ECCouncil.312-50v13.v2026-06-24.q254

Exam Code:	312-50v13
Exam Name:	Certified Ethical Hacker Exam (CEHv13)
Certification Provider:	ECCouncil
Free Question Number:	254
Version:	v2026-06-24
# of views:	106
# of Questions views:	2540
https://www.freepdfdumps.com/ECCouncil.312-50v13.v2026-06-24.q254.html	

NEW QUESTION: 1
During a red team test, a web application dynamically builds SQL queries using a numeric URL parameter.
The tester sends the following request:
http://vulnerableapp.local/view.php?id=1;
DROP TABLE users;
The application throws errors and the users table is deleted. Which SQL injection technique was used?
A. UNION-based SQL injection
B. Stacked (Piggybacked) queries
C. Boolean-based SQL injection
D. Error-based SQL injection
Answer: B (LEAVE A REPLY)
The CEH SQL Injection module defines stacked (piggybacked) queries as attacks where an attacker appends an additional SQL statement using a statement delimiter such as a semicolon.
In this scenario, the attacker executed a second query (DROP TABLE users) after the original query, resulting in destructive behavior.
Option B is correct.
Option A retrieves data, not execute destructive commands.
Option C infers logic outcomes.
Option D relies on error messages for data extraction.
CEH classifies stacked queries as high-impact SQL injection attacks.

NEW QUESTION: 2
During a penetration test at Pacific Trust Bank in Seattle, ethical hacker Mia Chen suspects that a server hosting customer transaction data may be a honeypot. To

investigate, she repeatedly sends crafted queries and observes how quickly the system responds. She notices that responses are consistently faster and more uniform than those of other production servers, raising her suspicion that the environment is designed to lure attackers.

Which technique is Mia most likely using to determine if the server is a honeypot?

A. Analyzing MAC Address

B. Analyzing Response Time

C. Fingerprinting the Running Service

D. Analyzing System Configuration and Metadata

Answer: (SHOW ANSWER)

The correct answer is B. Analyzing Response Time because the scenario explicitly describes Mia's method as repeatedly sending crafted queries and comparing the speed and consistency of responses with other production servers. In CEH-aligned honeypot and deception detection concepts, one practical way to suspect a decoy environment is to measure how it behaves under interaction and whether that behavior differs from real production systems. Honeypots are often instrumented to monitor attacker activity and may run simplified stacks, isolated resources, or simulated services. This can produce response characteristics that are noticeably different-such as responses that are too fast, too consistent, or unusually uniform even under varying query conditions-because the system may be returning pre-generated or emulated outputs rather than processing real workloads.

Real production servers typically show natural variance in response time due to legitimate traffic load, database I/O, caching effects, rate limiting, and resource contention. When a target consistently responds with minimal jitter and unusually stable latency, it can indicate a controlled or simulated environment designed for observation rather than normal business operations. By baselining and comparing response timing across multiple hosts, Mia is using timing behavior as a distinguishing signal to assess whether the server is behaving like a genuine production system or a monitored decoy.

Why the other options are less correct: Analyzing MAC Address is generally a local-network technique and not a primary way to validate honeypot behavior for an external-facing transaction server; it also does not align with the described repeated query timing. Fingerprinting the running service can help identify service type/version, but the question centers on consistency and speed rather than identifying signatures. Analyzing system configuration and metadata would involve inspecting headers, banners, OS/service metadata, or environment artifacts; useful, but not what Mia is doing here.

Therefore, Mia is most likely using response time analysis to assess whether the server behaves like a honeypot.

NEW QUESTION: 3

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: 4
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: D (LEAVE A REPLY)

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: 5
A financial startup in Chicago hires an ethical hacker to evaluate its exposure on hidden networks. The client is particularly concerned that confidential administrative documents might be circulating on .onion sites. To remain passive, the hacker relies on advanced search filters to look for files with headers suggesting management-related content. Which of the following queries would best meet this objective?
A. filetype:docx " credentials "
B. filetype:pdf intitle: " secure login " site:onion
C. filetype:pdf intitle: " admin access " site:onion
D. filetype:docx intitle: " user accounts " site:onion
Answer: C (LEAVE A REPLY)
The objective is to conduct passive reconnaissance for potentially exposed administrative documents on .
onion sites, using advanced search operators. The query should therefore (1) restrict results to the hidden- network domain space, (2) focus on document formats likely to contain internal material, and (3) use a title
/header hint that aligns with management or administration content.
Option C is the best match because it combines:
site:onion to constrain results to .onion resources (the target environment of concern), filetype:pdf to focus on a common format for internal documents (policies, reports, procedures, administrative exports), and intitle: " admin access " to search for pages/files whose title/header metadata indicates administrative relevance. Using intitle aligns with the requirement to look for files "with headers suggesting management- related content," because titles are a practical proxy for document headers and indexing metadata.
By comparison, A does not include site:onion, so it is not scoped to hidden services, and it targets
"credentials" rather than administrative documents. B includes site:onion and filetype:pdf, but the title focus is "secure login," which is more likely to find authentication pages or generic security guidance rather than administrative document exposure. D is also

plausible (docx + user accounts), but "user accounts" tends to point to account lists or HR-style docs rather than broader administrative access documentation, and PDFs are frequently used for formal administrative documentation and may be more commonly indexed.
Thus, C best satisfies the passive, targeted reconnaissance requirement for admin-related documents on .onion sites.

NEW QUESTION: 6
During an internal red team engagement at Orion Tech Labs, a leading software firm in Austin, Texas, ethical hacker Emily Carter was tasked with evaluating the resilience of the organization ' s software deployment processes. Knowing that the finance team frequently downloaded utility tools for generating PDFs, she repackaged a trusted PDF converter installer with a secondary payload. When an employee executed the installer, the converter installed and functioned normally, but in the background, a hidden executable silently initiated outbound network communication. The user remained unaware of any suspicious activity.
Which technique did Emily most likely use to ensure the malware executed alongside the legitimate application?
A. Downloader
B. Packer
C. Dropper
D. Wrapper
Answer: D (LEAVE A REPLY)
A wrapper is the most accurate choice because it describes a technique where a legitimate program is bundled together with a malicious payload so that, when the user launches what appears to be a normal installer or application, both the real software and the malware run. CEH materials commonly explain wrappers in the context of Trojanization: the attacker "wraps" a trusted executable or installer with an additional hidden component. This preserves normal functionality to avoid suspicion while still achieving covert execution of the malicious code. In the scenario, the PDF converter installs and works as expected, but a hidden executable runs silently and begins outbound communication-this is classic wrapper behavior designed to maintain user trust and reduce detection through normal user experience.
The other options do not fit as well. A downloader is malware whose primary purpose is to fetch additional payloads from the network; while outbound communication occurs here, the scenario emphasizes bundling and simultaneous execution with a legitimate installer, not primarily downloading. A packer is used to compress/obfuscate an executable to evade signature-based detection; it changes how a binary looks, but it does not inherently describe combining a legitimate installer with another payload. A dropper is designed to deliver and install malware onto a system, often extracting the payload; however, the hallmark detail here is that the legitimate application runs normally while the malicious

component is hidden within the same package, which aligns more precisely with a wrapper/Trojanized installer.
Defensively, CEH recommends controls such as application allowlisting, verifying digital signatures and hashes, using trusted software repositories, endpoint detection and response, and monitoring unusual outbound connections after software installation

