "Annual Performance Review 2024." The email contains a downloadable PDF that installs a backdoor when opened. The email appears to come from the CEO and includes company branding. Which phishing method does this best illustrate?
A. Broad phishing sent to all employees
B. Pharming using DNS poisoning
C. Whaling attack aimed at high-ranking personnel
D. Email clone attack with altered attachments
Answer: C (LEAVE A REPLY)
This scenario is a textbook example of a Whaling Attack, a highly targeted phishing technique described in the CEH v13 Social Engineering module. Whaling specifically targets senior executives or high-ranking individuals, exploiting their authority, access privileges, and decision-making roles.
In the given case, the attacker crafts a personalized email, impersonates the CEO, and uses legitimate corporate branding to build trust. The malicious PDF attachment delivers a backdoor, aligning with CEH v13 descriptions of advanced spear-phishing techniques used against executives.
CEH v13 differentiates whaling from other phishing types:
Broad phishing targets large groups indiscriminately.
Pharming redirects users via DNS manipulation.
Email clone attacks copy legitimate emails but typically target peers, not executives.

Whaling attacks are particularly dangerous because executives often bypass security scrutiny and possess elevated system access. CEH v13 emphasizes executive awareness training as a key mitigation strategy.
Therefore, the correct answer is Whaling attack aimed at high-ranking personnel.

NEW QUESTION: 164
In Seattle, Washington, ethical hacker Mia Chen is tasked with testing the network defenses of Pacific Shipping Co., a major logistics firm. During her penetration test, Mia targets the company's external-facing web server, which handles customer tracking requests. She observes that the security system filtering traffic to this server analyzes incoming SSH and DNS requests to block unauthorized access attempts. Mia plans to craft specific payloads to bypass this system to expose vulnerabilities to the IT department.
Which security system is Mia attempting to bypass during her penetration test of Pacific Shipping Co.'s web server?
A. Stateful Multilayer Inspection Firewall
B. Application-Level Firewall
C. Packet Filtering Firewall
D. Circuit-Level Gateway Firewall
Answer: B (LEAVE A REPLY)
An Application-Level Firewall, commonly called an application-level gateway or proxy firewall, inspects traffic at the application layer and enforces rules based on specific application protocols and commands. In CEH-aligned coverage of perimeter defenses, this firewall type is distinguished by its ability to understand protocol behavior and content for services such as DNS and SSH, rather than relying only on IP addresses, ports, and basic connection state.
The question states the filtering system "analyzes incoming SSH and DNS requests to block unauthorized access attempts." That wording points directly to application-aware inspection: it is evaluating protocol- specific requests, not merely allowing or denying traffic based on port numbers. A packet filtering firewall generally makes decisions using network and transport layer information such as source and destination IP, protocol, and port, without parsing DNS queries or SSH negotiation details. A circuit-level gateway firewall focuses on validating session establishment and connection properties, typically without deep inspection of the application commands inside the session. A stateful multilayer inspection firewall can track connection state and sometimes incorporate deeper inspection, but the strongest and most explicit match to "analyzes SSH and DNS requests" in CEH terminology is the application-level firewall, which uses proxies or protocol engines to parse and filter application traffic.
From an ethical testing perspective, attempts to "craft specific payloads" often involve probing how the firewall validates protocol fields, handles malformed requests, or enforces policy on application commands.

Defenders mitigate these risks through strict proxy policy configuration, robust protocol validation, patching, logging, and limiting exposed services to only what is required.

NEW QUESTION: 165
Which scenario best describes a slow, stealthy scanning technique?
A. FIN scanning
B. TCP connect scanning
C. Xmas scanning
D. Zombie-based idle scanning
Answer: D (LEAVE A REPLY)
CEH v13 identifies Idle (Zombie) Scanning as one of the most stealthy reconnaissance techniques. In this method, attackers use a third-party system (the zombie) to send probes to the target, obscuring the attacker's true identity.
Because the attacker never directly interacts with the target, detection and attribution become extremely difficult. FIN and Xmas scans are stealthy but still originate from the attacker's IP. TCP connect scans are noisy and easily detected.
CEH v13 highlights idle scanning as the gold standard for stealth reconnaissance, making option D correct.

NEW QUESTION: 166
During a penetration test at an e-commerce company in Boston, ethical hacker Sophia launches an HTTP flood against the checkout page of the site. The simulated traffic consists of repeated GET and POST requests designed to overload application-layer resources. In response, the IT team activates a security tool that inspects and filters malicious HTTP traffic while allowing legitimate customer requests to pass, ensuring service continuity during the exercise.
Which DoS/DDoS protection tool is most likely being used in this scenario?
A. Load Balancer
B. Web Application Firewall
C. Intrusion Prevention System
D. Firewall
Answer: B (LEAVE A REPLY)
An HTTP flood is an application-layer (Layer 7) DoS/DDoS technique that targets web application resources by sending large volumes of seemingly valid HTTP GET/POST requests. Because the traffic can look
"legitimate" at the protocol level, controls that primarily focus on network/transport characteristics (such as basic firewalls) are often insufficient. The tool described in the scenario is explicitly inspecting and filtering malicious HTTP traffic while allowing legitimate customer requests-that behavior aligns most directly with a Web Application Firewall (WAF).

A WAF is designed to protect web applications by analyzing HTTP/S requests and responses, applying security rules that detect and block abnormal or malicious patterns. In an HTTP flood scenario, a WAF can enforce rate limiting, detect request anomalies (e.g., repeated requests to resource-intensive endpoints like checkout), identify bot-like behavior, and apply signatures/behavioral policies to mitigate attacks while continuing to permit valid users. The key clue is the focus on HTTP-level inspection and filtering to maintain service continuity-a classic WAF use case during Layer 7 attacks.
Why the other options are less suitable:
A Load Balancer (A) improves availability by distributing traffic across servers, but it does not inherently inspect and filter malicious HTTP requests. It can help absorb load, yet it's not primarily a security inspection
/filtering control.
An Intrusion Prevention System (C) can block malicious activity, but many IPS deployments are stronger at network/transport-layer patterns and may not provide the same depth of application-aware HTTP policy enforcement as a WAF for targeted web endpoints.
A traditional Firewall (D) mainly filters by IP/port/protocol and cannot reliably distinguish malicious vs legitimate HTTP GET/POST floods when they use allowed ports (80/443).

NEW QUESTION: 167
A penetration tester targets a WPA2-PSK wireless network. The tester captures the handshake and wants to speed up cracking the pre-shared key. Which approach is most effective?
A. Conduct a Cross-Site Scripting (XSS) attack on the router ' s login page
B. Use a brute-force attack to crack the pre-shared key manually
C. Use a dictionary attack with a large wordlist to crack the WPA2 key
D. Perform a SQL injection attack to bypass the WPA2 authentication
Answer: (SHOW ANSWER)
CEH v13 explains that WPA2-PSK security relies on the strength of the pre-shared key. Once the 4-way handshake is captured, the attacker must attempt offline cracking. CEH emphasizes that the dictionary attack is the most efficient and commonly used cracking method because it tests structured wordlists, human-derived passwords, and hybrid

permutations, dramatically reducing time compared to full brute force. Brute forcing (Option B) is computationally heavy and often impractical unless the password is extremely short. XSS (Option A) and SQL injection (Option D) have no relevance to WPA2 authentication, which occurs at the wireless protocol level, not the router's web interface. The dictionary attack is highlighted in CEH as the principal technique used with tools like aircrack-ng, hashcat, and pyrit, allowing rapid key testing using optimized GPU or CPU cracking. Thus, Option C is the most effective and CEH-aligned method.

NEW QUESTION: 168
Bob, a seasoned security analyst at XYZ Aerospace, was investigating a series of misaligned transaction timestamps coming from one of the data archival systems. Suspecting that the server might be syncing with an unstable time source, Bob decided to extract a detailed list of all peer servers associated with the target machine, including metrics such as delay, offset, and jitter, to determine whether the issue stemmed from time synchronization drift.
Which of the following commands should Bob use to retrieve this information?
A. ntptrace [-n] [-m maxhosts] [servername/IP_address]
B. ntpq -p [host]
C. ntpdc [-n] [-s] [-c command] [host] [...]
D. ntpq [-n] [-l] [-c command] [host] [...]
Answer: B (LEAVE A REPLY)
The command that best matches Bob's goal is ntpq -p. In CEH-aligned coverage of network services and operational troubleshooting, NTP is highlighted as a critical dependency because inaccurate time can break authentication, distort logs, and cause incorrect transaction ordering. When investigating suspected time drift, the most useful first step is to view the active NTP associations and their quality metrics. The ntpq utility queries an NTP daemon and reports peer status and performance data. Specifically, ntpq -p displays a peer table that includes each configured or discovered time source along with fields such as delay, offset, and jitter.
These values help determine whether the server is locked to a stable source or being influenced by a poor or rogue time server. Offset indicates how far the local clock differs from the peer, delay reflects network latency to the peer, and jitter shows the variability in timing measurements, all of which are directly mentioned in the question.
Option A, ntptrace, is used to trace the chain of NTP servers back to a reference clock and is useful for understanding hierarchy, but it does not provide the detailed delay, offset, and jitter peer metrics in the same way. Option C, ntpdc, is an older monitoring tool that can query NTP, but CEH references more commonly emphasize ntpq for peer statistics and associations. Option D is a generic ntpq invocation with interactive command support, but the -p option is the explicit mode that outputs the peer list with the required metrics.

NEW QUESTION: 169

A penetration tester is attempting to gain access to a wireless network that is secured with WPA2 encryption.
The tester successfully captures the WPA2 handshake but now needs to crack the pre-shared key. What is the most effective method to proceed?
A. Perform a brute-force attack using common passwords against the captured handshake
B. Use a dictionary attack against the captured WPA2 handshake to crack the key
C. Execute a SQL injection attack on the router's login page
D. Conduct a de-authentication attack to disconnect all clients from the network
Answer: (SHOW ANSWER)
WPA2-PSK networks authenticate users using a pre-shared key derived from a passphrase. After capturing the 4-way handshake, CEH teaches that the standard and most effective method to recover the key is to perform an offline dictionary attack, where wordlist entries are hashed and compared against the captured handshake values. Offline cracking avoids detection and is significantly faster than brute-force attempts.

NEW QUESTION: 170
A security analyst is tasked with gathering detailed information about an organization's network infrastructure without making any direct contact that could be logged or trigger alarms. Which method should the analyst use to obtain this information covertly?
A. Examine leaked documents or data dumps related to the organization
B. Use network mapping tools to scan the organization's IP range
C. Initiate social engineering attacks to elicit information from employees
D. Perform a DNS brute-force attack to discover subdomains
Answer: (SHOW ANSWER)
Passive reconnaissance focuses on collecting intelligence without interacting with the target's systems. CEH materials emphasize reviewing publicly available information, including leaked documents, breach data, reports, or exposed metadata, as this yields internal network structure details while generating no detectable traffic. This method avoids triggering monitoring systems and aligns with stealth requirements for covert intelligence gathering.

NEW QUESTION: 171
Michael, an ethical hacker at a San Francisco-based fintech startup, is conducting a security assessment of the company's cloud-based payment processing platform, which uses Kubernetes, an open-source system for automating the deployment, scaling, and management of containerized applications. During his review, Michael identified a feature that automatically replaces and reschedules containers from failed nodes to ensure high availability of services a critical requirement for uninterrupted payment operations. Based on his study of cloud container technology principles, which Kubernetes feature should Michael highlight as responsible for this capability?
A. Container vulnerabilities

B. Kube-controller-manager
C. Container orchestration
D. Self-healing
Answer: D (LEAVE A REPLY)
The capability described is Kubernetes self-healing, a core behavior emphasized in CEH cloud and container security coverage when discussing resilience, availability, and fault tolerance in containerized environments.
Self-healing means Kubernetes continuously monitors the desired state of workloads and automatically acts when the current state deviates due to failures. If a node crashes, a container exits unexpectedly, or a pod becomes unhealthy, Kubernetes responds by restarting containers, recreating pods, and rescheduling workloads onto healthy nodes to maintain service continuity. This directly matches the scenario where containers are "automatically replaced and rescheduled" from failed nodes to keep payment services highly available.
While several Kubernetes components participate in achieving this outcome, the feature name most aligned with the described behavior is self-healing. Kubernetes uses controllers and the scheduler to implement it:
deployments and replica sets ensure the correct number of pod replicas exist; liveness and readiness probes detect unhealthy containers; and when nodes become NotReady, pods are evicted and recreated elsewhere.
This is exactly how Kubernetes supports uninterrupted operations for critical applications such as payment processing platforms.
Option B, kube-controller-manager, is a control-plane component that runs multiple controllers, and it contributes to enforcing desired state, but the question asks for the feature capability rather than the specific internal process that provides it. Option C, container orchestration, is broader and includes deployment, scaling, and management, but it is less precise than self-healing for the specific behavior of automatic replacement and rescheduling after failures. Option A is unrelated to availability behavior.

NEW QUESTION: 172
During a red team assessment, an ethical hacker must map a large multinational enterprise's external attack surface. Due to strict rules of engagement, no active scans may be used. The goal is to identify publicly visible subdomains to uncover forgotten or misconfigured services. Which method should the ethical hacker use to passively enumerate the organization's subdomains?
A. Leverage tools like Netcraft or DNSdumpster to gather subdomain information
B. Attempt to guess admin credentials and access the company's DNS portal
C. Conduct a brute-force DNS subdomain enumeration
D. Request internal DNS records using spoofed credentials
Answer: (SHOW ANSWER)

CEH clearly distinguishes between active and passive reconnaissance. Passive methods involve gathering publicly available data without directly interacting with the target's infrastructure, thus avoiding detection.
Tools such as Netcraft, DNSdumpster, VirusTotal, Certificate Transparency logs, and search engine indexing are recommended by CEH for discovering subdomains through public metadata, cached DNS records, WHOIS data, SSL certificate entries, and third-party enumeration databases. These platforms provide insights into externally accessible assets without sending packets or queries to the target organization. Brute- force enumeration is active and violates the rules of engagement. Attempting credential guessing or requesting internal DNS data are unauthorized and clearly active reconnaissance activities. Passive OSINT- based subdomain enumeration is a core CEH technique used to uncover hidden infrastructure safely and legally. It is especially crucial in red team operations where stealth is a priority.