NEW QUESTION: 7
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: 8
In the bustling tech hub of Silicon Valley, cybersecurity investigator Elena Martinez found herself deep into a late-night investigation at Horizon Tech Solutions on July 7, 2025. The company had reported sporadic network disruptions affecting their research team ' s access to critical project files. Elena, working under the cover of a maintenance window

from midnight to 3 AM PDT, began monitoring the internal network, focusing on a subnet reserved for the R & D department. She noticed a pattern of failed connection attempts logged just before each disruption, with multiple hosts reporting temporary IP address conflicts. Suspecting foul play, Elena deployed a discreet test to simulate an internal threat scenario. Shortly afterward, several workstations began showing unfamiliar gateway settings and redirected users to misleading login portals during routine access attempts. Despite these anomalies, no security alerts were triggered.
What type of attack technique did Elena most likely simulate?
A. DHCP Starvation Attack
B. Packet Sniffing
C. MAC Flooding
D. Rogue DHCP Server Attack
Answer: D (LEAVE A REPLY)
A Rogue DHCP Server attack best fits the symptoms because it directly explains unexpected gateway changes, IP conflicts, and traffic redirection to deceptive portals. In CEH network attack coverage, DHCP is a foundational service that automatically provides clients with IP configuration such as IP address, subnet mask, default gateway, and DNS servers. If an attacker introduces a rogue DHCP server on the same broadcast domain, clients may accept leases from the rogue server-especially if it responds faster than the legitimate DHCP infrastructure. Once that happens, the attacker can push a malicious default gateway or DNS server to victims. This allows redirection of traffic, man-in-the-middle positioning, and phishing-style interception, which matches the "unfamiliar gateway settings" and "misleading login portals" described.
The mention of "temporary IP address conflicts" also aligns: a rogue server can hand out addresses that overlap with legitimate allocations, causing intermittent connectivity issues and failed connection attempts.
While a DHCP starvation attack can create disruption by exhausting the DHCP pool, the key difference is outcome: starvation primarily denies service until a rogue server takes over. Here, the defining observable behavior is not just outage-it is misconfiguration and redirection, which points to the presence of a rogue DHCP server actively issuing malicious leases.
Packet sniffing alone would not change gateway settings, and MAC flooding is aimed at forcing switches to behave like hubs, not issuing IP configuration. Defensive controls include DHCP snooping, port security, network segmentation, and monitoring for unauthorized DHCP offers and anomalous lease patterns.

NEW QUESTION: 9
A fintech startup in Austin, Texas deploys several virtual machines within a public cloud environment.
During an authorized cloud security assessment, a tester uploads a small script to one of the instances through a web application vulnerability. After executing the script locally on

the instance, the tester retrieves temporary access credentials associated with the instance ' s assigned role. These credentials are then used to enumerate storage resources and access additional cloud services within the same account. Which cloud attack technique best corresponds to this activity?

A. Cloud Snooper Attack

B. Wrapping Attack

C. IMDS Attack

D. CP DoS Attack

Answer: C (LEAVE A REPLY)

The correct answer is IMDS Attack. CEH cloud security material explains that cloud instances often obtain temporary credentials from an Instance Metadata Service, commonly called IMDS, which supplies identity and role-based access details to workloads running on the virtual machine. If an attacker gains code execution on the instance, even through a separate web application flaw, the attacker may query the metadata endpoint locally and retrieve temporary credentials associated with the instance role. That is precisely what happens in this scenario: the tester runs a script on the VM, extracts temporary role credentials, and then uses them to enumerate storage and other services within the same cloud account. Wrapping attacks target SOAP message manipulation, while cloud snooper and CP DoS do not match the behavior of harvesting role credentials from local cloud metadata. CEH emphasizes that overprivileged instance roles and exposed metadata access can allow attackers to pivot from a single compromised workload into broader cloud service access. Because the key step is retrieving temporary credentials from the instance metadata service, the best match is IMDS Attack.

NEW QUESTION: 10

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: 11
A digital media company in Seattle, Washington deploys an Nginx-based infrastructure to support its internal analytics dashboard and content publishing portal. During an authorized red team engagement, a tester evaluates the web-based administrative interface used to upload configuration bundles and manage application components. While analyzing a file-upload feature, the tester observes that certain user-supplied parameters submitted with uploaded content are incorporated into backend processing routines with limited validation. By adjusting specific values in the request, he alters how the server-side component interprets those inputs. Subsequent log analysis shows that the modified input affected system-level operations executed under the web service context, despite no direct shell access being obtained. Which Nginx-related vulnerability best describes the weakness identified in this scenario?
A. Improper certificate validation
B. NULL pointer dereference in HTTP/3
C. OS command injection in nginxWebUI
D. Server-side request forgery (SSRF) vulnerability
Answer: (SHOW ANSWER)

The correct choice is OS command injection in nginxWebUI because the question describes untrusted input being passed into backend processing in a way that affects system-level operations. CEH web application material classifies command injection as an injection flaw that occurs when a vulnerable application allows attacker-controlled input to be interpreted by the operating system or shell environment. The key clue is that the tester manipulates parameters associated with uploaded content, and those altered values influence commands executed in the server-side web service context. That is the hallmark of command injection rather than SSRF, which would involve the server making unintended outbound requests, or certificate validation issues, which relate to TLS trust decisions. The mention of no direct shell access is also consistent with command injection, because the attacker does not need an interactive shell if malicious input can still alter system commands behind the application. CEH guidance repeatedly stresses that unvalidated input in web applications can lead to injection attacks, including command injection, when user-controlled values reach backend interpreters without strict sanitization, parameter control, or allow-list validation.

NEW QUESTION: 12
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: (SHOW ANSWER)
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: 13
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: 14

During a penetration test at a retail company in Seattle, Washington, an ethical hacker needs to disguise her scans so they appear to originate from a specific hardware vendor. The organization uses MAC-based logging, and by assigning a vendor-associated identifier, she can make her traffic blend in with legitimate devices on the network. Which Nmap command should she use to achieve this?

A. nmap -sT -Pn --spoof-mac 00:11:22 10.10.1.11

B. nmap -sT -Pn --spoof-mac Dell 10.10.1.11

C. nmap -sT -Pn --spoof-mac 0 10.10.1.11

D. nmap -sT -Pn --spoof-mac 00:01:02:25:56:AE 10.10.1.11

Answer: B (LEAVE A REPLY)

The correct option is B because it uses vendor-based MAC spoofing, which is the most direct way to make traffic appear to come from a device manufactured by a specific, recognizable vendor (in this case, "Dell"). In MAC addressing, the first portion of the MAC address is the OUI (Organizationally Unique Identifier), which identifies the vendor/manufacturer. Many security and asset tools perform lightweight device profiling by correlating observed OUIs with known vendors, and MAC-based logs may record or flag devices based on whether their OUIs match expected corporate endpoints.

Nmap supports MAC spoofing in a way that allows specifying a vendor name so the resulting MAC address is generated with an OUI associated with that vendor. This matches the requirement in the scenario: the tester wants the scan traffic to "blend in with legitimate devices" by adopting a vendor-associated identifier rather than using a random or obviously unusual MAC prefix.

Why the other options are less appropriate:

A provides only a partial prefix-like value (not a full MAC), and it does not explicitly map to a vendor name, making it less aligned with "specific hardware vendor" blending.

C uses 0 (zero), which is commonly associated with generating a random MAC rather than selecting a specific vendor identity; randomization does not guarantee blending with a chosen vendor's footprint.

D supplies a full explicit MAC address; while this can spoof a MAC, it does not inherently express the intent to "appear as a specific vendor" unless you already know that exact MAC's OUI belongs to the desired vendor. The question emphasizes selecting a vendor-associated identifier directly, which is exactly what option B does.

So, the best match for vendor-based disguise is B.

NEW QUESTION: 15

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: 16
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: (SHOW ANSWER)
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: 17
During a covert red team engagement, a penetration tester is tasked with identifying live hosts in a target organization's internal subnet (10.0.0.0/24) without triggering intrusion detection systems (IDS). To remain undetected, the tester opts to use the command nmap -sn -PE 10.0.0.0/24, which results in several " Host is up
" responses, even though the organization's IDS is tuned to detect high-volume scans. After the engagement, the client reviews the logs and is surprised that the scan was not flagged. What allowed the scan to complete without triggering alerts?
A. It used TCP ACK packets that were allowed through.
B. It used UDP packets that bypassed ICMP inspection.
C. It scanned only the ports open in the firewall whitelist.
D. It performed an ICMP Echo ping sweep without port probing.
Answer: D (LEAVE A REPLY)
CEH v13 explains that IDS systems are often tuned to detect active scanning behavior, especially port scans and TCP/UDP probing that generate recognizable signatures. The command nmap -sn -PE performs a pure ICMP Echo Request ping sweep without sending any TCP SYN, UDP probes, or other packets normally associated with port enumeration. Since this mode disables port scanning entirely, it produces minimal traffic that resembles legitimate network behavior. CEH emphasizes that many networks allow ICMP Echo traffic internally for diagnostics, so such pings may not be treated as suspicious unless rate thresholds are exceeded.
Because the tester avoided SYN packets, ACK probes, and UDP scans, the IDS saw no malicious pattern or connection attempts. The effectiveness of this technique is highlighted in CEH under passive and stealth reconnaissance, where minimal interaction is used to avoid detection. Thus, the scan succeeded because it relied solely on ICMP host discovery, not port scanning.

NEW QUESTION: 18

An attacker has partial root access to a mobile application. What control best prevents further exploitation?

A. Secure coding and automated reviews

B. Certificate pinning

C. Regular penetration testing

D. Mobile Application Management (MAM)

Answer: D (LEAVE A REPLY)

When partial root access exists, preventing further privilege abuse is the immediate priority. CEH v13 explains that Mobile Application Management (MAM) enforces granular access control, application isolation, and permission enforcement-even on compromised devices.

Secure coding (Option A) and testing (Option C) are preventative measures but do not contain an active compromise. Certificate pinning (Option B) protects communications, not application control.

MAM solutions allow administrators to revoke access, enforce policies, and isolate apps, limiting attacker capabilities post-compromise. Therefore, Option D is correct.

NEW QUESTION: 19

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: 20
In Portland, Oregon, ethical hacker Olivia Harper is hired by Cascade Biotech to test the security of their research network. During her penetration test, she simulates an attack by sending malicious packets to a server hosting sensitive genetic data. To evade detection, she needs to understand the monitoring system deployed near the network's perimeter firewall, which analyzes incoming and outgoing traffic for suspicious patterns across the entire subnet. Olivia's goal is to bypass this system to highlight vulnerabilities for the security team.
Which security system is Olivia attempting to bypass during her penetration test of Cascade Biotech's network?
A. Network-Based Intrusion Detection System
B. Host-Based Firewalls
C. Network-Based Firewalls
D. Host-Based Intrusion Detection System
Answer: (SHOW ANSWER)
The system described is a Network-Based Intrusion Detection System because it is positioned near the perimeter firewall and inspects traffic flowing across the network segment rather than activity on a single endpoint. In CEH-aligned coverage, a NIDS is deployed at strategic network points such as behind a firewall, on core switches, or on SPAN or TAP links to monitor inbound and outbound packets. Its purpose is to detect suspicious patterns, signatures, protocol anomalies, and indicators of scanning or exploitation attempts across multiple hosts and an entire subnet. The question explicitly says it "analyzes incoming and outgoing traffic" and looks for patterns "across the entire subnet," which matches NIDS scope and placement.
A Host-Based IDS, by contrast, runs on individual servers or workstations and monitors local events such as system calls, logs, file integrity, registry changes, and local network connections for that specific host. That does not match the perimeter-positioned, subnet-wide traffic analysis described. Host-based firewalls also operate per endpoint, enforcing rules for that machine only, and do not provide centralized subnet-wide packet inspection from a perimeter vantage point. A network-based firewall primarily enforces allow or deny policy and may perform stateful filtering, but it is not primarily described as a detection tool analyzing suspicious patterns; IDS is the detection-focused control.
Therefore, Olivia is attempting to bypass a Network-Based Intrusion Detection System to demonstrate how malicious traffic might evade monitoring controls placed near the firewall and to help the security team strengthen detection coverage and alerting.

NEW QUESTION: 21
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: (SHOW ANSWER)
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: 22
A U.S.-based online securities trading firm in New York is reviewing its transaction authentication process.
The security team confirms that each transaction is processed by first generating a hash of the transaction data. The hash value is then signed using the sender ' s private key. During verification, the recipient uses the corresponding public key to validate the signature before approving the transaction. The system documentation specifies that the same algorithm supports encryption, digital signatures, and key exchange mechanisms within the

organization ' s secure communications infrastructure. Which encryption algorithm is being used in this implementation?

A. ElGamal

B. Diffie-Hellman

C. DSA

D. RSA

Answer: D (LEAVE A REPLY)

The correct answer is RSA. CEH cryptography coverage describes RSA as a widely used asymmetric algorithm that supports encryption and digital signatures and is commonly deployed in public-key infrastructures. The question states that the transaction data is hashed, the hash is signed with the sender's private key, and the recipient verifies the signature with the matching public key. That is the classic RSA signature model presented in CEH materials. The additional clue is that the same algorithm is said to support encryption, digital signatures, and secure communications use cases. Diffie-Hellman is mainly a key exchange mechanism and is not used for digital signatures in the way described here. DSA is designed for digital signatures, but not for general encryption. ElGamal can support encryption and signatures, but CEH exam framing most strongly associates this full combination of encryption plus digital-signature verification with RSA. CEH references repeatedly emphasize RSA as the standard asymmetric cryptosystem for confidentiality, authentication, integrity, and nonrepudiation in enterprise communications. Because the described implementation combines hashing, private-key signing, and public-key verification within a broad asymmetric framework, RSA is the most accurate answer.

NEW QUESTION: 23

During a red team engagement for a client in the financial sector, ethical hacker Tyler Brooks conducts a phishing campaign using a crafted internal web page disguised as a company VPN login. After several users enter their credentials, Tyler confirms that the payload successfully recorded input without triggering antivirus or requiring local installation privileges. The captured keystrokes came exclusively from a web-based form embedded in the fake login page.

Based on the technique used, which type of keylogger did Tyler most likely deploy?

A. Keylogger Keyboard

B. Hypervisor-based Keylogger

C. Application Keylogger

D. JavaScript-based Keylogger

Answer: D (LEAVE A REPLY)

The scenario points to a JavaScript-based keylogger because the data capture occurs entirely within a web page and does not require installing software on the victim's machine. In CEH-aligned social engineering and web attack concepts, phishing pages commonly include client-side scripts that capture form inputs in real time. When a user types credentials into a fake login form, JavaScript event handlers can record keystrokes or the

final field values and transmit them to an attacker-controlled endpoint. This explains why Tyler's
"payload" works without local privilege, without dropping executables, and without triggering traditional antivirus focused on file-based malware. The key detail is that "captured keystrokes came exclusively from a web-based form embedded in the fake login page," which matches browser-based capture rather than OS- level logging.
The other options imply deeper system access than the prompt describes. A keyboard keylogger typically operates at the operating-system level by intercepting keyboard input system-wide, which usually requires running code on the host and is more likely to be detected by endpoint protections. A hypervisor-based keylogger is a highly advanced technique that relies on virtualization-layer control and is not consistent with a simple phishing web page. An application keylogger usually targets specific processes on the endpoint (such as browsers or email clients), again requiring execution on the local machine.
From a defensive viewpoint emphasized in CEH, mitigations include user awareness training to spot phishing pages, enforcing MFA to reduce the value of stolen credentials, using anti-phishing protections and URL filtering, monitoring for lookalike domains, and deploying browser and email security controls that detect credential-harvesting pages and suspicious form-post destinations.