NEW QUESTION: 173
A penetration tester suspects that the web application's "Order History" page is vulnerable to SQL injection because it displays user orders based on an unprotected user ID parameter in the URL. What is the most appropriate approach to test this?
A. Inject JavaScript into the URL parameter to test for Cross-Site Scripting (XSS)
B. Modify the URL parameter to userID=1 OR 1=1 and observe if all orders are displayed
C. Perform a directory traversal attack to access sensitive system files
D. Use a brute-force attack on the login form to identify valid user credentials
Answer: B (LEAVE A REPLY)
CEH v13 identifies URL parameters used in dynamic SQL queries as common injection points. When user- controlled values are passed directly into database queries without validation, attackers can manipulate query logic. Injecting a test payload such as 1 OR 1=1 into the userID parameter is a standard method to determine whether the application concatenates input into SQL statements. If the page displays all user orders instead of only the authenticated user's orders, this confirms SQL injection. CEH teaches that conditional tautologies are one of the safest and most reliable ways to probe SQL vulnerabilities, especially in GET parameters.
JavaScript injection (Option A) tests XSS, not SQLi. Directory traversal (Option C) targets filesystem issues, not database logic. Brute-forcing user credentials (Option D) does not test query sanitization. Therefore, modifying the userID parameter with a SQL injection payload is the correct CEH-aligned method.

NEW QUESTION: 174
A critical flaw exists in a cloud provider's API. What is the most likely threat?
A. Physical security breaches
B. Unauthorized access to cloud resources
C. DDoS attacks

D. Compromise of encrypted data at rest

Answer: (SHOW ANSWER)

In CEH v13 Cloud Computing, APIs are identified as the primary control plane for managing cloud resources.

A vulnerability in a cloud API can allow attackers to bypass authentication, escalate privileges, and manipulate resources.

Unauthorized access may lead to:

Data exposure

Resource abuse

Account takeover

Lateral movement within the cloud environment

Physical security (Option A) and encryption at rest (Option D) are unrelated to API flaws.

DDoS attacks (Option C) are possible but not the primary risk of API vulnerabilities.

Thus, Option B is correct.

NEW QUESTION: 175

Which advanced session hijacking technique is hardest to detect and mitigate in a remote-access environment?

A. Session sidejacking over public Wi-Fi

B. ARP spoofing on local networks

C. Brute-force session guessing

D. Cookie poisoning

Answer: B (LEAVE A REPLY)

ARP spoofing-based session hijacking is identified in CEH v13 Web Application and Network Attacks as one of the most stealthy and difficult-to-detect session compromise techniques, especially within internal or VPN-connected networks.

In ARP spoofing, attackers poison ARP caches to position themselves as a man-in-the-middle (MitM). Once in place, they can silently intercept, modify, or replay session data-even when encryption is used-by redirecting traffic transparently between endpoints.

Option A (sidejacking) is mitigated by HTTPS. Option C (session guessing) is noisy and detectable. Option D (cookie poisoning) relies on weak validation and is easier to detect via integrity checks.

CEH v13 highlights ARP spoofing as particularly dangerous because:

* It exploits trusted local network behavior
* It does not require breaking encryption directly
* It is often invisible to users and applications

Therefore, Option B is the most challenging to detect and mitigate and is the correct answer.

NEW QUESTION: 176

A penetration tester runs a vulnerability scan and identifies an outdated version of a web application running on the company's server. The scan flags this as a medium-risk vulnerability. What is the best next step for the tester?

A. Ignore the vulnerability since it is only flagged as medium-risk

B. Brute-force the admin login page to gain unauthorized access

C. Perform a denial-of-service (DoS) attack to crash the web application

D. Research the vulnerability to check for any available patches or known exploits

Answer: D (LEAVE A REPLY)

CEH methodology emphasizes validating and researching identified vulnerabilities to determine exploitability, patch status, and business impact. Even medium-risk findings require investigation to assess their real severity.

NEW QUESTION: 177

A penetration tester completes a vulnerability scan showing multiple low-risk findings and one high-risk vulnerability tied to outdated server software. What should the tester prioritize as the next step?

A. Perform a brute-force attack on the server to gain access

B. Ignore the high-risk vulnerability and proceed with testing other systems

C. Focus on exploiting the low-risk vulnerabilities first

D. Verify if the high-risk vulnerability is exploitable by checking for known exploits

Answer: (SHOW ANSWER)

CEH methodology stresses prioritization based on risk, exploitability, and business impact. High-severity vulnerabilities-especially those related to outdated or unsupported server software-are frequently associated with known, publicly documented exploits. The proper next step after identifying such vulnerabilities is to confirm exploitability safely, typically by researching available exploit code, validating version-specific weaknesses, and determining whether the vulnerability can be successfully leveraged under the defined scope of engagement. CEH highlights that exploitation attempts must be evidence-driven, not arbitrary, and focusing on high-risk vulnerabilities allows testers to demonstrate meaningful security impacts.

Brute-forcing (Option A) is unnecessary and high-noise. Ignoring or deprioritizing the high-risk finding (Options B and C) contradicts CEH risk-based assessment principles. Therefore, verifying exploitability of the high-risk vulnerability is the correct step.

NEW QUESTION: 178

What is the most plausible attack vector an APT group would use to compromise an IoT-based environmental control system?

A. Exploiting zero-day firmware vulnerabilities

B. Using stolen user credentials

C. Encrypted MitM attack

D. DDoS attack

Answer: A (LEAVE A REPLY)
According to CEH v13 Mobile, IoT, and OT Hacking, Advanced Persistent Threat (APT) groups prioritize stealth, persistence, and long-term control. In IoT environments, the most attractive and effective entry point is firmware-level zero-day vulnerabilities.
IoT devices often:
Run outdated or proprietary firmware
Lack regular patching mechanisms
Operate with high privileges
Have minimal monitoring
Exploiting a zero-day vulnerability in firmware allows attackers to gain deep, persistent access that survives reboots and avoids traditional security controls. This aligns directly with APT objectives.
Credential theft (Option B) is common but less reliable for IoT systems. Encrypted MitM (Option C) is complex and less persistent. DDoS (Option D) disrupts services but does not provide control.
CEH v13 explicitly identifies firmware exploitation as the primary APT vector in IoT and OT environments.
Therefore, Option A is correct.

NEW QUESTION: 179
A tester evaluates a login form that constructs SQL queries using unsanitized user input. By submitting 1 OR
'T'='T'; --, the tester gains unauthorized access to the application. What type of SQL injection has occurred?
A. Tautology-based SQL injection
B. Error-based SQL injection
C. Union-based SQL injection
D. Time-based blind SQL injection
Answer: (SHOW ANSWER)
This scenario represents a Tautology-Based SQL Injection, a fundamental SQL injection technique covered under the Web Application Hacking module in the CEH v13 curriculum. The defining characteristic of this attack is the injection of a condition that always evaluates to TRUE, thereby bypassing authentication or authorization controls.
In the given example, the injected input 1 OR 'T'='T'; -- manipulates the logical condition of the SQL query. A typical vulnerable login query may resemble:
SELECT * FROM users WHERE user_id = 1 AND password = 'input';
When the attacker submits the injected payload, the resulting SQL statement becomes:
SELECT * FROM users WHERE user_id = 1 OR 'T'='T'; --';
The expression 'T'='T' is a tautology, meaning it always evaluates to TRUE regardless of context. As a result, the database returns records without properly validating the user's credentials, granting unauthorized access.

According to EC-Council CEH v13, tautology-based SQL injection is classified as a Boolean-based injection technique where attackers exploit improper input validation to alter the logical flow of SQL queries. This attack does not depend on database error messages (as in Error-Based SQL Injection), does not extract data using UNION statements (Union-Based SQL Injection), and does not rely on response delays (Time-Based Blind SQL Injection).
CEH v13 emphasizes that such attacks are especially effective against login forms and authentication mechanisms when developers fail to implement input sanitization, parameterized queries, or prepared statements. This attack is one of the most common and exam-tested SQL injection types because it clearly demonstrates how flawed logic can compromise application security without advanced techniques.
Understanding tautology-based SQL injection is critical for ethical hackers, as it forms the foundation for identifying and mitigating more complex SQL injection variants.

NEW QUESTION: 180
A serverless application was compromised through an insecure third-party API used by a function. What is the most effective countermeasure?
A. Use a CASB for third-party services
B. Regularly update serverless functions
C. Deploy a cloud-native security platform
D. Enforce function-level least privilege permissions
Answer: (SHOW ANSWER)

NEW QUESTION: 181
Which action would most effectively increase the security of a virtual-hosted web server?
A. Implement LAMP architecture
B. Change IP addresses regularly
C. Regularly update and patch server software
D. Move document root to another disk
Answer: C (LEAVE A REPLY)
According to CEH v13 Web Application and Server Security, regular patching and updates are the most effective way to reduce server attack surfaces. Vulnerabilities in web servers, proxies, and supporting services are frequently exploited if patches are delayed.
While architectural choices and directory placement influence organization, they do not mitigate known vulnerabilities. Changing IP addresses does not prevent exploitation, and moving directories does not address underlying software flaws.
CEH v13 consistently emphasizes patch management as a primary defensive control. Therefore, Option C is correct.

NEW QUESTION: 182
At a fast-growing startup in Austin, Texas, an ethical hacker is asked to simulate how attackers might gather information to gain initial access. During the assessment, she poses as a recruiter on a professional networking site and convinces several employees to share details about the company's internal software and VPN setup.
Which type of threat best represents this adversary's method of information gathering?
A. System and Network Attacks
B. Social Engineering
C. Information Leakage
D. Corporate Espionage
Answer: B (LEAVE A REPLY)
The correct answer is B. Social Engineering because the attacker's primary method is manipulating people- not exploiting a technical vulnerability-to obtain information that can enable initial access. In CEH-aligned security concepts, social engineering is defined by the use of deception, impersonation, and psychological influence to persuade victims to reveal sensitive information, perform actions, or bypass normal security procedures. Here, the ethical hacker "poses as a recruiter" on a professional networking site, which is a classic impersonation / pretexting approach. The goal is to build credibility and trust so employees voluntarily disclose internal details that should not be shared externally.
The information gathered-"internal software and VPN setup"-is exactly the sort of intelligence attackers seek during reconnaissance and pre-attack planning. VPN details, remote access workflows, authentication methods, and internal tooling can be used to craft highly convincing phishing messages, identify weak points (such as outdated clients or exposed portals), or target specific employees and administrators. In a real intrusion, this social engineering-driven intelligence collection often precedes credential harvesting, password spraying, MFA fatigue attempts, or tailored malware delivery.
Why the other options are less correct: System and Network Attacks refer to direct technical exploitation such as scanning, sniffing, or attacking services and protocols; the scenario contains none of that. Information Leakage describes the condition where sensitive data is exposed (for example, public documents, misconfigured repositories, error messages), but the scenario focuses on active interpersonal manipulation to extract information. Corporate Espionage is a broader motive/category describing theft of trade secrets, often by competitors or nation-state actors; while social engineering can be used

in espionage, the question asks about the method of information gathering, which is clearly social engineering.
Therefore, the threat method demonstrated is social engineering (pretexting/impersonation via a recruiter persona).

NEW QUESTION: 183
At Horizon Legal Services in Boston, Massachusetts, ethical hacker Daniel Price is tasked with assessing the security of the firm's mobile case-tracking app. During testing, he finds that confidential case notes and client records are kept locally on the device without encryption. By browsing the file system with a standard explorer tool, he can open sensitive information without any authentication. Which OWASP Top 10 Mobile Risk is most clearly present in the app?
A. Insecure Communication
B. Improper Credential Usage
C. Insecure Data Storage
D. Inadequate Privacy Controls
Answer: C (LEAVE A REPLY)
The correct answer is C. Insecure Data Storage because the vulnerability described is the storage of sensitive information locally on the mobile device in a manner that is not encrypted and is accessible by simply browsing the file system. In mobile application security, this is a classic risk category: when an app stores confidential data (case notes, client records, tokens, documents, cached responses, databases, logs, or exported files) in clear text or in insecure locations, an attacker who gains device access-or uses backup extraction, file explorers, rooted/jailbroken access, or malware with storage permissions-may retrieve that data without needing to authenticate to the application.
The scenario makes the weakness unmistakable: Daniel can use a "standard explorer tool" to open sensitive records "without any authentication." This indicates the app is failing to apply appropriate protections such as encryption at rest, secure key handling, proper file permissions, and secure storage mechanisms. In secure mobile design, sensitive records should be encrypted using platform-supported protections (e.g., using OS keystores/keychains for keys, encrypting databases/files, and minimizing local retention). Additionally, apps should avoid storing highly sensitive regulated data unless essential, and should implement secure session controls and data lifecycle management (cache control, expiration, remote wipe support in enterprise settings).
Why the other options are not the best fit: Insecure communication concerns data exposure while transmitted over networks (e.g., lack of TLS, weak TLS, MITM susceptibility), whereas the issue here is purely local storage. Improper credential usage relates to mishandling passwords, tokens, or authentication secrets (hard- coded credentials, weak storage of credentials), but the prompt focuses on stored records themselves.

Inadequate privacy controls is broader and typically involves over-collection, improper disclosure, or weak user privacy settings, not direct clear-text storage exposure.
Therefore, the most clearly present OWASP Top 10 Mobile Risk is Insecure Data Storage.

NEW QUESTION: 184
A financial services firm is experiencing a sophisticated DoS attack on their DNS servers using DNS amplification and on their web servers using HTTP floods. Traditional firewall rules and IDS are failing to mitigate the attack effectively. To protect their infrastructure without impacting legitimate users, which advanced mitigation strategy should the firm implement?
A. Increase server capacity and implement simple rate limiting
B. Block all incoming traffic from suspicious IP ranges using access control lists
C. Deploy a Web Application Firewall (WAF) to filter HTTP traffic
D. Utilize a cloud-based DDoS protection service with traffic scrubbing capabilities
Answer: D (LEAVE A REPLY)
Cloud-based DDoS mitigation services provide upstream traffic scrubbing, detecting and filtering high- volume attacks such as DNS amplification and HTTP floods before the traffic reaches the victim's network.
These services use distributed infrastructures capable of handling multi-vector attacks that surpass the capacity of traditional on-premises firewalls and IDS. Traffic scrubbing centers distinguish legitimate traffic from malicious traffic, allowing normal operations to continue without service disruption.

NEW QUESTION: 185
SCADA anomalies suggest a side-channel attack. Which investigation best confirms this?
A. Review user interfaces
B. Measure hardware-level operational fluctuations
C. Identify weak crypto settings
D. Assess network latency
Answer: B (LEAVE A REPLY)
Side-channel attacks, as explained in CEH v13 OT and SCADA Security, extract sensitive information by observing physical characteristics of a system rather than exploiting software flaws directly. These characteristics may include power consumption, electromagnetic emissions, timing variations, or thermal output.
In SCADA environments, side-channel attacks are especially dangerous because they bypass traditional network defenses. The most reliable way to confirm such an attack is by analyzing hardware-level anomalies-such as unexpected power usage spikes or irregular signal emissions during normal device operations.
Option B directly aligns with CEH v13 guidance.
Options A, C, and D focus on software, cryptography, or network behavior, which are not primary indicators of side-channel exploitation.

Therefore, Option B is correct.