NEW QUESTION: 24
In Boston, Massachusetts, network administrator Daniel Carter is monitoring the IT infrastructure of New England Insurance, a prominent firm, after receiving alerts about sluggish system performance. While reviewing traffic patterns, Daniel observes an unusual volume of concurrent requests overwhelming critical servers. To validate his suspicion of a session hijacking attempt, he begins capturing and reviewing live network traffic to identify unauthorized session behaviors before escalating to the security team.
What detection method should Daniel use to confirm the session hijacking attack in this scenario?
A. Use an intrusion detection system (IDS)
B. Check for predictable session tokens
C. Monitor for ACK storms
D. Perform manual packet analysis using packet sniffing tools
Answer: D (LEAVE A REPLY)
The scenario emphasizes that Daniel "begins capturing and reviewing live network traffic" to identify unauthorized session behaviors. In CEH-aligned network analysis practice, the most direct method to confirm session hijacking when you already have a packet capture is manual packet analysis using packet sniffing tools. By inspecting live traffic, Daniel can correlate sessions, verify whether multiple sources are reusing the same session identifiers, identify abnormal TCP sequence and acknowledgment behavior, and detect patterns such as duplicated cookies/tokens, replayed requests, inconsistent client IP or

user-agent shifts, or sudden session reuse across hosts. This approach provides evidentiary detail beyond an alert and allows validation before escalation.
An IDS can be helpful, but it is a detection system that generates alerts based on signatures or anomalies; it does not inherently "confirm" the issue unless it provides clear supporting evidence, and the question specifically frames Daniel's action as hands-on traffic review. Checking for predictable session tokens is a preventive and diagnostic step for weak session management design, but it does not directly confirm an in- progress hijacking event from observed network behavior. Monitoring for ACK storms can indicate certain TCP-level hijacking/desynchronization conditions, but it is narrower and may not apply to application-layer session hijacking, which is far more common in enterprise environments and would be validated by inspecting session identifiers and request flows in the capture.
Therefore, given the described workflow and the need to confirm unauthorized session activity from live traffic, CEH methodology aligns best with manual packet analysis using sniffing tools.

NEW QUESTION: 25
During a large-scale network assessment of a telecom provider in Dallas, Texas, a cybersecurity consultant uses Recon-ng and Nmap to enumerate legacy and infrastructure-level services across multiple nodes. The tools uncover open Telnet ports, FTP directories with anonymous login enabled, active TFTP services, and exposed SMB shares. The consultant also detects a service that responds to VRFY, EXPN, and RCPT commands, allowing the enumeration of user identities and delivery addresses due to weak input validation.
IPv6 tunneling protocols are also detected. Concerned about information leakage, the consultant flags these services for immediate remediation.
Which classification best describes this set of enumeration activities?
A. LDAP Enumeration
B. VoIP Enumeration
C. SMTP Enumeration
D. DNS Enumeration
Answer: (SHOW ANSWER)
SMTP enumeration is the correct classification because the scenario explicitly references the SMTP commands VRFY, EXPN, and RCPT, which are well-known techniques for discovering valid user accounts and email routing information on mail servers. In CEH-aligned enumeration methodology, attackers and testers use these commands to determine whether specific usernames or mailbox addresses exist. VRFY is used to verify a user, EXPN can expand a mailing list or alias into individual recipients, and RCPT TO is commonly tested during an SMTP conversation to see whether a recipient address is accepted or rejected.

When a server provides detailed responses, it can leak account validity and internal addressing formats, enabling targeted phishing, password spraying against known usernames, and broader social engineering campaigns.
Although the assessment also identifies Telnet, FTP with anonymous access, TFTP, and SMB shares, those findings represent additional exposed services and misconfigurations rather than the named enumeration classification in the answer choices. LDAP enumeration would focus on directory queries against services such as LDAP or Active Directory to extract users and groups. VoIP enumeration would involve SIP endpoints, extensions, and call infrastructure. DNS enumeration would center on zone transfers, record harvesting, and subdomain discovery. The distinguishing clue here is the use of VRFY, EXPN, and RCPT, which is uniquely tied to SMTP behavior and mail server user enumeration, making SMTP Enumeration the best fit.

NEW QUESTION: 26
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: 27
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: 28
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: A (LEAVE A REPLY)
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: 29
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: 30
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: (SHOW ANSWER)
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: 31
A sophisticated injection attack bypassed validation using obfuscation. What is the best future defense?
A. Continuous code review and penetration testing
B. Deploy WAF with evasion detection
C. SIEM monitoring
D. Enforce 2FA
Answer: (SHOW ANSWER)
CEH v13 emphasizes that advanced injection attacks often evade input validation through encoding and obfuscation. A Web Application Firewall (WAF) with evasion detection can analyze request patterns, payload behavior, and anomalies in real time.
Code reviews are important but reactive. SIEM correlates logs after attacks. 2FA does not prevent injection.
Thus, Option B provides the most effective immediate protection.

NEW QUESTION: 32
A financial institution's online banking platform is experiencing intermittent downtime caused by a sophisticated DDoS attack that combines SYN floods and HTTP GET floods from a distributed botnet.
Standard firewalls and load balancers cannot mitigate the attack without affecting legitimate users. To protect their infrastructure and maintain service availability, which advanced mitigation strategy should the institution implement?
A. Configure firewalls to block all incoming SYN and HTTP requests from external IPs
B. Increase server bandwidth and apply basic rate limiting on incoming traffic
C. Deploy an Intrusion Prevention System (IPS) with deep packet inspection capabilities
D. Utilize a cloud-based DDoS protection service that offers multi-layer traffic scrubbing and auto-scaling
Answer: (SHOW ANSWER)
Comprehensive Explanation from CEH v13 Courseware:
CEH v13 underscores that modern multi-vector DDoS attacks-particularly SYN floods combined with Layer

7 HTTP floods-cannot be effectively mitigated by traditional firewalls, IPS devices, or local traffic filters.
These systems become overwhelmed or risk blocking legitimate clients. CEH emphasizes the use of cloud- based DDoS mitigation platforms that provide traffic scrubbing, distributed filtering, rate shaping, and automatic scaling to absorb massive volumes of malicious traffic. Such services differentiate legitimate versus malicious traffic using global intelligence, behavioral analysis, and multi-layer protection strategies.
Increasing bandwidth or blocking broad traffic categories is ineffective and harmful to users. An IPS cannot scale to handle volumetric attacks. Only cloud scrubbing solutions (e.g., Cloudflare, Akamai, AWS Shield Advanced) meet CEH's recommended defenses for high-volume distributed attacks. These services ensure continuous availability and minimize collateral damage by filtering traffic upstream before it reaches the organization's infrastructure.