NEW QUESTION: 186
During network analysis, clients are receiving incorrect gateway and DNS settings due to a rogue DHCP server. What security feature should the administrator enable to prevent this in the future?
A. DHCP snooping on trusted interfaces
B. ARP inspection across VLANs
C. Port security on all trunk ports
D. Static DHCP reservations for clients
Answer: (SHOW ANSWER)
According to CEH v13, one of the most effective defenses against rogue DHCP servers is DHCP snooping, a Layer 2 security feature that classifies switch ports as either trusted or untrusted. DHCP responses are permitted only on trusted ports, typically those connected to legitimate DHCP servers. Any DHCP OFFER or ACK originating from an untrusted port is dropped automatically. In the scenario, the rogue DHCP server is sending unauthorized configuration settings because the switch is forwarding DHCP messages from all ports without restriction. CEH specifically warns that unmanaged or misconfigured switches allow rogue DHCP servers to assign malicious DNS, gateway, or IP configurations, enabling traffic redirection, interception, or man-in-the-middle attacks. ARP inspection (Option B) protects against ARP spoofing but not DHCP abuses.
Port security (Option C) prevents MAC flooding, not DHCP impersonation. Static reservations (Option D) do not scale and do not stop rogue DHCP servers. DHCP snooping directly mitigates this threat.

NEW QUESTION: 187
Amid the vibrant buzz of Miami's digital scene, ethical hacker Sofia Alvarez embarks on a mission to fortify the web server of Sunshine Media's streaming platform. Diving into her security assessment, Sofia sends a meticulously crafted GET / HTTP/1.0 request to the server, scrutinizing its response. The server obligingly returns headers exposing its software version and operating system, a revelation that could empower malicious actors to tailor their attacks. Committed to bolstering the platform's defenses, Sofia documents her findings to urge the security team to address this exposure.
What approach is Sofia using to expose the vulnerability in Sunshine Media's web server?
A. Information Gathering from Robots.txt File
B. Vulnerability Scanning
C. Directory Brute Forcing
D. Web Server Footprinting Banner Grabbing
Answer: D (LEAVE A REPLY)
The described action is classic web server footprinting through banner grabbing. In CEH reconnaissance methodology, banner grabbing is used to identify a target's service details

by eliciting and analyzing standard protocol responses. When Sofia sends a simple HTTP request such as GET / HTTP/1.0, the server often responds with HTTP headers that may include fields like Server and sometimes X-Powered-By, which can reveal the web server product and version, and occasionally information that hints at the underlying operating system or framework. This disclosure is valuable to attackers because it enables targeted exploitation: once the exact server and version are known, an attacker can correlate that information with known vulnerabilities, misconfigurations, and exploit code.
This is not information gathering from robots.txt, which is a web file used to suggest crawler behavior and sometimes reveals hidden paths but does not inherently expose server software versions. It is also not directory brute forcing, which involves systematically guessing directories and files to find hidden endpoints.
Vulnerability scanning is broader and typically involves automated checks to detect vulnerabilities; while banner information can be an input to scanning, the technique shown here is specifically identification through response headers.
CEH-aligned mitigation includes disabling or minimizing server signature information, removing unnecessary headers, keeping server software patched, and using secure configurations and reverse proxies to reduce information leakage during reconnaissance.

NEW QUESTION: 188
During a black-box internal penetration test, a security analyst identifies an SNMPv2-enabled Linux server using the default community string "public." The analyst wants to enumerate running processes. Which Nmap command retrieves this information?
A. nmap -sU -p 161 --script snmp-sysdescr
B. nmap -sU -p 161 --script snmp-win32-services
C. nmap -sU -p 161 --script snmp-processes
D. nmap -sU -p 161 --script snmp-interfaces
Answer: C (LEAVE A REPLY)
CEH v13 highlights that SNMPv1/v2 environments configured with default community strings such as
"public" or "private" present significant security risks because they allow unauthorized users to query system information. SNMP enumeration can reveal processes, interfaces, routing tables, users, device configurations, and more. The snmp-processes Nmap NSE script is specifically designed to enumerate running processes on an SNMP-enabled host. It queries the Host Resources MIB (HR-MIB), which stores operational information about system processes, CPU usage, and memory consumption. This information provides attackers with insights into what services may be exploitable or misconfigured. CEH stresses that SNMPv2 is particularly vulnerable due to lack of encryption and authentication hardening. By enumerating processes, penetration testers can identify potential privilege escalation paths, outdated services, or rogue applications that may aid lateral movement. Other scripts such as snmp-sysdescr or snmp-interfaces retrieve system description or interface data but do not enumerate processes.

NEW QUESTION: 189
During a routine security audit, administrators discover that cloud storage backups were illegally accessed and modified. Which countermeasure would most directly mitigate such incidents in the future?
A. Implementing resource auto-scaling
B. Regularly conducting SQL injection testing
C. Deploying biometric entry systems
D. Adopting the 3-2-1 backup model
Answer: D (LEAVE A REPLY)
The Certified Ethical Hacker (CEH) Cloud Computing and Data Protection module emphasizes the importance of resilient backup strategies to protect against data tampering, ransomware, and unauthorized modification.
The 3-2-1 backup model is a widely recommended best practice referenced in CEH materials. It requires maintaining:
* 3 copies of data
* Stored on 2 different media types
* With 1 copy stored offsite
This approach ensures that even if cloud backups are compromised or altered, clean and uncompromised versions remain available. CEH documentation highlights this model as a core defense against data integrity attacks in cloud environments.
Option D directly mitigates the risk of backup tampering.
Options A, B, and C address unrelated security concerns and do not protect backup integrity.

NEW QUESTION: 190
Which WPA2 vulnerability allows packet interception and replay?
A. Hole196 vulnerability
B. KRACK vulnerability
C. WPS PIN recovery
D. Weak RNG
Answer: (SHOW ANSWER)
The KRACK (Key Reinstallation Attack) vulnerability is a critical WPA2 flaw covered extensively in CEH v13 Wireless Network Hacking. KRACK exploits weaknesses in the four-way handshake process, allowing attackers to force reinstallation of encryption keys. This key reinstallation resets nonces and counters, enabling attackers to decrypt, replay, and forge packets, even on encrypted WPA2 networks. CEH v13 highlights that KRACK does not break encryption mathematically but exploits protocol logic flaws.
Hole196 affects GTK misuse, and WPS PIN attacks target authentication, not replay of encrypted traffic.
Weak RNG issues are unrelated to WPA2 replay.

Thus, Option B is correct.

NEW QUESTION: 191
Which algorithm best protects encrypted traffic patterns?
A. PSA
B. AES
C. DES
D. HMAC
Answer: (SHOW ANSWER)
AES is the industry-standard symmetric encryption algorithm endorsed by CEH v13. It provides strong confidentiality and resists traffic analysis when used with proper modes (e.g., CBC, GCM).
DES is obsolete, HMAC ensures integrity not encryption, PSA is not a standard encryption algorithm.
Thus, Option B is correct.

NEW QUESTION: 192
During a red team exercise at Orion Tech Systems in San Jose, ethical hacker Nadia creates a campaign of fraudulent messages targeting employees. She uses compromised social media accounts to distribute bulk invitations that contain links to a fake cloud collaboration site. Several employees click the links and are prompted to log in with their corporate credentials, which Nadia captures. Although the lure appears to be a professional networking opportunity, the tactic relies on unsolicited deceptive messages delivered at scale.
Which social engineering threat is Nadia simulating in this campaign?
A. Catfishing
B. Angler Phishing
C. Spam and Phishing
D. Involuntary Data Leakage
Answer: C (LEAVE A REPLY)
The correct answer is C. Spam and Phishing because the campaign is based on unsolicited deceptive messages sent in bulk with the intent to lure many recipients into clicking a link and submitting credentials on a fake site. In CEH-aligned social engineering concepts, phishing is a deception technique used to trick users into revealing sensitive information (such as corporate usernames and passwords) by impersonating a trusted entity or presenting a convincing pretext. When phishing is executed "at scale" using mass messaging-often through email, messaging platforms, or social media-it overlaps strongly with spam, which refers to unsolicited bulk communications distributed to large numbers of targets.
The scenario contains the classic phishing flow: a fraudulent invitation contains a link to a counterfeit "cloud collaboration" login page, and users are prompted to authenticate.

Credential capture ("which Nadia captures") confirms the objective is credential harvesting rather than mere awareness disruption. The detail that she used "compromised social media accounts" is consistent with modern phishing operations that abuse trusted accounts to increase credibility and bypass initial suspicion. This also helps attackers evade some basic filtering and encourages victims to trust the message because it appears to come from a legitimate profile.
Why the other options are less correct: Catfishing typically involves building a fake persona and maintaining a relationship over time (often one-to-one) to manipulate a victim; it is not mainly defined by bulk unsolicited messages. Angler phishing specifically refers to phishing conducted through social media channels, often by impersonating customer support or hijacking brand interactions. While the platform here is social media, the question's strongest discriminator is "unsolicited deceptive messages delivered at scale," which points to the combined threat category spam and phishing rather than the more specific "angler" support-impersonation pattern. Involuntary data leakage describes accidental exposure of information, not active deception.
Therefore, Nadia's campaign most clearly simulates spam and phishing.

NEW QUESTION: 193
A payload causes a significant delay in response without visible output when testing an Oracle-backed application. What SQL injection technique is being used?
A. Time-based SQL injection using WAITFOR DELAY
B. Heavy query-based SQL injection
C. Union-based SQL injection
D. Out-of-band SQL injection
Answer: A (LEAVE A REPLY)
This scenario precisely matches Time-Based Blind SQL Injection, a technique detailed in CEH v13 Web Application Hacking. When applications suppress error messages and sanitize outputs, attackers rely on response timing to infer whether injected SQL statements are executed.
In time-based SQL injection, the attacker injects database-specific delay functions (such as WAITFOR DELAY, DBMS_LOCK.SLEEP, or SLEEP()). If the injected condition is true, the database pauses execution, causing a noticeable delay.
The key indicators described-no visible output but increased response time-are classic signs of time- based SQL injection. CEH v13 explains that this method is particularly useful when:
* Errors are hidden
* UNION queries fail
* Output is not reflected
Union-based and out-of-band SQL injections require data exfiltration channels or visible outputs, which are absent here. "Heavy query-based" is not a formal CEH classification.
Thus, Option A is the correct answer.

NEW QUESTION: 194
In Raleigh, North Carolina, ethical hacker Ethan Brooks is conducting a penetration test for Triangle FinTech, a rising financial startup. During his assessment, Ethan aims to bypass the company's network security to access a restricted internal server. He crafts network packets to disguise his traffic as legitimate, forcing some TCP header information into subsequent packets to evade the firewall's checks. His aim is to demonstrate how an attacker could slip past the security perimeter undetected, alerting the IT team to potential weaknesses.
Which technique is Ethan employing to bypass Triangle FinTech's firewall during his penetration test?
A. Source Routing
B. Tiny Fragments
C. HTTP Tunneling
D. IP Address Spoofing
Answer: (SHOW ANSWER)
Tiny Fragments is the technique described because it relies on IP fragmentation to evade firewall or packet- filter inspection by splitting critical header and payload information across multiple fragments. In CEH- aligned network evasion concepts, some security devices make allow or deny decisions by inspecting specific fields and patterns in the first fragment of a packet or by performing limited reassembly. If the attacker deliberately crafts fragments that are unusually small, the first fragment may not contain enough of the TCP header or higher-layer data for the firewall to properly evaluate the packet against its rules and signatures. The remaining TCP header bytes or meaningful payload patterns can be pushed into subsequent fragments, which may pass through because the device cannot correlate them correctly or does not fully reassemble traffic before inspection.
The question's key clue is that Ethan is "forcing some TCP header information into subsequent packets" to bypass checks. That phrasing is a direct match to fragmentation-based evasion rather than identity deception or tunneling. IP address spoofing changes the apparent source IP, but it does not specifically move TCP header details into later fragments. Source routing is an old technique to influence packet pathing using IP options and is typically blocked in modern environments; it also does not describe splitting TCP header content. HTTP tunneling encapsulates non-HTTP traffic inside HTTP to pass through proxies or firewalls, which is a different mechanism than fragmentation.
Therefore, the correct firewall bypass technique in this scenario is Tiny Fragments.

NEW QUESTION: 195
During a compliance review at a law firm in Chicago, an ethical hacker tests the firm's secure email gateway.
She observes that sensitive legal documents are being transmitted in clear text over the Internet, allowing anyone intercepting the traffic to read the contents. The firm is concerned

about unauthorized individuals being able to view these communications. Which principle of information security is being violated?

A. Confidentiality

B. Integrity

C. Non-Repudiation

D. Availability

Answer: (SHOW ANSWER)

The correct answer is A. Confidentiality because the scenario describes sensitive information being transmitted in clear text, meaning the contents can be read by any unauthorized party who is able to intercept the traffic. In information security, confidentiality is the principle that ensures information is accessible only to authorized individuals, entities, or processes. When communications are sent without adequate protection- such as encryption-attackers performing network interception (for example, through man-in-the-middle positioning, packet sniffing on compromised routers, malicious Wi-Fi, or upstream monitoring) can directly view the document contents. That is a direct failure of confidentiality controls.

The prompt's key phrase is that "anyone intercepting the traffic can read the contents." This is not describing altered messages or forged emails; it is describing unauthorized disclosure. Confidentiality is typically protected using mechanisms such as encryption in transit (e.g., TLS for SMTP submission and server-to- server transport where possible, S/MIME, PGP), secure key management, and policy enforcement at email gateways. In legal environments, confidentiality is particularly critical because client communications and legal documents often contain privileged or regulated information. Clear-text transmission exposes the firm to compliance violations, reputational harm, and potential legal consequences.

Why the other options are not correct: Integrity concerns whether the message or document is altered in transit (tampering, modification, insertion). The scenario does not mention changes-only unauthorized reading. Non-repudiation ensures parties cannot deny sending or receiving a message (often supported by digital signatures and logging). The issue here is not proof-of-origin but exposure. Availability relates to whether systems and data remain accessible when needed (uptime, resilience, DoS). Nothing indicates service disruption.

Therefore, transmitting sensitive legal documents in clear text violates the fundamental security principle of confidentiality.

NEW QUESTION: 196

Abnormal DNS resolution behavior is detected on an internal network. Users are redirected to altered login pages. DNS replies come from an unauthorized internal IP and are faster than legitimate responses. ARP spoofing alerts are also detected. What sniffing-based attack is most likely occurring?

A. Internet DNS spoofing

B. Intranet DNS poisoning via local spoofed responses
C. Proxy-based DNS redirection
D. Upstream DNS cache poisoning
Answer: B (LEAVE A REPLY)
This is a textbook case of Intranet DNS Poisoning, often combined with ARP spoofing, as described in CEH v13 Network Sniffing and MITM Attacks. The attacker positions themselves inside the local network, intercepts DNS requests, and responds faster than the legitimate DNS server.
ARP spoofing enables the attacker to perform a Man-in-the-Middle attack, allowing sniffing and modification of DNS traffic. CEH v13 notes that faster rogue responses are a strong indicator of local DNS poisoning.

NEW QUESTION: 197
A penetration tester is tasked with assessing the security of an Android mobile application that stores sensitive user data. The tester finds that the application does not use proper encryption to secure data at rest. What is the most effective way to exploit this vulnerability?
A. Access the local storage to retrieve sensitive data directly from the device
B. Use SQL injection to retrieve sensitive data from the backend server
C. Execute a Cross-Site Scripting (XSS) attack to steal session cookies
D. Perform a brute-force attack on the application's login credentials
Answer: (SHOW ANSWER)
CEH training emphasizes that mobile applications frequently mishandle local storage, leaving sensitive data such as tokens, passwords, API keys, or personal information unencrypted within SQLite databases, shared preferences, or flat-file storage. When encryption is absent or improperly implemented, attackers can directly access this data through filesystem extraction, Android Debug Bridge (ADB) access, physical device access, or rooted environments. CEH identifies "Insecure Data Storage" as one of the most critical mobile vulnerabilities because it bypasses server-side defenses entirely. Since the vulnerability specifically concerns data at rest, the most direct and effective exploitation method is to retrieve the locally stored unencrypted data. SQL injection (Option B) evaluates backend security, not device storage. XSS (Option C) is a web attack and

unrelated to local encryption. Brute-forcing credentials (Option D) is unnecessary when sensitive information is already stored insecurely. Therefore, accessing local storage is the correct exploitation method.

NEW QUESTION: 198
In the crisp mountain air of Denver, Colorado, ethical hacker Lila Chen investigates the security framework of MediVault, a U.S.-based healthcare platform used by regional clinics to manage patient data. During her review, Lila discovers that sensitive records are weakly protected, allowing attackers to intercept and manipulate the information in transit. She warns that such weaknesses could be exploited to commit credit- card fraud, identity theft, or similar crimes. Further analysis reveals that MediVault is vulnerable to well- documented flaws such as cookie snooping and downgrade attacks.
Which issue is MOST clearly indicated?
A. Broken Access Control
B. Cryptographic Failures
C. Security Misconfiguration
D. Identification and Authentication Failures
Answer: B (LEAVE A REPLY)
The best answer is B. Cryptographic Failures because the scenario centers on weak protection of sensitive data in transit, enabling an attacker to intercept and manipulate the information. In CEH-aligned web and application security concepts (and consistent with modern web risk categories), cryptographic failures occur when an application does not properly use cryptography or secure transport protections to ensure confidentiality and integrity of sensitive data. If transport encryption is missing, weak, or incorrectly configured, attackers can perform man-in-the-middle style interception, tamper with traffic, steal session material, and exfiltrate regulated data-leading to outcomes like identity theft and payment card fraud, exactly as described.
The references to cookie snooping and downgrade attacks further reinforce this. Cookie snooping is commonly associated with session cookies being exposed due to insecure transport (for example, lack of HTTPS, mixed content, or cookies missing secure attributes), allowing an attacker on the network path to capture session identifiers and hijack accounts. Downgrade attacks occur when an attacker forces a connection to use weaker security settings (such as older TLS versions or insecure cipher suites) or coerces a fallback from HTTPS to HTTP when protections like HSTS are absent or misapplied. Both issues are tightly linked to improper cryptographic configuration and transport-layer security weaknesses.
Why the other options are not the best match: Broken Access Control concerns authorization-what users are allowed to access-not interception/manipulation of traffic. Identification and Authentication Failures focus on login/session identity mechanisms (passwords, MFA, session handling) but the key failure here is the weakness of cryptographic protection for data in transit. Security Misconfiguration can be a contributing

cause (e.g., misconfigured TLS), but the question emphasizes the resulting weakness category-insufficient cryptographic/transport protections-making Cryptographic Failures the most precise answer.
Therefore, MediVault's exposure to interception, manipulation, cookie snooping, and downgrade attacks most clearly indicates Cryptographic Failures.

NEW QUESTION: 199
During a red team engagement at Apex Biotech in Dallas, ethical hacker Rachel calls the company's HR desk pretending to be Mark Stevens, a senior finance manager. She pressures the HR staffer by citing his
"upcoming presentation for the CFO" and insists he urgently needs a copy of the updated employee benefits spreadsheet. The staffer feels compelled to help due to Rachel's convincing manner and authoritative tone.
Which social engineering technique is Rachel demonstrating in this exercise?
A. Quid Pro Quo
B. Impersonation
C. Vishing
D. Reverse Social Engineering
Answer: (SHOW ANSWER)
The correct answer is B. Impersonation because Rachel's primary technique is pretending to be a specific, legitimate employee ("Mark Stevens, a senior finance manager") to induce the HR staffer to disclose or transmit sensitive information. In CEH-aligned social engineering concepts, impersonation is the act of assuming another person's identity or role-often someone with authority or a believable business need-to gain trust and persuade the target to perform an action they otherwise should not (such as sharing confidential documents, resetting credentials, or bypassing verification steps).
The scenario includes multiple social engineering influence factors commonly emphasized in CEH: authority (claiming to be a senior finance manager and referencing the CFO), urgency ("upcoming presentation" and
"urgently needs"), and pressure to reduce the likelihood the staffer follows standard validation procedures.
These elements strengthen the impersonation by making the request feel both legitimate and time-sensitive, increasing compliance. The target's reaction-feeling compelled due to Rachel's authoritative tone-matches the expected psychological effect of impersonation attacks.
Why the other options are less correct: Vishing (voice phishing) is a delivery channel-social engineering conducted via phone calls. While this interaction occurs over the phone, the question asks for the technique being demonstrated. The defining technique here is the identity deception (impersonation) rather than merely the medium. Quid pro quo involves offering something in exchange (e.g., "I'll fix your issue if you give me your password"), which is not present. Reverse social engineering involves the attacker creating a problem

and positioning themselves as the helper so the victim contacts them; that is not described because Rachel initiates the call and directly requests the document.
Therefore, the most accurate classification of Rachel's method is Impersonation.

NEW QUESTION: 200
A penetration tester evaluates a company's susceptibility to advanced social engineering attacks targeting its executive team. Using detailed knowledge of recent financial audits and ongoing projects, the tester crafts a highly credible pretext to deceive executives into revealing their network credentials. What is the most effective social engineering technique the tester should employ to obtain the necessary credentials without raising suspicion?
A. Send a mass phishing email with a link to a fake financial report
B. Create a convincing fake email from the CFO asking for immediate credential verification
C. Conduct a phone call posing as an external auditor requesting access to financial systems
D. Develop a spear-phishing email that references specific financial audit details and requests login confirmation
Answer: D (LEAVE A REPLY)
Spear-phishing is a targeted form of phishing that uses personalized and context-rich information to increase credibility. CEH emphasizes that referencing specific internal projects, financial data, or organizational events significantly raises the success rate when attacking high-value targets such as executives. This tailored approach avoids suspicion and exploits trust more effectively than broad or generic phishing attempts.

NEW QUESTION: 201
A penetration tester suspects that a web application's login form is vulnerable to SQL injection due to improper sanitization of user input. What is the most appropriate approach to test for SQL injection in the login form?
A. Inject JavaScript into the input fields to test for Cross-Site Scripting (XSS)
B. Enter ' OR '1'='1 in the username and password fields to bypass authentication
C. Perform a directory traversal attack to access sensitive files
D. Use a brute-force attack on the login page to guess valid credentials
Answer: (SHOW ANSWER)
CEH v13 explains that SQL injection typically occurs when user inputs are concatenated into SQL queries without proper validation or parameterization. The login form is one of the most common injection targets, and testers use specific test payloads designed to manipulate the authentication query. A classic test string such as ' OR '1'='1 exploits conditional logic to force the SQL statement to evaluate as true, effectively bypassing authentication if the application is vulnerable. CEH notes that this technique is a standard initial test because it is low-risk, easily detectable if vulnerable, and directly confirms improper sanitization.

JavaScript injection (Option A) tests for XSS, not SQLi. Directory traversal (Option C) targets file path vulnerabilities rather than SQL queries. Brute-force attacks (Option D) rely on guessing credentials and do not test input sanitization. Therefore, using a logical SQL injection payload is the most appropriate and CEH- aligned method.

NEW QUESTION: 202
A penetration tester is assessing a company's executive team for vulnerability to sophisticated social engineering attacks by impersonating a trusted vendor and leveraging internal communications. What is the most effective social engineering technique to obtain sensitive executive credentials without being detected?
A. Develop a fake social media profile to connect with executives and request private information
B. Conduct a phone call posing as the CEO to request immediate password changes
C. Create a targeted spear-phishing email that references recent internal projects and requests credential verification
D. Send a mass phishing email with a malicious link disguised as a company-wide update
Answer: C (LEAVE A REPLY)
CEH categorizes spear phishing as a highly targeted, research-driven social engineering technique that tailors the message to the victim's role, responsibilities, and current organizational activities. When attackers reference specific internal projects, personnel names, vendor relationships, or operational details, the message appears authentic and bypasses normal suspicion. Executives are especially vulnerable because they routinely receive sensitive operational updates and work closely with vendors and partners, making them prime targets for tailored deception. CEH stresses that spear phishing is significantly more effective than generic phishing because personalization increases trust. Social media-based attempts and mass phishing lack specificity and raise suspicion. Impersonating the CEO over the phone is riskier and more detectable due to real-time human interaction. A targeted spear-phishing email referencing internal projects best aligns with CEH-described advanced social engineering strategy.

NEW QUESTION: 203
A penetration tester is assessing a web application that uses dynamic SQL queries for searching users in the database. The tester suspects the search input field is vulnerable to SQL injection. What is the best approach to confirm this vulnerability?
A. Input DROP TABLE users; -- into the search field to test if the database query can be altered
B. Inject JavaScript into the search field to test for Cross-Site Scripting (XSS)
C. Use a directory traversal attack to access server configuration files
D. Perform a brute-force attack on the user login page to guess weak passwords
Answer: A (LEAVE A REPLY)

CEH explains that SQL injection testing should begin with controlled, intentional manipulation of SQL syntax to determine whether user input is improperly concatenated into backend queries. While destructive queries like DROP TABLE are not recommended in real-world ethical hacking engagements, CEH uses this example as a conceptual demonstration of how SQLi can influence database commands. In practice, a penetration tester would more safely use benign tautologies such as ' OR '1'='1 to test whether unauthorized data is returned. However, within CEH's theoretical framing, injecting a clearly malicious SQL command demonstrates whether the input is executed at the database level. This validates improper sanitization, the use of dynamic SQL queries, and missing parameterized input handling. CEH stresses that SQLi is among the most critical vulnerabilities because it allows attackers to bypass authentication, exfiltrate data, or manipulate the database structure. XSS, brute-forcing, and directory traversal do not test SQL query manipulation and therefore do not confirm SQL injection.

NEW QUESTION: 204
In an enterprise environment, the network security team detects unusual behavior suggesting advanced sniffing techniques exploiting legacy protocols to intercept sensitive communications. Which of the following sniffing-related techniques presents the greatest challenge to detect and neutralize, potentially compromising confidential enterprise data?
A. Steganographic payload embedding within SMTP email headers
B. Encrypted data extraction via HTTP header field overflows
C. Covert data interception via X2S packet fragmentation
D. Covert channel establishment through Modbus protocol manipulation
Answer: D (LEAVE A REPLY)
According to the CEH Sniffing and Network Protocol Attacks module, covert channels represent one of the most sophisticated and difficult-to-detect data interception techniques. These channels hide malicious communication within legitimate protocol behavior, making them extremely challenging for traditional IDS
/IPS and packet inspection tools to identify.
Industrial and legacy protocols such as Modbus, widely used in OT and legacy enterprise environments, lack encryption and authentication by design. CEH documentation highlights that attackers can manipulate unused or poorly validated Modbus fields to covertly transmit or intercept data while appearing as normal control traffic.
Option D is correct because covert channels over trusted legacy protocols blend seamlessly with legitimate traffic and bypass many security controls.
Option A is not a sniffing technique but a data-hiding method.
Option B describes exploitation, not sniffing.
Option C is a theoretical evasion method but is more detectable through reassembly.
CEH emphasizes covert channels as one of the most formidable sniffing challenges.

NEW QUESTION: 205

During a red team exercise at Horizon Financial Services in Chicago, ethical hacker Clara crafts an email designed to trick the company's CEO. The message, disguised as an urgent memo from the legal department, warns of a pending lawsuit and includes a link to a fake internal portal requesting the executive's credentials.
Unlike generic phishing, this attack is tailored specifically toward a high-ranking individual with decision- making authority.
A. Whaling
B. Spear Phishing
C. Clone Phishing
D. Consent Phishing
Answer: A (LEAVE A REPLY)
Whaling is the correct answer because the scenario describes a highly targeted phishing attempt aimed at a
"big fish"-a senior executive (the CEO). In CEH terminology, whaling is a specialized form of phishing that focuses on high-profile, high-authority individuals (e.g., CEOs, CFOs, directors) to maximize impact. These targets often have access to sensitive data, financial approvals, privileged systems, and strategic communications, making their credentials significantly more valuable than those of typical employees.
The attacker (Clara) uses classic social engineering drivers emphasized in CEH training: authority (impersonating the legal department), urgency/fear (a "pending lawsuit"), and trust in internal processes (a link to a supposed internal portal). This combination is designed to short-circuit normal verification behavior and prompt quick compliance. The inclusion of a credential-harvesting link aligns with common phishing goals: capturing usernames/passwords, enabling account takeover, and potentially facilitating broader compromise (e.g., email access for business email compromise, lateral movement, or privileged escalation).
Why the other options are less accurate: Spear phishing is also targeted, but it is a broader category aimed at specific individuals or groups at any level. The defining clue here is the executive-level target, which elevates it to whaling. Clone phishing involves copying a legitimate email previously received and swapping a malicious link or attachment-this detail is not present. Consent phishing typically abuses legitimate OAuth
/app consent flows rather than a fake portal requesting credentials.

NEW QUESTION: 206
A WPA2-PSK wireless network is tested. Which method would allow identification of a key vulnerability?
A. De-authentication attack to capture the four-way handshake
B. MITM to steal the PSK directly
C. Jamming to force PSK disclosure
D. Rogue AP revealing PSK
Answer: A (LEAVE A REPLY)

CEH v13 states that the only viable way to attack WPA2-PSK is by capturing the four-way handshake. De- authentication forces clients to reconnect, allowing the handshake to be captured and later cracked offline.
MITM, jamming, and rogue AP attacks do not directly expose the PSK.

NEW QUESTION: 207
Which countermeasure best mitigates brute-force attacks on Bluetooth SSP?
A. Use BLE exclusively
B. Increase Diffie-Hellman key length
C. Apply rate-limiting
D. Device whitelisting
Answer: C (LEAVE A REPLY)
In CEH v13 Wireless Hacking, brute-force attacks against Secure Simple Pairing (SSP) exploit repeated attempts to guess cryptographic values. The most effective defense is rate limiting, which restricts how many pairing attempts can be made in a given timeframe. Increasing key length does not stop brute-force attempts if unlimited tries are allowed. BLE still uses pairing mechanisms and is not immune. Whitelisting controls access but does not prevent cryptographic attacks during pairing.
CEH v13 explicitly recommends rate limiting and pairing attempt thresholds as primary mitigations.
Therefore, Option C is correct.