NEW QUESTION: 33
On July 25, 2025, during a security assessment at Apex Technologies in Boston, Massachusetts, ethical hacker Sophia Patel conducts a penetration test to evaluate the company's defenses against a simulated DDoS attack targeting their e-commerce platform. The simulated attack floods the platform with traffic from multiple sources, attempting to overwhelm server resources. The IT team activates a specific tool that successfully mitigates this attack by distributing traffic across multiple servers and filtering malicious requests. Sophia's test aims to verify the effectiveness of this tool in maintaining service availability.
Which DoS DDoS protection tool is most likely being utilized by the IT team in this scenario?
A. Web Application Firewall WAF
B. Load Balancer
C. Intrusion Prevention System IPS
D. Firewall
Answer: B (LEAVE A REPLY)
A load balancer is the best match because the key mitigation behavior described is distributing incoming traffic across multiple servers to prevent any single system from being overwhelmed. In CEH coverage of availability attacks, one of the most practical architectural defenses against flooding-based DoS and DDoS is to scale horizontally and place a load-balancing layer in front of a server pool. This allows the organization to absorb spikes by spreading connections and requests across multiple backend nodes, improving resilience and maintaining uptime.
The scenario also mentions filtering malicious requests. Modern load balancers commonly provide health checks, rate limiting, connection limiting, and integration with access control rules, and they are often deployed alongside DDoS scrubbing or edge protections. Even when the filtering logic is implemented through integrated security policies or upstream

services, the defining characteristic in the prompt is traffic distribution across multiple servers, which is a primary function of load balancing and a common CEH- referenced mitigation strategy for volumetric attacks.
A web application firewall focuses on inspecting and blocking malicious HTTP and application-layer payloads such as injection, request anomalies, and known attack patterns, but it is not primarily responsible for distributing traffic across multiple servers. An IPS can block suspicious patterns and exploit attempts, yet it does not typically provide the core traffic distribution function described. A traditional firewall enforces network-level rules and may help with rate limits, but it does not inherently balance traffic across a server farm. Therefore, the most likely tool in use here is a load balancer.

NEW QUESTION: 34
During a penetration test at Rocky Mountain Insurance in Denver, ethical hacker Sophia Nguyen attempts to evade detection by fragmenting malicious traffic into smaller packets. The IT security team counters her strategy with a system that monitors traffic for deviations from established baselines, flagging behavior that does not match normal network activity. This allows them to stop Sophia's evasion attempts in real time.
Which detection technique is the IT team most likely using in this case?
A. Deep Packet Inspection
B. Stateful Packet Inspection
C. Signature-Based Detection
D. Anomaly-Based Detection
Answer: (SHOW ANSWER)
The correct answer is D. Anomaly-Based Detection because the scenario explicitly states that the system
"monitors traffic for deviations from established baselines" and flags behavior that does not match normal network activity. In CEH-aligned IDS/IPS concepts, anomaly-based detection (also called behavior-based detection) works by building a profile of what "normal" looks like-such as typical packet rates, protocol usage, session patterns, timing, connection distributions, and expected traffic flows-and then identifying events that deviate significantly from those norms. This makes it particularly useful against evasion techniques and previously unseen patterns, because it is not limited to matching known signatures. Sophia's tactic-packet fragmentation-is a classic evasion approach intended to bypass simplistic inspection systems by splitting malicious payloads or attack patterns across multiple fragments so they are harder to reconstruct or match. A baseline-driven anomaly system can still detect the attack because fragmentation itself (or the resulting traffic characteristics) may appear abnormal: unusual fragment counts, unexpected fragment sizes, atypical reassembly behavior, irregular session characteristics, or protocol violations compared to normal traffic profiles. Because the detection is based on behavior rather than a fixed pattern, it can trigger alerts even if the exact malicious payload is not recognized.

Why the other options are less correct: Signature-based detection relies on known patterns and may be evaded when attackers modify payloads or fragment traffic to avoid matches. Stateful packet inspection tracks connection state and can help with session validation, but it is not inherently a baseline deviation detector.
Deep packet inspection inspects packet contents and can sometimes reassemble fragments depending on implementation, but the question's key clue is "deviations from established baselines," which directly points to anomaly-based detection.
Therefore, the IT team is most likely using anomaly-based detection.

NEW QUESTION: 35
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: 36
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: 37
A technology consulting firm in Portland, Oregon began experiencing repeated topology recalculations across its switching infrastructure. Shortly after a newly connected device came online in a conference room, spanning-tree convergence events were triggered across multiple distribution switches. Engineers determined that the access-layer interface connected to that device was influencing path-selection decisions, introducing a more favorable bridge priority value into the environment and affecting the established hierarchy. To preserve the intended switching structure and prevent unauthorized devices from altering root selection decisions, which control should be employed?

A. Configuring Loop Guard on non-designated ports
B. Activating UDLD (Unidirectional Link Detection) on uplinks
C. Applying Root Guard on designated interfaces
D. Enabling BPDU Guard on edge ports
Answer: (SHOW ANSWER)
The best answer is BPDU Guard on edge ports. CEH network defense material explains that BPDU Guard is used on access or edge ports where end-user devices are expected, not switches. If a device connected to such a port begins sending Bridge Protocol Data Units, the switch treats that as an abnormal condition and can shut the port down or place it in an error-disabled state. This prevents unauthorized or misconfigured devices from participating in spanning-tree and influencing root bridge election or topology decisions. That matches the scenario, where a newly connected device introduced a more favorable bridge priority and triggered spanning- tree recalculations. Root Guard is also related to protecting spanning-tree hierarchy, but it is typically applied where you want to prevent a downstream switch from becoming root while still allowing BPDU participation under controlled conditions. CEH exam framing usually expects BPDU Guard when the threat originates from an end-host-facing access port in a conference room or office edge location. Because the goal is to stop unauthorized edge-connected devices from affecting spanning-tree at all, enabling BPDU Guard on edge ports is the most appropriate control.

NEW QUESTION: 38
In the heart of Silicon Valley, California, network administrator Jake Henderson oversees the web infrastructure for TechTrend Innovations, a startup specializing in cloud solutions. During a routine architecture review, Jake evaluates the setup of their web server, which handles high-traffic API requests. He notes that the server's primary module processes incoming requests and works with additional modules to manage encryption, URL rewriting, and authentication. Curious about the server's design, Jake consults the documentation to ensure optimal performance and security.
Which web server component is Jake analyzing as part of TechTrend Innovations' architecture?
A. Virtual Document Tree
B. Application Server
C. Document Root
D. HTTP Server Core
Answer: D (LEAVE A REPLY)
The correct answer is HTTP Server Core because the scenario describes the primary module of a web server that processes incoming requests and coordinates with additional modules responsible for encryption, URL rewriting, and authentication. In CEH-aligned web server architecture concepts, the core HTTP engine is responsible for handling client requests, managing connections, parsing HTTP headers, and passing requests to the appropriate modules for further processing.

Modern web servers such as Apache HTTP Server or Nginx operate using a modular architecture. The core component manages the fundamental HTTP protocol operations, while optional or loadable modules extend functionality. For example, SSL or TLS modules handle encryption, rewrite modules manage URL manipulation, and authentication modules enforce access controls. The description in the question clearly aligns with this architecture, where a central processing unit works in conjunction with supporting modules. The other options do not fit. The Document Root refers only to the directory location from which web content is served. A Virtual Document Tree relates to how URLs are logically mapped to file paths. An Application Server is a separate server component that processes business logic, often interacting with backend systems, rather than directly managing HTTP request parsing at the core level.
Therefore, Jake is analyzing the HTTP Server Core, which is responsible for handling incoming requests and integrating modular security and performance features within the web server environment.

NEW QUESTION: 39
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: 40
You are Evelyn, an ethical hacker at LoneStar Health in Austin, Texas, engaged to investigate a recent compromise of archived patient records. During the investigation you recover a large set of encrypted records from a compromised backup and, separately, obtain several original template records (standard headers and form fields) that correspond to some entries in the encrypted set. You plan to use these paired examples (the original templates and their encrypted counterparts) to attempt to recover keys or deduce other plaintext values. Which cryptanalytic approach is most appropriate for this situation?