NEW QUESTION: 208
An attacker gained escalated privileges on a critical server. What should be done FIRST to contain the threat with minimal disruption?
A. Engage a forensic team immediately
B. Power down the server and isolate it
C. Monitor, analyze, and then isolate the server
D. Conduct a vulnerability scan on all servers
Answer: (SHOW ANSWER)
CEH v13 follows the Incident Response Lifecycle, which prioritizes identification and analysis before containment, unless there is immediate risk of catastrophic damage. In this scenario, the attacker has escalated privileges, but the organization still needs to understand what actions are being taken, what systems are affected, and whether lateral movement is occurring.
Option C aligns with CEH v13 best practices. Real-time monitoring and documentation allow analysts to:
* Identify attacker techniques and tools
* Preserve volatile evidence
* Understand scope and impact
* Implement targeted containment

Immediately powering down the server (Option B) may destroy volatile forensic evidence and disrupt services unnecessarily. Engaging forensic teams (Option A) is important but premature without initial analysis.
Running vulnerability scans (Option D) does not address the active threat.
CEH v13 stresses that informed containment is more effective than reactive shutdowns.
Therefore, Option C is correct.

NEW QUESTION: 209
Fleet vehicles with smart locking systems were compromised after attackers captured unique signals from key fobs. What should the security team prioritize to confirm and prevent this attack?
A. Secure firmware updates
B. Increase physical surveillance
C. Deploy anti-malware on smartphones
D. Monitor wireless signals for jamming or interference
Answer: D (LEAVE A REPLY)
This scenario aligns with a Replay Attack against RF-based smart key systems, covered in CEH v13 IoT and OT Hacking. Attackers capture radio-frequency signals transmitted by key fobs and replay them to unlock vehicles.
CEH v13 emphasizes that detecting and preventing such attacks requires monitoring wireless RF signals for anomalies such as signal replay, interference, or jamming patterns.
RF analysis helps confirm unauthorized signal capture and retransmission.
Firmware updates may mitigate future vulnerabilities, but confirmation requires RF monitoring. Physical surveillance and smartphone malware controls are unrelated to RF replay attacks. Therefore, option D is correct.

NEW QUESTION: 210
Under the neon glow of Seattle ' s skyline, ethical hacker Elena Vasquez slips into her role as a cybersecurity consultant for Cascade Financial ' s online banking platform. Tasked with probing the web server ' s defenses, Elena simulates a series of rapid login attempts to the admin portal. She notes that the system allows unlimited tries without locking the account, exposing a gap that could invite relentless password-guessing attacks.
Determined to safeguard the bank ' s assets, Elena drafts a recommendation to fortify the server ' s authentication process against such threats.
What countermeasure should Elena recommend to strengthen Cascade Financial ' s web server against the vulnerability identified?
A. Implement 2FA or MFA
B. Force users to periodically change passwords
C. Use CAPTCHA challenges on login and registration pages
D. Use strong, one-way hashing algorithms such as bcrypt, scrypt, or Argon2
Answer: C (LEAVE A REPLY)

The weakness described is a classic online password-guessing condition: the application permits unlimited authentication attempts without any throttling, lockout, or challenge mechanism. In CEH guidance, this exposure enables brute-force attacks and automated credential stuffing, where attackers rapidly test many passwords or reused credential pairs until successful. A practical and commonly recommended control at the web application layer is adding CAPTCHA challenges to the login workflow, especially after a small number of failed attempts or when anomalous behavior is detected. CAPTCHA increases the cost of automation by forcing human interaction, directly disrupting high-speed scripted guessing against the admin portal.
While implementing MFA is an excellent additional safeguard and is strongly encouraged for privileged access, the question asks for the best countermeasure to address the specific issue of unlimited rapid attempts.
CAPTCHA is a direct mitigation for automated login abuse, and CEH commonly pairs it with rate limiting, progressive delays, and account lockout policies. Periodic password changes do not prevent an attacker from guessing a password today, and CEH materials note that forced rotation can even reduce security if it drives predictable password patterns. Strong password hashing such as bcrypt, scrypt, or Argon2 is critical for protecting stored passwords if a database is compromised, but it does not stop online guessing against the login form itself. Therefore, the most fitting countermeasure for the identified vulnerability is using CAPTCHA challenges on login and registration pages, ideally combined with throttling and lockout for stronger defense in depth

NEW QUESTION: 211
During a code review at a defense technology contractor in Virginia, penetration tester Lucas identifies that a newly deployed payroll application encrypts sensitive employee data using a weak custom algorithm. In addition, its session validation logic allows certain requests to bypass access controls altogether. These oversights are traced back to flawed system logic and poor encryption design decisions made during the development phase. Which vulnerability category BEST describes the issue Lucas discovered?
A. Design Flaws
B. Application Flaws
C. Misconfigurations/Weak Configurations
D. Poor Patch Management
Answer: (SHOW ANSWER)
The correct answer is A. Design Flaws because the weaknesses originate from fundamental development-time decisions in how the application was architected-specifically (1) selecting or creating a weak custom encryption algorithm and (2) implementing session validation in a way that allows requests to bypass access controls. In CEH-aligned vulnerability classification, design flaws are problems embedded in the application's design and logic, not merely bugs from implementation mistakes,

misconfiguration of a server setting, or missing vendor patches. They are often systemic: even if the code is "working as intended," the intent itself is insecure.
The prompt explicitly states the issues are "traced back to flawed system logic and poor encryption design decisions made during the development phase." That description maps directly to design flaws: using
"homegrown crypto" instead of vetted cryptographic primitives and protocols is a classic design error because it typically lacks proper peer review, threat modeling, and proven resistance to cryptanalysis. Likewise, session validation that permits bypassing access controls indicates the application's authorization/session model was designed incorrectly (for example, trusting client-side state, failing to enforce server-side checks consistently, or allowing unauthenticated endpoints to access privileged operations).
Why the other options are less accurate: Application flaws is a broad label that can include coding bugs, but the question is asking for the best category given that the root cause is architectural decisions rather than a narrow coding mistake. Misconfigurations/weak configurations usually refer to insecure settings in deployment (default credentials, permissive headers, weak TLS configuration), not a custom crypto algorithm and flawed session logic baked into the app. Poor patch management concerns failing to update known vulnerable components; here, the weakness is custom logic, not an unpatched third-party vulnerability.
Therefore, the most accurate category for these development-phase encryption and session/authorization weaknesses is Design Flaws.

NEW QUESTION: 212
During a post-exploitation phase in a network compromise simulation, ethical hacker Devon Hughes gains a Meterpreter session on a manager's Windows 10 workstation. To maintain stealth, he avoids actions that generate obvious signs of tampering such as privilege escalation or file system changes. Instead, he wants to monitor the user's live activity over time without their knowledge, focusing specifically on input patterns and active sessions.
Which Meterpreter command should he use to achieve this objective with minimal visibility?
A. keyscan_start

B. AThis scenario is testing recognition of a post-exploitation objective focused on covertly observing user activity, specifically "input patterns," which directly aligns with keystroke capture or keylogging behavior. In CEH coverage of System Hacking and Post-Exploitation, attackers who already have interactive access commonly shift to information-gathering actions that reveal credentials and sensitive business data without performing noisy changes such as privilege escalation or writing artifacts to disk.
Keystroke monitoring is a classic example because it can capture usernames, passwords, internal system commands, chat messages, and other sensitive inputs as the user works, often with lower visibility than actions that alter system configuration.The remaining options map to different post- exploitation goals and are less consistent with the prompt's emphasis on stealth and "no obvious signs of tampering." Dumping password hashes (hashdump) targets stored credential material and is typically associated with higher privilege requirements and higher detection potential due to access to sensitive security databases. Persistence is about maintaining long-term access across reboots and usually introduces artifacts such as registry changes, scheduled tasks, or services-precisely the type of detectable modification the prompt says Devon wants to avoid. Privilege escalation (getsystem) explicitly attempts to elevate rights, increasing operational risk and logging footprint.From a defensive perspective, CEH emphasizes mitigating this class of activity with strong endpoint monitoring and EDR, least-privilege controls, rapid patching, application allowlisting, and credential protections such as MFA and hardened authentication storage. Teams should alert on suspicious input-capture behaviors, abnormal process activity, and unusual remote sessions to detect post-exploitation collection attempts early.
C. hashdump
D. persistence
E. getsystem
Answer: A,B,C,D,E (LEAVE A REPLY)

NEW QUESTION: 213
You are Michael Rivera, a cybersecurity consultant at FortiSec Solutions, hired to strengthen the wireless network of DesertTech Innovations, a startup in Phoenix, Arizona. After a recent penetration test revealed vulnerabilities, the IT manager, Lisa Nguyen, asks you to recommend a defense mechanism to prevent unauthorized devices from connecting to the corporate Wi-Fi. You suggest a method that requires each connecting device to authenticate through a centralized server using a unique username and password. Based on the described approach, which wireless security countermeasure should DesertTech implement?
A. Use 802.1X Authentication
B. Disable TKIP
C. MAC Address Filtering
D. Upgrade to WPA3

Answer: A (LEAVE A REPLY)
The requirement that each device authenticate through a centralized server using unique usernames and passwords aligns directly with 802.1X authentication, which CEH materials describe as port-based Network Access Control used in enterprise wired and wireless environments. In Wi-Fi, 802.1X is typically implemented as WPA2-Enterprise or WPA3-Enterprise and relies on EAP methods with a backend AAA server, most commonly RADIUS. The access point acts as the authenticator, forwarding the client's authentication exchange to the RADIUS server, which validates the user or device identity and returns an accept or reject decision along with session keys and policy attributes. This provides strong control and auditing because access can be tied to individual identities, supports account disablement, and can enforce different access levels.
The other options do not match the "centralized server with unique credentials" description. Disabling TKIP improves security by removing an outdated encryption protocol, but it does not provide per-user authentication. MAC address filtering is weak because MAC addresses are easily discovered and spoofed, and it does not use centralized identity validation. Upgrading to WPA3 improves cryptographic strength, and WPA3-Enterprise can work with 802.1X, but WPA3 alone does not guarantee centralized username and password authentication unless the enterprise mode with 802.1X is specifically deployed. Therefore, the correct countermeasure that fits the described design is to use 802.1X authentication with a centralized authentication server, enabling strong access control, accountability, and improved resistance to unauthorized device connections.

NEW QUESTION: 214
A penetration tester is tasked with identifying vulnerabilities on a web server running outdated software. The server hosts several web applications and is protected by a basic firewall. Which technique should the tester use to exploit potential server vulnerabilities?
A. Conduct a SQL injection attack on the web application's login form
B. Perform a brute-force login attack on the admin panel
C. Execute a buffer overflow attack targeting the web server software
D. Use directory traversal to access sensitive configuration files
Answer: (SHOW ANSWER)
Outdated server software often contains memory corruption flaws. CEH notes that buffer overflow exploits are a primary method for compromising vulnerable server binaries, allowing remote code execution. This approach targets the underlying service rather than application-layer input validation issues.

NEW QUESTION: 215
A cybersecurity analyst monitors competitors' web content for changes indicating strategic shifts. Which missing component is most crucial for effective passive surveillance?
A. Participating in competitors' blogs and forums
B. Setting up Google Alerts for competitor names and keywords

C. Using a VPN to hide the analyst's IP address
D. Hiring a third party to hack competitor databases
Answer: B (LEAVE A REPLY)
The CEH Footprinting and Reconnaissance module highlights Google Alerts as a key passive reconnaissance tool for monitoring changes in web content, news, and online mentions.
Option B is correct.
Option A is active engagement.
Option C aids anonymity but not monitoring.
Option D is illegal and unethical.
CEH strongly promotes automated alerting for competitive intelligence.

NEW QUESTION: 216
Noah, a security analyst at a Seattle-based healthcare provider, is responding to a real-time data breach where attackers accessed patient records stored on a compromised server. During incident response, he must quickly secure sensitive files located on the system's primary storage to prevent further exfiltration. The data resides in a mounted partition that needs full-volume encryption, but standard file encryption isn't sufficient. Noah selects a solution that supports encrypted containers, strong key lengths like 256-bit AES, and can conceal secure volumes within standard ones to reduce detection. His goal is to ensure confidentiality while forensic operations continue without disrupting system functionality.
Which disk encryption tool should Noah deploy to meet these objectives?
A. BitLocker Drive Encryption
B. FileVault
C. Rohos Disk Encryption
D. VeraCrypt
Answer: (SHOW ANSWER)
The best match is VeraCrypt because the scenario explicitly requires three capabilities commonly associated with it in CEH cryptography and data protection coverage: encrypted containers, strong modern ciphers such as AES with 256-bit keys, and the ability to hide a protected volume inside another volume to reduce detectability. VeraCrypt is a successor to TrueCrypt and is widely referenced in ethical hacking curricula as a practical disk encryption utility that can create encrypted file containers and encrypt entire partitions or drives.
It supports multiple algorithms and combinations, including AES-256, and can mount encrypted containers as virtual drives so applications can access data normally while it remains encrypted at rest.
The key distinguishing requirement is concealment of secure storage using hidden volumes. VeraCrypt supports plausible deniability by allowing a hidden volume to exist inside an outer encrypted volume. If compelled to reveal a password, a user can disclose

the outer volume password while the hidden volume remains undetectable without its separate credentials. The prompt's phrase "conceal secure volumes within standard ones" maps directly to this VeraCrypt feature and is not a standard capability of BitLocker or FileVault.
BitLocker and FileVault provide strong full-disk encryption, but they do not provide hidden volumes for plausible deniability. Rohos can create encrypted containers, but hidden-volume style plausible deniability is most strongly and commonly associated with VeraCrypt in CEH-oriented discussions. Therefore, VeraCrypt is the most appropriate tool for Noah's stated objectives.

NEW QUESTION: 217
A penetration tester discovers that a web application uses unsanitized user input to dynamically generate file paths. The tester identifies that the application is vulnerable to Remote File Inclusion (RFI). Which action should the tester take to exploit this vulnerability?
A. Inject a SQL query into the input field to perform SQL injection
B. Use directory traversal to access sensitive system files on the server
C. Provide a URL pointing to a remote malicious script to include it in the web application
D. Upload a malicious shell to the server and execute commands remotely
Answer: C (LEAVE A REPLY)
Remote File Inclusion occurs when an application allows external resources to be loaded from user-controlled input. CEH teaches that an attacker can supply a remote URL pointing to a malicious script (for example, a PHP shell). When the vulnerable application includes this external file, the attacker's code executes on the server. This can lead to full system compromise, remote command execution, or lateral movement.

NEW QUESTION: 218
A penetration tester is conducting a security assessment for a client and needs to capture sensitive information transmitted across multiple VLANs without being detected by the organization's security monitoring systems.
The network employs strict VLAN segmentation and port security measures. Which advanced sniffing technique should the tester use to discreetly intercept and analyze traffic across all VLANs?
A. Deploy a rogue DHCP server to redirect network traffic
B. Exploit a VLAN hopping vulnerability to access multiple VLANs
C. Implement switch port mirroring on all VLANs
D. Use ARP poisoning to perform a man-in-the-middle attack
Answer: (SHOW ANSWER)
VLAN hopping is an advanced attack technique described in CEH materials, used to bypass VLAN segmentation by exploiting switch misconfigurations or vulnerabilities. Two primary methods-switch spoofing and double tagging-allow attackers to gain access to

traffic from VLANs they are not authorized to view. This technique enables the capture of inter-VLAN traffic without requiring administrative privileges or triggering security tools. Port mirroring requires administrative control and is not an attack method. Rogue DHCP servers target IP assignment, not VLAN segmentation. ARP poisoning is effective only within a single broadcast domain and cannot traverse VLAN boundaries. Because the objective is to silently access multiple VLANs despite enforced segmentation, VLAN hopping is the correct technique as per CEH's network perimeter attack methodology.

NEW QUESTION: 219
You are an ethical hacker at Vanguard Cyber Defense, hired by Sunrise Logistics, a freight management company in Houston, Texas, to evaluate the security of their shipment tracking portal. During your engagement, you analyze how the application handles user-submitted data. You observe the behavior of the shipment search feature and monitor the HTTP GET requests being sent to the server. Your objective is to determine how user input is processed by the backend system and whether those parameters can be used to manipulate SQL queries. Based on this activity, which step of the SQL injection methodology are you performing?
A. Advanced SQL Injection
B. Launching SQL Injection Attacks
C. Database Enumeration
D. Identifying Data Entry Paths
Answer: D (LEAVE A REPLY)
In the CEH SQL injection methodology, the initial stages focus on understanding where and how user- controlled input enters the application and reaches backend components such as database queries. The activity described is reconnaissance and mapping of input vectors: Rachel is observing the shipment search function, watching HTTP GET parameters, and determining whether those parameters are processed in a way that could influence SQL logic. This directly corresponds to the phase commonly described as identifying data entry paths, where the tester locates all possible points of injection such as URL query strings, form fields, cookies, HTTP headers, and API parameters.
At this stage, the ethical hacker is not yet executing payloads to exploit the database. Instead, they are profiling the request structure, parameter names, values, and server responses to understand how the application behaves when supplied with different inputs. CEH guidance emphasizes that effective SQL injection testing begins by enumerating input sources and determining which of them appear to be reflected in server-side operations. Monitoring HTTP GET requests is a typical technique because query string parameters often map to backend search queries, filters, or record lookups, making them frequent injection candidates if server-side validation and query construction are weak.
The other options occur later. Launching SQL injection attacks involves actively injecting test characters and payloads to confirm injection. Database enumeration happens after a vulnerability is confirmed, to extract schema information and data. Advanced SQL injection

refers to more specialized techniques such as out-of- band, time-based blind, or WAF evasion. Since the task here is identifying and assessing potential injection points, the correct step is identifying data entry paths.

NEW QUESTION: 220
A penetration tester has gained access to a target system using default credentials. What is the most effective next step to escalate privileges on the system?
A. Perform a denial-of-service (DoS) attack to crash the system
B. Use a known local privilege escalation vulnerability to gain admin access
C. Execute a Cross-Site Scripting (XSS) attack on the system's login page
D. Use a dictionary attack to brute-force the root password
Answer: B (LEAVE A REPLY)
Once initial access is obtained-especially through weak or default credentials-the CEH system hacking methodology directs the tester to proceed to privilege escalation. The objective is to elevate user-level access to administrative or system-level privileges so the attacker can perform unrestricted actions such as installing tools, modifying configurations, accessing protected files, and pivoting laterally. CEH materials emphasize using privilege escalation vulnerabilities, such as misconfigured services, kernel exploits, unpatched local privilege escalation flaws, weak file permissions, and token impersonation. A denial-of-service attack is counterproductive and does not support post-exploitation goals. XSS is a web application attack vector and unrelated to operating system privilege manipulation. Brute-forcing the root password is noisy, slow, and unnecessary when authenticated access is already established. Therefore, exploiting a known local privilege escalation vulnerability is the appropriate CEH-aligned next step.

NEW QUESTION: 221
During a penetration test for a global e-commerce platform in Dallas, ethical hacker Maria simulates a large- scale DoS campaign. Instead of sending attack traffic directly, she forges requests to multiple open services across the internet. These services unknowingly reply to the victim system, multiplying the amount of traffic hitting the target. Within minutes, the victim ' s server is overwhelmed by a flood of responses, even though Maria ' s own machine generated only a small amount of traffic.
Which attack technique is Maria most likely demonstrating?
A. Smurf Attack
B. Distributed Reflection Denial-of-Service (DRDoS)
C. Botnet
D. NTP Amplification Attack
Answer: B (LEAVE A REPLY)
The correct answer is B. Distributed Reflection Denial-of-Service (DRDoS) because the scenario describes the two defining elements of DRDoS: reflection and amplification at scale using third-party systems. Maria

"forges requests" (i.e., spoofs the victim's IP address as the source) to "multiple open services across the internet." Those services then send their replies to the spoofed source-the victim-so the victim receives a large volume of unsolicited responses. This is reflection: the attacker does not attack the victim directly; instead, the attacker reflects traffic off other servers. The "multiplying the amount of traffic" indicates amplification: many protocols/services respond with packets significantly larger than the request, so the attacker's small outbound traffic results in a much larger inbound flood against the target. The mention of "multiple open services" and being overwhelmed by a "flood of responses" is classic DRDoS behavior. From a defender's perspective, DRDoS attacks are difficult because the traffic often appears to come from legitimate servers, and the victim is receiving replies to requests it never sent. Mitigations include source address validation (BCP 38 anti-spoofing), rate limiting, filtering/ACLs for abused UDP services, and upstream scrubbing/CDN or DDoS protection.
Why the other options are less accurate: Smurf is a specific reflection/amplification attack using ICMP to a broadcast address (now largely mitigated by disabling directed broadcasts). Botnet describes the attacker's infrastructure (many compromised machines) but not the reflection/amplification mechanism; a botnet can be used to launch many types of DDoS attacks. NTP amplification is one specific DRDoS variant using misconfigured NTP servers (UDP/123). The question describes the broader technique across "multiple open services" rather than naming NTP specifically, so the best match is the general category DRDoS.
Therefore, Maria is demonstrating a Distributed Reflection Denial-of-Service (DRDoS) attack.

NEW QUESTION: 222
A corporation migrates to a public cloud service, and the security team identifies a critical vulnerability in the cloud provider's API. What is the most likely threat arising from this flaw?
A. Distributed Denial-of-Service (DDoS) attacks on cloud servers
B. Unauthorized access to cloud resources
C. Physical security compromise of data centers
D. Compromise of encrypted data at rest
Answer: (SHOW ANSWER)
The CEH Cloud Computing module identifies cloud APIs as one of the most critical attack surfaces in public cloud environments. APIs control provisioning, configuration, authentication, and management of cloud resources.
A vulnerability in a cloud API can allow attackers to:
* Bypass authentication
* Escalate privileges
* Access or modify cloud resources
* Create or delete services

Option B is therefore correct.
Option A relates to availability, not API flaws.
Option C is managed by the provider and unrelated to APIs.
Option D would require key compromise, not just API weakness.
CEH strongly emphasizes API security as a top cloud risk.

NEW QUESTION: 223
During an internal red team engagement at a financial services firm, an ethical hacker named Anika tests persistence mechanisms after successfully gaining access to a junior employee's workstation. As part of her assessment, she deploys a lightweight binary into a low-visibility system folder. To maintain long-term access, she configures it to launch automatically on every system reboot without requiring user interaction.
Which of the following techniques has most likely been used to ensure the persistence of the attacker's payload?
A. Installing a keylogger
B. Creating scheduled tasks
C. Modifying file attributes
D. Injecting into the startup folder
Answer: B (LEAVE A REPLY)
Creating scheduled tasks is the most likely persistence technique because it can be configured to execute automatically at system startup or on reboot without requiring a user to log in or manually launch anything. In CEH-aligned post-exploitation and persistence concepts, attackers commonly use operating system native mechanisms that blend into normal administrative activity. A scheduled task fits this goal well because it can be named to look legitimate, set to run under a specific account, and triggered by events such as system boot, user logon, or a timed schedule. The scenario explicitly states the payload launches on every reboot without user interaction, which aligns with a boot-triggered scheduled task.
Injecting into the startup folder usually triggers execution when a user logs on, not strictly on system reboot, and it depends on an interactive user session. That contradicts the requirement of no user interaction.
Modifying file attributes, such as setting hidden or system attributes, improves stealth and makes a file less noticeable, but it does not create an automatic execution mechanism by itself. Installing a keylogger is a capability for capturing keystrokes, not a persistence method, and it does not inherently guarantee execution after reboot unless paired with an auto-start mechanism.
Therefore, the action that directly ensures the binary runs after each reboot in a controlled and reliable way is creating scheduled tasks, which is a classic persistence method emphasized in ethical hacking workflows for demonstrating real-world attacker behavior and improving defensive detection and hardening.

NEW QUESTION: 224
An e-commerce platform hosted on a public cloud infrastructure begins to experience significant latency and timeouts. Logs show thousands of HTTP connections sending headers extremely slowly and never completing the full request. What DoS technique is most likely responsible?
A. Slowloris holding web server connections
B. Fragmentation flood attack
C. UDP application-layer flooding
D. SYN flood with spoofed source IPs
Answer: A (LEAVE A REPLY)
CEH v13 identifies Slowloris as a low-bandwidth yet highly effective application-layer DoS technique that works by opening many HTTP connections and sending headers very slowly, never completing the request.
Because the server must maintain these half-open HTTP sessions, its connection pool becomes saturated, preventing it from servicing legitimate users. Slowloris is particularly dangerous because it does not rely on malformed packets, high traffic volume, or protocol abuses; instead, it mimics legitimate HTTP behavior, making it difficult for firewalls or IDS systems to distinguish malicious traffic. This aligns exactly with the described scenario, where thousands of legitimate-looking HTTP connections are gradually consuming server resources. Fragmentation attacks (Option B) target packet reconstruction, UDP floods (Option C) generate high-bandwidth noise, and SYN floods (Option D) impact the TCP handshake layer, not the HTTP header behavior. Slowloris' unique use of slow HTTP headers directly matches the symptoms described.

NEW QUESTION: 225
Which patch management strategy is most effective?
A. External-only patches
B. Automated patch management with monitoring
C. Manual patching on live servers
D. Applying all patches regardless of source
Answer: (SHOW ANSWER)
CEH v13 identifies automated patch management as the most secure and scalable approach. Automated tools ensure timely deployment, validation, rollback capability, and compliance reporting.
Manual patching increases human error. Applying patches from unknown sources introduces malware risk.
Limiting patches contradicts best practices.
Therefore, Option B is correct.

NEW QUESTION: 226

You discover an unpatched Android permission-handling vulnerability on a device with fully updated antivirus software. What is the most effective exploitation approach that avoids antivirus detection?

A. Develop a custom exploit using obfuscation techniques

B. Use Metasploit to deploy a known payload

C. Install a rootkit to manipulate the device

D. Use SMS phishing to trick the user

Answer: (SHOW ANSWER)

The CEH Mobile Platform Security module explains that mobile antivirus solutions rely heavily on signatures and known exploit patterns. A custom exploit with obfuscation is far more likely to bypass detection.

CEH explicitly teaches that:

Zero-day or unpatched vulnerabilities

Custom, obfuscated payloads

Minimal use of known frameworks

are the most effective for bypassing endpoint defenses during controlled testing.

Option A is correct.

Options B and C are easily detected.

Option D is social engineering, not a technical exploit.

NEW QUESTION: 227

A cybersecurity company wants to prevent attackers from gaining information about its encrypted traffic patterns. Which of the following cryptographic algorithms should they utilize?

A. HMAC

B. RSA

C. DES

D. AES

Answer: D (LEAVE A REPLY)

According to the CEH Cryptography module, strong symmetric encryption algorithms are essential for protecting data confidentiality and obscuring traffic content.

AES (Advanced Encryption Standard) is the industry-standard symmetric encryption algorithm approved by NIST and recommended by CEH for encrypting data in transit and at rest. AES provides strong resistance against cryptanalysis and prevents attackers from deriving meaningful information from encrypted traffic.
Option D is correct because AES is efficient, secure, and widely implemented.
Option A (HMAC) provides integrity and authentication, not encryption.
Option B (RSA) is computationally expensive and not suitable for bulk traffic encryption.
Option C (DES) is deprecated due to weak key length.
CEH materials clearly recommend AES over legacy algorithms.

NEW QUESTION: 228
A cybersecurity team at a regional healthcare provider is conducting an internal red team exercise to assess their exposure to service enumeration attacks. Amanda, a senior penetration tester, is assigned to probe the internal network for services that may reveal usernames, group information, or system details without requiring prior authentication. She decides to target common services running on specific ports that are often misconfigured or loosely monitored. During her reconnaissance, Amanda identifies several open ports across various hosts and must now prioritize which ones to probe first for maximum information gain related to enumeration. Which of the following services should Amanda target as a priority to enumerate usernames and group information without authentication?
A. TCP 139 and UDP 137, 138
B. TCP 21 and UDP 137, 138
C. TCP 23 and UDP 137, 138
D. TCP 25 and UDP 133
Answer: A (LEAVE A REPLY)
TCP 139 and UDP 137 and 138 correspond to NetBIOS over TCP/IP services that are closely associated with Windows file and printer sharing and legacy SMB browsing. In CEH methodology, these ports are high-value enumeration targets because NetBIOS name service and datagram service can disclose hostnames, domain or workgroup names, logged-in users, and shared resource details, often before any strong authentication occurs.
UDP 137 is used for NetBIOS Name Service, which supports name registration and lookup. UDP 138 supports NetBIOS Datagram Service, commonly tied to browsing and announcement traffic. TCP 139 supports NetBIOS Session Service, historically used to establish sessions for SMB traffic and to query share and user-related information when configurations are weak.
In real environments, misconfigurations such as permissive share settings, legacy protocols, or anonymous and guest-access allowances can allow an attacker to enumerate user accounts, groups, and policies indirectly through browsing data, share lists, and RPC-related exposure that frequently accompanies SMB environments. CEH training emphasizes prioritizing enumeration against Windows networking services because the

information gained can rapidly support follow-on attacks such as password spraying, targeted phishing, lateral movement, and privilege escalation planning.
The other choices include TCP 21 FTP, TCP 23 Telnet, and TCP 25 SMTP, which may expose banners or allow limited user enumeration in specific configurations, but they are not the primary ports associated with classic Windows user and group enumeration. UDP 133 is not a standard enumeration target in this context.
Therefore, TCP 139 with UDP 137 and 138 is the best priority set for username and group-related enumeration.