A. Chosen-ciphertext attack
B. Known-plaintext attack
C. Chosen-plaintext attack
D. Ciphertext-only attack
Answer: B (LEAVE A REPLY)
The correct answer is B. Known-plaintext attack because the scenario explicitly provides paired samples of plaintext and ciphertext for the same underlying data. In a known-plaintext attack, the analyst possesses one or more examples where the original message (plaintext) is known and the corresponding encrypted output (ciphertext) is also available. These pairs can be used to analyze the cipher's behavior, validate hypotheses about modes/parameters, and-depending on the algorithm, implementation weaknesses, and key management-attempt to recover the encryption key or decrypt other ciphertexts encrypted under the same key.
Here, Evelyn has "original template records (standard headers and form fields)" and their "encrypted counterparts" in the stolen backup set. Medical record formats commonly contain predictable structures (fixed headers, repeated field names, standardized forms), which increases the likelihood of having accurate known plaintext segments. With enough known plaintext/ciphertext pairs, an attacker may identify patterns caused by weak encryption choices, reused keys, reused IVs/nonces, insecure modes (e.g., ECB revealing structure), or flawed custom crypto. Even when strong algorithms are used, known-plaintext material can still be valuable for confirming the encryption scheme and detecting implementation errors.
Why the other options are not correct: Ciphertext-only assumes the attacker has only encrypted data and no plaintext examples-contradicted by the templates. Chosen-plaintext requires the ability to submit arbitrary plaintexts to an encryption oracle and receive ciphertexts, which the scenario does not indicate. Chosen- ciphertext requires the ability to submit ciphertexts to a decryption oracle and observe outputs, also not described.
Because Evelyn has real, matching plaintext-ciphertext pairs from the same dataset, the most appropriate cryptanalytic approach is a known-plaintext attack.

NEW QUESTION: 41
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: 42

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: 43
A zero-day vulnerability is actively exploited in a critical web server, but no vendor patch is available. What should be the FIRST step to manage this risk?
A. Shut down the server
B. Apply a virtual patch using a WAF
C. Perform regular backups and prepare IR plans
D. Monitor for suspicious activity
Answer: B (LEAVE A REPLY)
According to CEH v13 Security Operations and Incident Response, zero-day vulnerabilities pose one of the highest operational risks because exploits exist before official remediation is available. When active exploitation is observed and no vendor patch exists, immediate compensating controls must be deployed.
The first and most effective action is implementing virtual patching, typically through a Web Application Firewall (WAF) or Intrusion Prevention System (IPS). CEH v13 defines virtual patching as a security measure that blocks exploitation attempts at the network or application layer without modifying the vulnerable software. This approach allows organizations to maintain service availability while reducing exposure.
Shutting down the server (Option A) may prevent exploitation but introduces unacceptable business disruption and is not recommended as a first response. Backups and incident response planning (Option C) are critical but do not actively prevent exploitation. Passive monitoring (Option D) allows attackers to continue exploiting the vulnerability unchecked.
CEH v13 emphasizes that virtual patching is the preferred first response for zero-day threats, especially when systems are mission-critical. It provides immediate risk reduction while allowing time for vendor patch development and controlled deployment.

NEW QUESTION: 44
Maria is conducting passive reconnaissance on a competitor without interacting with their systems. Which method would be least appropriate and potentially risky?
A. Using the Wayback Machine
B. Running an intensive port scan on public IPs
C. Reviewing forums and social media
D. Examining patent databases and public records
Answer: B (LEAVE A REPLY)
CEH v13 defines passive reconnaissance as information gathering without directly interacting with the target's systems. Activities such as reviewing archived websites, social media, forums, and public records are all passive and legal.

Running an intensive port scan, however, is an active reconnaissance technique. According to CEH v13, port scanning directly interacts with target systems and can trigger IDS/IPS alerts, logs, and even legal consequences if done without authorization. Therefore, option B violates the principles of passive reconnaissance and is the riskiest choice.

NEW QUESTION: 45
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: B (LEAVE A REPLY)
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: 46
While testing a web application that relies on JavaScript-based client-side security controls, which method is most effective for bypassing these controls without triggering server-side alerts?
A. Reverse-engineering the proprietary encryption algorithm
B. Disabling JavaScript in the browser and submitting invalid data
C. Injecting malicious JavaScript into the login page
D. Using a proxy tool to intercept and modify client-side requests
Answer: (SHOW ANSWER)
The Certified Ethical Hacker (CEH) Web Application Security module emphasizes that client-side controls cannot be trusted.
Disabling JavaScript allows attackers to bypass:
* Password complexity enforcement
* CAPTCHA validation
* Input validation logic
Option B is the simplest and most effective CEH-approved method.
Option A is unnecessary and noisy.
Option C risks detection.
Option D is effective but more complex and detectable.
CEH explicitly teaches testers to disable JavaScript to evaluate server-side enforcement.

NEW QUESTION: 47
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: 48
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: 49
You are working as a threat intelligence analyst for a fintech startup that recently discovered a spike in credential stuffing attempts against its admin panel. The security team believes this may be due to leaked internal files circulating on underground forums. You are tasked with investigating potential exposure on the dark web without directly interacting with any service or forum. You decide to use advanced search filters to identify documents hosted on hidden services that may contain sensitive access details. The team suspects these documents might include account-related keywords in their titles.
Which of the following search queries would best support this investigation?
A. filetype:pdf intitle: " admin access " site:onion
B. filetype:docx intitle: " login credentials "
C. filetype:pdf intitle: " secure login " site:onion
D. filetype:docx intitle: " user accounts " site:onion
Answer: A (LEAVE A REPLY)
This task describes passive reconnaissance using advanced search operators, a technique covered in CEH as search engine reconnaissance or Google dorking. The objective is to find potentially exposed documents on hidden services while avoiding direct interaction with forums or services. The most important element in the query is restricting results to hidden service domains using the site:onion operator. Any option that does not include site:onion is less suitable because it will return results from the public web rather than from .onion resources.
Option A is the strongest fit because it combines three high-value filters: filetype:pdf to focus on document artifacts that are commonly leaked or shared, intitle: " admin access " to target titles suggesting privileged access or administrative information, and site:onion to restrict the scope to hidden services. In CEH reporting and threat intelligence workflows, targeting high-signal keywords such as admin access, credentials, password list, or vpn access in document metadata is a practical way to identify likely leak sources without active engagement.
Option B lacks site:onion, so it fails the hidden-service requirement. Option C includes site:onion but the phrase secure login is more generic and may return many benign pages, reducing precision. Option D includes site:onion and filetype targeting, but user accounts is broader and less indicative of immediate access data than admin access. Therefore, A

best supports efficient passive discovery of high-risk documents relevant to credential exposure on hidden services.

NEW QUESTION: 50
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: (SHOW ANSWER)
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: 51
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: (SHOW ANSWER)
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: 52
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: 53
A penetration tester is tasked with mapping an organization's network while avoiding detection by sophisticated intrusion detection systems (IDS). The organization employs advanced IDS capable of recognizing common scanning patterns. Which scanning technique should the tester use to effectively discover live hosts and open ports without triggering the IDS?
A. Execute a FIN scan by sending TCP packets with the FIN flag set
B. Use an Idle scan leveraging a third-party zombie host
C. Conduct a TCP Connect scan using randomized port sequences
D. Perform an ICMP Echo scan to ping all network devices
Answer: B (LEAVE A REPLY)
CEH v13 highlights the Idle Scan as one of the stealthiest reconnaissance methods available, designed specifically to avoid detection by IDS and security monitoring tools. Idle scanning leverages a "zombie host"
-a system with a predictable IPID sequence-to route all probe packets through it. Since no packets ever originate directly from the attacker's IP, IDS systems are unable to attribute the port scan to the attacker. CEH emphasizes that this technique creates zero direct traffic between the attacker and the target, making it extremely evasive and ideal for highly

monitored networks. FIN scans (Option A) are somewhat stealthy but still originate from the attacker and are detectable. TCP Connect scans (Option C) are the most detectable because they complete full connections. ICMP Echo scans (Option D) are easily logged and flagged by IDS.
Idle scanning is uniquely suited for bypassing advanced detection systems while still identifying open ports and live hosts.