NEW QUESTION: 229
A cybersecurity research team identifies suspicious behavior on a user's Android device. Upon investigation, they discover that a seemingly harmless app, downloaded from a third-party app store, has silently overwritten several legitimate applications such as WhatsApp and SHAREit. These fake replicas maintain the original icon and user interface but serve intrusive advertisements and covertly harvest credentials and personal data in the background. The attackers achieved this by embedding malicious code in utility apps like video editors and photo filters, which users were tricked into installing. The replacement occurred without user consent, and the malicious code communicates with a command-and-control (C&C) server to execute further instructions. What type of attack is being carried out in this scenario?
A. Simjacker attack
B. Man-in-the-Disk attack
C. Agent Smith attack
D. Camfecting attack
Answer: C (LEAVE A REPLY)
CEH v13 describes Agent Smith-style attacks as malicious Android operations where an app silently replaces legitimate applications by exploiting weaknesses in the Android app update and installation processes. These attacks often begin when users download seemingly innocent apps from untrusted third-party marketplaces.
Once installed, the malicious application injects harmful code into other apps, overwriting them while preserving their icons and interface, allowing the attacker to harvest credentials, display ads, or maintain persistence without detection. CEH explains that this technique takes advantage of Android's APK structure, sideloading vulnerabilities, and lack of signature validation in compromised environments. Simjacker (Option A) targets SIM toolkit vulnerabilities and does not replace apps. Man-in-the-Disk (Option B) abuses external storage operations but does not overwrite applications. Camfecting (Option D) refers to hijacking smartphone cameras. The described malicious replacement of legitimate apps exactly matches the Agent Smith attack pattern.

NEW QUESTION: 230

You are instructed to perform a TCP NULL scan. In the context of TCP NULL scanning, which response indicates that a port on the target system is closed?

A. ICMP error message

B. TCP SYN/ACK packet

C. No response

D. TCP RST packet

Answer: (SHOW ANSWER)

TCP NULL scanning is a stealth scanning technique covered in CEH v13 Reconnaissance and Network Scanning. In a NULL scan, all TCP flags are set to zero. According to RFC 793 and CEH documentation, closed ports must respond with a TCP RST (Reset) packet. If the port is open, the target typically does not respond, making this technique useful for firewall evasion.

Therefore:

RST response = Closed port

No response = Open or filtered port

Other options do not apply to NULL scans:

SYN/ACK is associated with SYN scans.

ICMP errors may indicate filtering, not port state.

NEW QUESTION: 231

During a routine security audit, administrators found that cloud storage backups were illegally accessed and modified. What countermeasure would most directly mitigate such incidents in the future?

A. Deploying biometric entry systems

B. Implementing resource auto-scaling

C. Regularly conducting SQL injection testing

D. Adopting the 3-2-1 backup model

Answer: D (LEAVE A REPLY)

According to CEH v13 Cloud Computing, backup integrity and resilience are critical components of cloud security. The 3-2-1 backup model is a widely recommended best practice to mitigate unauthorized access, data corruption, and ransomware-related incidents.

The 3-2-1 rule dictates that organizations should maintain:

3 copies of critical data

Stored on 2 different media types

With 1 copy stored offsite or offline

This approach ensures that even if one backup is compromised, altered, or deleted-as described in the scenario-clean and trusted versions of the data remain available for restoration. CEH v13 emphasizes that offline or immutable backups significantly reduce the impact of malicious modification.

Option A focuses on physical security, which does not protect cloud backups. Option B addresses availability, not integrity. Option C is relevant to web application security, not backup protection.
CEH v13 explicitly highlights backup segregation and redundancy as key countermeasures against cloud data compromise. Therefore, Option D is the most direct and effective mitigation strategy.

NEW QUESTION: 232
You perform a SYN (half-open) scan and receive a SYN/ACK packet in response. How should this result be interpreted?
A. The target IP is not reachable
B. The scanned port is open
C. The scanned port is filtered
D. The scanned port is closed
Answer: B (LEAVE A REPLY)
In CEH v13 Network Scanning, a SYN scan-also known as a half-open scan-is one of the most common and reliable techniques used to identify open TCP ports. This method involves sending a TCP SYN packet to a target port and analyzing the response without completing the full three-way handshake.
When a scanner sends a SYN packet:
* SYN/ACK response # The port is OPEN
* RST response # The port is CLOSED
* No response or ICMP unreachable # The port is FILTERED
In this scenario, the receipt of a SYN/ACK packet clearly indicates that the target system is willing to establish a TCP connection on that port. The scanner typically responds with a RST packet instead of an ACK to avoid completing the connection, thereby remaining stealthy.
Option B is therefore correct and aligns exactly with CEH v13 definitions.
Option A is incorrect because unreachable hosts do not respond with SYN/ACK.
Option C is incorrect because filtered ports usually do not respond or return ICMP errors.
Option D is incorrect because closed ports respond with RST, not SYN/ACK.
CEH v13 emphasizes SYN scanning as a preferred method due to its balance of accuracy and reduced logging. Understanding TCP flag behavior is fundamental for interpreting scan results correctly.

NEW QUESTION: 233
Which sophisticated DoS technique is hardest to detect and mitigate?
A. Distributed SQL injection DoS
B. Coordinated UDP flood on DNS servers
C. Zero-day exploit causing service crash
D. Smurf attack using ICMP floods

Answer: A (LEAVE A REPLY)
CEH v13 classifies application-layer DoS attacks as the most difficult to detect and mitigate. A distributed SQL injection-based DoS exploits database query processing by overwhelming backend systems with malicious but syntactically valid requests.
Unlike volumetric attacks, this method generates low-bandwidth, high-impact traffic that appears legitimate.
Traditional DDoS protections often fail to identify such traffic, especially when it targets authenticated services like online banking.
UDP floods, Smurf attacks, and ICMP-based attacks are well-known and more easily mitigated with rate limiting and filtering. Zero-day exploits cause service disruption but are not primarily DoS techniques.
CEH v13 highlights that application-layer DoS attacks blend seamlessly with normal traffic patterns, making them exceptionally challenging. Thus, option A is correct.

NEW QUESTION: 234
You are Ethan Brooks, an ethical hacker at Vanguard Security Solutions, hired to perform a wireless penetration test for Pacific Logistics, a shipping company in Seattle, Washington. Your task is to identify all Wi-Fi networks in range without alerting the network administrators. Using a laptop with a Wi-Fi card, you monitor radio channels to detect access points and their BSSIDs without sending any probe requests or injecting data packets.
Based on the described method, which Wi-Fi discovery technique are you employing?
A. Network Discovery Software
B. Active Footprinting
C. Wash Command
D. Passive Footprinting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 235
In the financial hub of Charlotte, North Carolina, ethical hacker Raj Patel is contracted by TrustBank, a regional U.S. bank, to evaluate their online loan application portal. During testing, Raj submits crafted input into the portal ' s form fields and notices that the server ' s HTTP responses are unexpectedly altered. His payloads cause additional headers to appear and even inject unintended content into the output, creating opportunities for attackers to manipulate web page behavior and deliver malicious data to users.
Which type of vulnerability is Raj most likely exploiting in TrustBank ' s online loan application portal?
A. HTTP Response Splitting
B. XML Poisoning
C. XML External Entity (XXE) Injection
D. Server-Side Request Forgery (SSRF)

Answer: A (LEAVE A REPLY)
The described behavior strongly matches HTTP Response Splitting. This vulnerability occurs when an application includes unsanitized user input in HTTP response headers. By injecting carriage return and line feed characters (CRLF), an attacker can "split" the server's response into multiple parts-causing additional headers to appear or injecting unintended body content. The scenario explicitly says Raj's payloads cause "additional headers to appear" and "inject unintended content into the output," which is the classic outcome of response splitting.
Why this matters: response splitting can enable attacks such as web cache poisoning, cookie manipulation, redirection, and cross-site scripting-like impacts through header/body injection. For example, if an attacker can inject a Set-Cookie header, they may set or overwrite cookies in the victim's browser. If they can inject a Location header, they may force redirects. If they inject content into the body, they may deliver malicious scripts or alter page behavior-especially when combined with caching intermediaries. The vulnerability typically arises in features that reflect user input into headers such as Location, Set-Cookie, Content- Disposition, or custom headers.
The other options do not match the symptoms:
XML Poisoning (B) and XXE (C) relate to XML parsing and entity resolution; they do not directly cause added HTTP headers in responses.
SSRF (D) involves forcing the server to make outbound requests to internal/external resources; it may expose data but does not primarily manifest as injected response headers and altered response structure.
Therefore, Raj is most likely exploiting A. HTTP Response Splitting.

NEW QUESTION: 236
A multinational company plans to deploy an IoT-based environmental control system across global manufacturing units. The security team must identify the most likely attack vector an Advanced Persistent Threat (APT) group would use to compromise the system. What is the most plausible method?
A. Launching a DDoS attack to overload IoT devices
B. Compromising the system using stolen user credentials
C. Exploiting zero-day vulnerabilities in IoT device firmware
D. Performing an encryption-based Man-in-the-Middle attack
Answer: C (LEAVE A REPLY)
The CEH IoT and APT Threat modules describe APT groups as highly skilled adversaries that favor stealth, persistence, and advanced exploitation techniques. IoT environments are particularly attractive due to:
Limited monitoring
Infrequent firmware updates
Weak or proprietary security mechanisms

CEH highlights that APT actors often exploit zero-day vulnerabilities in firmware to gain long-term, covert access to IoT systems. Firmware-level exploitation allows attackers to maintain persistence while evading traditional security controls.
Option C is correct.
Option A is noisy and short-term.
Option B is common but less sophisticated for APTs.
Option D is possible but secondary compared to firmware exploitation.
CEH emphasizes firmware security as a critical concern in IoT deployments.

NEW QUESTION: 237
A penetration tester is tasked with uncovering historical content from a company's website, including previously exposed login portals or sensitive internal pages. Direct interaction with the live site is prohibited due to strict monitoring policies. To stay undetected, the tester decides to explore previously indexed snapshots of the organization's web content saved by external sources. Which approach would most effectively support this passive information-gathering objective?
A. Search with intext:"login" site:target.com to retrieve login data
B. Use the link: operator to find backlinks to login portals
C. Apply the cache: operator to view Google's stored versions of target pages
D. Use the intitle:login operator to list current login pages
Answer: C (LEAVE A REPLY)
Passive reconnaissance is emphasized throughout CEH as an essential method for gathering intelligence without alerting monitoring systems. When the tester cannot interact with the live site, they must rely entirely on third-party archives or cached content stored by search engines or internet archival services. Google's cache function provides previously stored versions of web pages exactly for this purpose. CEH explains that attackers frequently use cached content to retrieve outdated login portals, administrative pages, exposed directories, or other sensitive elements that may no longer appear on the live web server. Unlike operators such as intext or intitle, which query live indexed metadata, the cache operator retrieves historical snapshots without accessing the target website. The link operator identifies backlinks but does not provide historical page content. Only the cache operator directly supports viewing previous versions of pages passively, aligning perfectly with the requirement to avoid detection while gathering intelligence on legacy web content.

NEW QUESTION: 238
A penetration tester is hired by a company to assess its vulnerability to social engineering attacks targeting its IT department. The tester decides to use a sophisticated pretext involving technical jargon and insider information to deceive employees into revealing their network credentials. What is the most effective social engineering technique the tester should employ to maximize the chances of obtaining valid credentials without raising suspicion?

A. Conduct a phone call posing as a high-level executive requesting urgent password resets
B. Send a generic phishing email with a malicious attachment to multiple employees
C. Create a convincing fake IT support portal that mimics the company's internal systems
D. Visit the office in person as a maintenance worker to gain physical access to terminals
Answer: (SHOW ANSWER)
CEH training emphasizes that highly tailored social engineering attacks-those exploiting trust in internal workflows and perceived technical authority-are far more effective than generic or mass-distributed phishing attempts. A fake IT support portal that mirrors internal systems leverages procedural familiarity: IT departments commonly instruct employees to log into support portals for troubleshooting, credential verification, or ticket updates. When the attacker enhances the pretext with insider terminology and references to real internal systems, employees are more likely to trust the portal and enter credentials. CEH highlights that successful social engineering attacks mimic legitimate processes to avoid suspicion. Phone calls posing as executives often introduce risk due to real-time interaction and scrutiny. Generic phishing lacks personalization and is easily detected. Physical impersonation introduces operational risk and may not yield credentials. Therefore, a fake IT support portal aligned with IT workflows is the optimal method.

NEW QUESTION: 239
You are Liam Chen, an ethical hacker at CyberGuard Analytics, hired to test the social engineering defenses of Coastal Trends, a retail chain in Los Angeles, California. During a covert assessment, you craft a deceptive message sent to the employees' company phones, claiming a critical account update is needed and directing them to a link that installs monitoring software. Several employees interact with the link, exposing a vulnerability to a specific mobile attack vector. Based on this approach, which mobile attack type are you simulating?
A. Bluebugging
B. SMS Phishing
C. Call Spoofing
D. OTP Hijacking
Answer: B (LEAVE A REPLY)
SMS Phishing, commonly called smishing, is the correct answer because the attack method is a deceptive text message sent to mobile devices that lures recipients into clicking a malicious link. In CEH-aligned social engineering coverage, smishing is a direct extension of phishing that uses SMS as the delivery channel. The attacker typically creates urgency or authority, such as "critical account update needed," to trigger fast compliance. The message then pushes the victim to a malicious URL that can deliver malware, prompt credential entry, or enroll the device into a monitoring or management profile depending on platform and permissions. The key indicators in the question are company phones, a crafted message, and a link that installs monitoring software, which fits smishing exactly.

Bluebugging is a Bluetooth-based attack where the attacker exploits Bluetooth weaknesses to gain unauthorized access to a device, read data, place calls, or send messages, and it does not rely on sending a deceptive SMS link. Call spoofing is manipulating caller ID to impersonate a trusted number during voice calls, not delivering a malicious installation link through text. OTP hijacking focuses on intercepting or tricking users into revealing one-time passwords, often through SIM swapping, malware, or real-time phishing, but the scenario emphasizes installing monitoring software through a link rather than capturing a one-time code.
Defenses highlighted in ethical security training include mobile security awareness, blocking unknown links, using mobile threat defense, restricting app installation from untrusted sources, enforcing MDM controls, and monitoring SMS-based social engineering indicators.