NEW QUESTION: 54
Which attack best demonstrates covert eavesdropping via smartphone sensors?
A. Malicious APK exploitation
B. Man-in-the-Disk attack
C. Spearphone attack
D. Tap 'n Ghost attack
Answer: C (LEAVE A REPLY)
The Spearphone attack, covered in CEH v13 Mobile Platform Hacking, exploits smartphone accelerometers to infer speech vibrations from loudspeakers-without microphone permissions.
This attack demonstrates how built-in sensors can be abused for covert surveillance, making it ideal for assessing privacy risks.
Other options involve different attack vectors not related to sensor-based eavesdropping.
Thus, Option C is correct.

NEW QUESTION: 55
A multinational corporation deploys a major internal tool built on a PowerShell-based automation framework.
Shortly after a scheduled rollout, the IT team notices intermittent system slowdowns and unexplained bandwidth spikes. Despite running updated endpoint protection and restrictive firewall rules, traditional scanning tools report no malicious files on disk. However, internal telemetry flags a trusted process repeatedly executing obfuscated PowerShell commands in memory. The anomalous activity vanishes upon reboot and appears to leave no footprint behind on the system.
Which type of malware is most likely responsible for this behavior?
A. Worm
B. Trojan
C. Rootkit
D. Fileless Malware
Answer: D (LEAVE A REPLY)
Fileless malware is the best match because the scenario highlights memory-resident execution with no malicious files written to disk and activity that disappears after a reboot.
In CEH-aligned malware concepts, fileless attacks commonly leverage legitimate system tools and trusted processes, often called living off the land, to execute malicious logic

without dropping traditional executables. PowerShell is one of the most frequently abused components for this purpose because it can download, decode, and run scripts directly in memory, including obfuscated commands that evade simple signature-based scans. The prompt explicitly states that endpoint scanners find no malicious files on disk, yet telemetry detects a trusted process executing obfuscated PowerShell commands in memory. That combination strongly indicates fileless behavior.
The fact that the anomaly vanishes on reboot also fits fileless techniques that rely on volatile memory artifacts rather than persistent file-based implants. While fileless attacks can establish persistence through registry run keys, scheduled tasks, WMI, or other mechanisms, the question emphasizes no footprint and reboot clearing the activity, which is consistent with a purely in-memory foothold or a short-lived execution chain.
A worm is characterized by self-replication across systems, which is not described. A trojan usually involves a malicious file disguised as legitimate software, conflicting with the "no files on disk" observation. A rootkit focuses on stealth and hiding by modifying system internals and can persist, but the scenario's defining indicators are PowerShell in-memory execution and lack of disk artifacts, which aligns most directly with fileless malware.

NEW QUESTION: 56
While reviewing exposed infrastructure for a logistics company in Denver, Joe, a security analyst, identifies that one host is synchronizing time using UDP port 123. Probing further, he issues queries to extract details about peers, offsets, and delays. This allows him to gather internal hostnames and client IP addresses connected to the time server. Such information leakage could provide insight into the company ' s internal network structure. Which technique was most likely used to obtain this information?
A. DNS Zone Transfer Enumeration
B. NTP Enumeration
C. VoIP Enumeration
D. NetBIOS Enumeration
Answer: B (LEAVE A REPLY)
The correct answer is B. NTP Enumeration because the indicators and the data obtained match enumeration of the Network Time Protocol (NTP) service, which commonly runs on UDP port 123. In CEH-aligned reconnaissance and enumeration concepts, attackers often enumerate exposed services to learn configuration and internal details that can assist with follow-on attacks. When NTP is reachable from untrusted networks and is misconfigured (or supports certain query modes), it can leak information about the time server's peers, synchronization status, and operational metrics such as offset and delay-exactly the attributes described in the scenario.
The prompt also notes that Joe can gather internal hostnames and client IP addresses connected to the time server. This aligns with how NTP can reveal associated systems and relationships: time servers often have multiple internal clients, upstream peers, or configured associations. Queries that expose peer/association information can

unintentionally disclose internal naming conventions, IP address ranges, and network structure-valuable intelligence for an attacker conducting mapping and target selection. In addition, time infrastructure is frequently centralized, so enumerating it can provide a hub-like view of the environment.
Why the other options are incorrect: DNS zone transfer enumeration is associated with DNS AXFR and typically yields DNS records such as subdomains and MX/CNAME entries-not NTP peers/offsets/delays and not UDP 123. VoIP enumeration targets telephony protocols and services (e.g., SIP) on different ports and would not center on time synchronization metrics. NetBIOS enumeration involves ports 137-139 and returns NetBIOS name and session information, not NTP operational data.
Therefore, the technique used to obtain peer, offset, delay, and connected client details from a UDP/123 time server is NTP enumeration.

NEW QUESTION: 57
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: 58
At a private aerospace research facility in Mesa, Arizona, an executive raises concerns after sensitive discussion points from speakerphone meetings begin surfacing externally. The device shows no indicators of active audio recording, and application permission history does not reflect recent camera or microphone authorization changes. A forensic mobile analysis identifies that an installed application has been continuously reading motion sensor output while the phone ' s loudspeaker is active. The collected sensor data was later transmitted to a remote server, where acoustic characteristics were reconstructed from the recorded measurements. Identify the attack technique responsible for this compromise.
A. Spearphone Attack
B. Storm Breaker Abuse
C. Android Camera Hijack Attack
D. Camfecting
Answer: (SHOW ANSWER)
The correct answer is Spearphone Attack. CEH mobile platform coverage describes Spearphone as a side- channel attack in which motion sensors, such as accelerometers or gyroscopes, are abused to infer or reconstruct audio from vibrations produced by a phone's loudspeaker. A key feature of this technique is that it may not require direct microphone access, which helps explain why no microphone permission changes or visible recording indicators appeared on the device. That detail is central to the scenario. The installed app continuously collected motion sensor data while speakerphone conversations occurred, and the information was later analyzed remotely to reconstruct acoustic content. That behavior is a textbook match for Spearphone. Android camera hijack attacks involve camera access, not speaker vibration analysis. Camfecting refers to webcam compromise, and Storm Breaker Abuse does not describe this sensor-based audio inference method. CEH materials use this example to show that seemingly low-risk sensors can still create serious privacy and espionage threats when correlated with physical effects such as sound-induced vibration. Because the attack depends on speaker-generated motion data rather than direct audio recording, Spearphone is the best answer.

NEW QUESTION: 59
During an internal red team engagement, an operator discovers that TCP port 389 is open on a target system identified as a domain controller. To assess the extent of LDAP exposure, the operator runs the command ldapsearch -h < Target IP > -x -s base namingcontexts and receives a response revealing the base distinguished name (DN): DC=internal,DC=corp. This naming context indicates the root of the LDAP directory structure. With this discovery, the operator plans the next step to continue LDAP enumeration and expand visibility into users and objects in the domain. What is the most logical next action?
A. Launch a brute-force attack against user passwords via SMB
B. Conduct an ARP scan on the local subnet
C. Attempt an RDP login to the domain controller
D. Use the base DN in a filter to enumerate directory objects
Answer: D (LEAVE A REPLY)
Once the base DN is identified through LDAP namingContexts, CEH teaches that the next step in enumeration is to query the directory tree using this DN. This allows retrieval of users, groups, computers, and other AD objects. LDAP-based enumeration requires valid search filters rooted in the base DN.