NEW QUESTION: 240
A penetration tester is conducting an external assessment of a corporate web server. They start by accessing
https://www.targetcorp.com/robots.txt and observe multiple Disallow entries that reference directories such as
/admin-panel/, /backup/, and /confidentialdocs/. When the tester directly visits these paths via a browser, they find that access is not restricted by authentication and gain access to sensitive files, including server configuration and unprotected credentials. Which stage of the web server attack methodology is demonstrated in this scenario?
A. Injecting malicious SQL queries to access sensitive database records
B. Performing a cross-site request forgery (CSRF) attack to manipulate user actions
C. Gathering information through exposed indexing instructions
D. Leveraging the directory traversal flaw to access critical server files
Answer: C (LEAVE A REPLY)
The CEH web server attack methodology describes reconnaissance as a key phase, where testers gather publicly available information before attempting exploitation. Robots.txt is commonly used by administrators to instruct web crawlers about which directories should not be indexed. CEH emphasizes that attackers regularly review robots.txt because it often exposes sensitive directories unintentionally, providing valuable intelligence about internal structure, configuration paths, administrative pages, and potential weak points. In this scenario, the tester observes "Disallow" entries and then discovers the directories are not protected by authentication, allowing direct access to sensitive files. This falls under information gathering through exposed indexing instructions rather than directory traversal, which involves path-manipulation exploits. The tester is not altering file paths or inserting traversal sequences; instead, they are reviewing publicly available indexing instructions and discovering misconfigured access controls. This perfectly aligns with the reconnaissance phase of the CEH methodology, where attackers learn about server architecture using passive or minimally intrusive techniques.

NEW QUESTION: 241
While assessing a web server, a tester sends malformed HTTP requests and compares responses to identify the server type and version. What technique is being employed?
A. Fingerprinting server identity using banner-grabbing techniques
B. Sending phishing emails to extract web server login credentials
C. Conducting session fixation using malformed cookie headers
D. Injecting scripts into headers for persistent XSS attacks
Answer: A (LEAVE A REPLY)
CEH v13 explains that fingerprinting is a core reconnaissance technique used to identify software versions, server types, and configurations by analyzing how systems respond to crafted or abnormal input. When testers send malformed HTTP verbs, unusual headers, or atypical URI structures, the server's specific response codes, banners, and error messages reveal distinctive behavioral patterns. These patterns allow tools like httprint, Nmap NSE scripts, and custom probes to match the responses to known server profiles. This technique is part of active reconnaissance, enabling attackers to determine vulnerabilities associated with specific versions. Phishing (Option B) is unrelated to protocol analysis. Session fixation (Option C) manipulates session identifiers, not HTTP response patterns. Persistent XSS (Option D) relies on web application vulnerabilities, not server fingerprinting. Thus, the tester is performing HTTP-based server fingerprinting.

NEW QUESTION: 242
You are Sameer Das, an ethical hacker hired by a national utilities provider to assess the resilience of its power grid infrastructure. During your red team operation, you conduct a phishing campaign targeting field engineers and successfully gain access to the internal OT network. From there, you identify unsecured access to the substation's programmable controllers and replace one of the system's firmware components with a custom payload. This payload silently processes your commands while maintaining access across reboots. Based on this action, which type of IoT OT threat are you simulating?
A. Forged malicious device
B. Firmware update attack
C. Remote access using backdoor

D. Exploit kits

Answer: B (LEAVE A REPLY)

The described activity most directly matches a firmware update attack. In CEH coverage of IoT and OT threats, firmware represents the low-level code that runs on embedded devices and industrial controllers, and compromising it is one of the most impactful persistence methods because it survives reboots and often persists through normal configuration resets. The scenario states that Sameer "replaces one of the system's firmware components with a custom payload" and that the payload "maintains access across reboots." Those are signature characteristics of a firmware-level compromise, typically achieved through insecure firmware update mechanisms, weak signing or verification controls, exposed update interfaces, or inadequate access controls on management ports.

A firmware update attack can occur when devices accept unsigned firmware, use weak integrity checks, allow downgrade to vulnerable versions, or expose update services without strong authentication. Once malicious firmware is installed, it can covertly execute commands, manipulate device behavior, hide its presence from higher-level monitoring, and create a durable foothold in OT environments where patching and reimaging are difficult. CEH emphasizes that OT devices such as programmable controllers and substation automation equipment are especially sensitive because firmware tampering can affect availability and safety, not just confidentiality.

Remote access using a backdoor is a broader concept and could be the payload's function, but the primary technique here is achieving persistence by modifying firmware. Forged malicious device refers to introducing rogue hardware, and exploit kits are typically used for automated exploitation on endpoints, not controller firmware replacement.

NEW QUESTION: 243

Joe, a cybersecurity analyst at Norwest Freight Services, has been assigned to run a vulnerability scan across the organization's infrastructure. He is specifically tasked with detecting weaknesses such as missing patches, unnecessary services, weak encryption, and authentication flaws across multiple servers. His scan identifies open ports and active services throughout the environment, providing a clear map of potential entry points for attackers.

Which type of vulnerability scanning best matches Joe's assignment?

A. Network-based Scanning

B. External Scanning

C. Application Scanning

D. Host-based Scanning

Answer: A (LEAVE A REPLY)

Joe's assignment is best described as network-based vulnerability scanning because the scan is mapping open ports and active services across multiple servers and identifying weaknesses visible through network exposure, such as unnecessary services, weak

encryption configurations on network services, and authentication-related flaws reachable over the network. Network-based scanning focuses on discovering and evaluating network-accessible entry points by probing hosts and services, enumerating versions /configurations, and correlating findings to known weaknesses.
The scenario highlights that the scan "identifies open ports and active services throughout the environment," producing "a clear map of potential entry points." That is the core outcome of network-based scanning: a view of the organization's externally or internally reachable services, where each listening port represents a possible attack path. From there, scanners can detect issues like outdated service versions (implying missing patches), insecure protocols (e.g., weak TLS ciphers), default credentials, and exposed administrative interfaces.
Why the other options are less accurate:
External scanning (B) refers to a scan performed from outside the organization's perimeter. The scenario says he is scanning across organizational infrastructure and focuses on multiple servers; it doesn't specify "from the Internet," so "external" is not the best classification.
Application scanning (C) targets web applications or specific application-layer logic (e.g., SQLi, XSS, auth bypass). Joe's focus is broader infrastructure exposure and service/port mapping.
Host-based scanning (D) typically involves local, credentialed inspection on the host (patch inventory, local config files, registry) rather than primarily mapping ports/services across many systems. While host-based scanning is valuable, the described output is network entry-point mapping.
Therefore, the scan type that best matches Joe's task is A. Network-based Scanning.

NEW QUESTION: 244
A penetration tester is tasked with scanning a network protected by an IDS and firewall that actively blocks connection attempts on non-standard ports. The tester needs to gather information on the target system without triggering alarms. Which technique should the tester use to evade detection?
A. Use a low-and-slow scan to reduce detection by the IDS
B. Conduct a full TCP Connect scan to confirm open ports
C. Perform a SYN flood attack to overwhelm the firewall
D. Execute a TCP ACK scan to map firewall rules and bypass the IDS
Answer: (SHOW ANSWER)
A low-and-slow scanning technique spreads probe attempts over long intervals, reducing the chance of triggering IDS signatures that rely on detecting rapid or high-volume scans. CEH highlights timing-based evasion as an effective method for reconnaissance against networks with strict perimeter controls.

NEW QUESTION: 245

In ethical hacking, what is black box testing?
A. Testing using only publicly available information
B. Testing without any prior knowledge of the system
C. Testing with full system knowledge
D. Testing knowing only inputs and outputs
Answer: B (LEAVE A REPLY)
According to CEH v13, black box testing refers to a testing approach where the ethical hacker has no prior knowledge of the internal structure, source code, or configuration of the system.
The attacker simulates a real-world external attacker, relying solely on discovery and exploitation techniques.
White box testing = full knowledge
Gray box testing = partial knowledge

NEW QUESTION: 246
During a penetration test at Pinnacle Bank in Chicago, ethical hacker Sarah injects crafted TCP packets into an active communication between a customer ' s browser and the online banking server. The victim ' s connection becomes unstable, allowing Sarah ' s system to maintain communication with the server in place of the legitimate client. She later demonstrates to the IT team how attackers could forcibly take control of live sessions through this approach.
Which type of session hijacking is Sarah performing in this scenario?
A. Passive Session Hijacking
B. Blind Hijacking
C. Man-in-the-Browser Attack
D. Active Session Hijacking
Answer: B (LEAVE A REPLY)
The correct answer is B. Blind Hijacking because the scenario describes injecting crafted TCP packets into an active client-server session to disrupt the legitimate client and take over the connection, without requiring the attacker to see (or fully rely on seeing) the server's responses. In CEH-aligned session hijacking classifications, blind hijacking is an active takeover technique at the TCP/session layer where the attacker forges packets (often with predicted or inferred TCP sequence numbers) to insert data into an existing session and potentially desynchronize the legitimate endpoints. By injecting traffic that causes instability (for example, triggering retransmissions, resets, or sequence/ack mismatch), the attacker can effectively push the victim out of sync or off the session while continuing to communicate with the server as if they were the client.
The key clue is that Sarah "injects crafted TCP packets" into an "active communication," and then the "victim' s connection becomes unstable," after which Sarah's system "maintain[s] communication with the server in place of the legitimate client." This aligns with blind hijacking concepts where the attacker does not simply observe (passive) but

actively manipulates the TCP stream to seize control. The attacker's goal is forced takeover of a live session, which often involves sequence prediction and packet injection to become the effective participant while the real client experiences disruption.
Why the other options are incorrect: Passive session hijacking is eavesdropping/monitoring traffic to capture session identifiers without altering the session; it does not involve injecting packets or destabilizing a connection. Man-in-the-Browser is a client-side attack (typically via malware in the browser) that manipulates transactions within the browser context; it is not a TCP packet injection technique. Active session hijacking is a broad category and is true at a high level, but the question asks for the type-and the specific technique described (TCP injection causing takeover) maps most directly to blind hijacking in CEH-style terminology.
Therefore, Sarah is demonstrating blind session hijacking.

NEW QUESTION: 247
Sarah, an ethical hacker at a San Francisco-based financial firm, is testing the security of their customer database after a recent data exposure incident. Her analysis reveals that the sensitive client information is safeguarded using a symmetric encryption algorithm. She observes that the algorithm processes data in 64-bit blocks and supports a variable key size from 32 to 448 bits. During her penetration test, Sarah intercepts a ciphertext transmission and notes that the encryption was developed as a replacement for DES, an older algorithm. She aims to determine if the algorithm's flexible key size could be susceptible to brute-force attacks. The algorithm is also noted for its use in secure storage, a critical application for the firm's data protection.
Which symmetric encryption algorithm should Sarah identify as the one used by the firm?
A. RC4
B. Twofish
C. AES
D. Blowfish
Answer: D (LEAVE A REPLY)
Blowfish is the only option that matches all the technical characteristics described. In CEH cryptography concepts, symmetric algorithms are commonly distinguished by their structure (block cipher versus stream cipher), block size, and supported key lengths. The question states the algorithm encrypts data in 64-bit blocks and supports a variable key size ranging from 32 bits up to 448 bits, and it was introduced as a replacement for DES. Blowfish fits precisely: it is a symmetric block cipher with a 64-bit block size and a configurable key length from 32 to 448 bits, designed to be fast in software and positioned historically as an alternative to older ciphers such as DES.
The other choices do not align with these identifying properties. RC4 is a stream cipher and does not operate on fixed-size blocks, so it cannot match the 64-bit block requirement. AES is a block cipher but uses a 128-bit block size with fixed key sizes of 128, 192, or 256

bits, not 32 to 448 bits. Twofish, while related historically as a successor-era design, also uses a 128-bit block size and fixed key sizes up to 256 bits, so it does not match either. From a CEH perspective, the mention of variable key sizes also hints at risk evaluation: shorter keys in any cipher can be brute-forced, so secure deployments require strong key length selection and proper key management. Additionally, Blowfish's 64-bit block size can be a concern in large-volume encryption scenarios due to block collision risks, which is why modern systems often prefer 128-bit block ciphers for new designs.

NEW QUESTION: 248
An attacker extracts the initial bytes from an encrypted file container and uses a tool to iterate through numeric combinations. What type of cryptanalytic technique is being utilized?
A. Seek identical digests across hash outputs
B. Test every possible password through automation
C. Force encryption key through quantum solving
D. Analyze output length to spot anomalies
Answer: B (LEAVE A REPLY)
CEH identifies brute-force cryptanalysis as a method in which an attacker systematically tests every possible key, password, or passphrase until the correct one is found. When an attacker obtains initial bytes from an encrypted container-often referred to as known plaintext-they can use this to validate attempts as the tool iterates through candidate keys. Automated brute-force tools compare decrypted results with known header patterns, file signatures, or expected byte structures to determine when the correct key is reached. This process aligns precisely with brute-force password testing described in CEH cryptography modules. Quantum solving is not part of CEH scope, digest comparison relates to collision attacks, and analyzing output length pertains to padding oracle detection. The correct classification is automated brute-force cryptanalysis.

NEW QUESTION: 249
Maya Patel from SecureHorizon Consulting is called to investigate a security breach at Dallas General Hospital in Dallas, Texas, where a lost employee smartphone was used to access sensitive patient records.
During her analysis, Maya finds that the hospital ' s mobile security policy failed to include a contingency to remotely secure compromised devices, allowing continued access to confidential data even after the device was lost. Based on this gap, which mobile security guideline should Maya recommend preventing similar incidents?
A. Utilize a secure VPN connection while accessing public Wi-Fi networks
B. Install device tracking software that allows the device to be located remotely
C. Register devices with a remote locate and wipe facility
D. Use anti-virus and data loss prevention DLP solutions
Answer: C (LEAVE A REPLY)

The central failure in the scenario is that a lost smartphone remained capable of accessing sensitive data, which means the organization lacked an effective lost device response control. In CEH-aligned mobile security guidance, one of the most important protections for lost or stolen devices is the ability to remotely secure the endpoint by locking it and wiping corporate data. This is typically implemented through Mobile Device Management tools and enterprise mobility controls. Registering devices with a remote locate and wipe facility ensures the security team can immediately take action once a device is reported missing, reducing the window in which an attacker can use stored sessions, cached credentials, saved tokens, or application access to reach protected resources such as patient records.
Option C is the best answer because it addresses both key needs implied by the incident: location capability to aid recovery and remote wipe to eliminate data exposure if recovery is uncertain. In healthcare environments, where protected health information is highly sensitive, CEH documentation emphasizes compensating controls that protect confidentiality when physical control of the device is lost. Remote wipe supports incident containment by preventing further access and limiting data disclosure.
Option B only provides tracking and does not guarantee data protection if the device cannot be recovered quickly. Option A helps protect data in transit on untrusted networks, but it does not solve the risk of a stolen device already authenticated to internal systems. Option D can help overall hygiene, but antivirus and DLP do not reliably stop misuse of a legitimately authenticated, lost device. Remote locate and wipe is the most direct mitigation for this exact gap.