NEW QUESTION: 60
Which social engineering attack involves impersonating a co-worker or authority figure to extract confidential information?
A. Phishing
B. Pretexting
C. Quid pro quo
D. Baiting
Answer: (SHOW ANSWER)
Pretexting is defined in CEH v13 Social Engineering as an attack where the attacker fabricates a believable scenario and impersonates a trusted individual to gain sensitive information.
This differs from phishing (mass messaging), baiting (malicious incentives), and quid pro quo (exchange of favors).

NEW QUESTION: 61
A penetration tester finds malware that spreads across a network without user interaction, replicating itself from one machine to another. What type of malware is this?
A. Keylogger
B. Ransomware
C. Virus
D. Worm
Answer: D (LEAVE A REPLY)

Comprehensive Explanation from CEH v13 Courseware:
CEH v13 describes worms as standalone malicious programs capable of self-replication without requiring user assistance. Unlike viruses, which need a host file and are triggered typically by user actions, worms propagate autonomously by scanning networks, exploiting vulnerabilities, or copying themselves to accessible machines. Worms are known for causing rapid, widespread damage by consuming bandwidth, degrading system performance, and creating backdoors for attackers. Classic examples such as Conficker, WannaCry, and SQL Slammer reinforce the destructive potential of automated propagation. CEH stresses that worms often use network shares, open ports, or unpatched vulnerabilities to move laterally. In contrast, keyloggers harvest keystrokes, ransomware encrypts data and demands payment, and viruses require user involvement to spread. The behavior in the scenario-automatic replication across the network-is the defining characteristic of worm activity according to CEH's malware taxonomy.

NEW QUESTION: 62
A penetration tester needs to identify open ports and services on a target network without triggering the organization's intrusion detection systems, which are configured to detect high-volume traffic and common scanning techniques. To achieve stealth, the tester decides to use a method that spreads out the scan over an extended period. Which scanning technique should the tester employ to minimize the risk of detection?
A. Use a stealth scan by adjusting the scan timing options to be slow and random
B. Perform a TCP SYN scan using a fast scan rate
C. Execute a UDP scan targeting all ports simultaneously
D. Conduct a TCP Xmas scan sending packets with all flags set
Answer: A (LEAVE A REPLY)
The CEH v13 content explains that stealth scanning involves modifying scan timing parameters to reduce packet frequency, randomize intervals, and avoid recognizable patterns typically flagged by intrusion detection systems. Slow, randomized timing-often achieved with Nmap's T0 or T1 timing templates- prevents bursts of traffic and allows scans to blend into normal network noise. IDS/IPS systems tuned for high-volume events may fail to detect such gradual reconnaissance. Fast SYN scans generate distinctive patterns easily identified by security monitoring tools. UDP scans, especially across all

ports, produce high traffic volume and are extremely noisy. Xmas scans, although sometimes used for stealth against stateless filters, are still signature-detectable and inappropriate when stealth over time is required. Therefore, applying slow, randomized timing options aligns with CEH-approved reconnaissance techniques for evading detection while enumerating open ports.

NEW QUESTION: 63
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: A (LEAVE A REPLY)
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: 64
During a quarterly security audit at a financial services company in Charlotte, North Carolina, you are tasked with reviewing exposed services on legacy servers inherited from a third-party vendor. While scanning, you discover that TCP port 1434 is open on a database node that is not listed in the company ' s active inventory.
The IT team has no records explaining why this service is running, and you are asked to determine whether the exposure of this port could indicate an unnecessary database-related risk. Based on standardized port assignments, which service is most likely running on this port and requires further review?
A. ms-sql-m
B. sqlsrv
C. sql*net
D. ms-sql-s
Answer: A (LEAVE A REPLY)
The correct answer is A. ms-sql-m because TCP/1434 is commonly associated with Microsoft SQL Server Monitor / SQL Server Browser-related services, which are used to help clients discover SQL Server instances and their connection details. In standardized service naming, ms-sql-m corresponds to Microsoft SQL
"monitor" functionality tied to instance discovery and related metadata exposure. When this port is reachable from networks where it is not needed, it can increase attack surface by

exposing information that helps attackers identify database instances, target the correct ports, and focus exploitation attempts.
In the context of a legacy server that is "not listed in the company's active inventory," an open 1434 is a red flag because it suggests an unnecessary or unmanaged database discovery component may be running.
Attackers often use exposed database-related ports for reconnaissance (identifying instance names, versions, and listening endpoints) and then pivot to authentication attacks or exploitation of known weaknesses. Even when the core SQL service port is controlled, discovery services can still leak useful environment details that lower the cost of an attack.
Why the other options are incorrect:
ms-sql-s typically refers to the primary Microsoft SQL Server service, most commonly associated with TCP
/1433 (the default SQL Server port), not 1434.
sql*net is associated with Oracle SQL*Net/Net8 traffic, typically using Oracle listener ports such as 1521, not
1434.
sqlsrv is not the standardized assignment for 1434 in the way ms-sql-m/ms-sql-s are used for Microsoft SQL- related services.
Therefore, based on standardized port associations and the database discovery/monitoring role of this service, the exposure most likely indicates ms-sql-m on TCP/1434, and it warrants further review and potential restriction if not required.

NEW QUESTION: 65
While analyzing logs, you observe a large number of TCP SYN packets sent to various ports with no corresponding ACKs. What scanning technique was likely used?
A. SYN scan (half-open scanning)
B. XMAS scan
C. SYN/ACK scan
D. TCP Connect scan
Answer: A (LEAVE A REPLY)
This activity clearly indicates a TCP SYN scan, also known as a half-open scan, which is a commonly used stealth scanning technique discussed in CEH v13 Reconnaissance and Network Scanning. In a SYN scan, the attacker sends TCP SYN packets to target ports and observes the responses without completing the TCP three- way handshake.
If the port is open, the target responds with a SYN/ACK packet. The scanner then immediately sends a RST packet instead of the final ACK, leaving the connection half-open. This behavior allows attackers to identify open ports while minimizing log entries and reducing detection by security monitoring tools.
The absence of ACK packets in logs supports this explanation, as the handshake is never completed.
Other options are incorrect because:

XMAS scans send packets with multiple flags set.
SYN/ACK scans are primarily used for firewall rule discovery.
TCP Connect scans complete the full handshake and generate ACKs.
CEH v13 emphasizes that SYN scans are widely used because they balance accuracy and stealth, making them a preferred reconnaissance method for attackers.

NEW QUESTION: 66
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: 67
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: (SHOW ANSWER)
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: 68
A penetration tester is running a vulnerability scan on a company's network. The scan identifies an open port with a high-severity vulnerability linked to outdated software. What is the most appropriate next step for the tester?
A. Execute a denial-of-service (DoS) attack on the open port
B. Perform a brute-force attack on the service running on the open port
C. Research the vulnerability and determine if it has a publicly available exploit
D. Ignore the vulnerability and focus on finding more vulnerabilities
Answer: C (LEAVE A REPLY)
CEH v13 outlines a structured approach to vulnerability assessment and exploitation. After identifying a high- severity vulnerability, the next critical step is verification and research, not immediate exploitation. This ensures accuracy, reduces false positives, and avoids unnecessary risk. CEH emphasizes that testers must validate vulnerability details, confirm version applicability, assess exploit availability (e.g., Metasploit, Exploit-DB), and evaluate potential impact. Attempting DoS attacks (Option A) is prohibited unless explicitly scoped

and does not align with responsible testing. Brute-force attacks (Option B) are unrelated to software version vulnerabilities. Ignoring the issue (Option D) violates CEH methodology. The correct process is to research and verify-ensuring exploitation is safe, relevant, and authorized. This aligns with CEH's vulnerability management lifecycle: discovery # verification # prioritization # exploitation (when allowed) # reporting.

NEW QUESTION: 69
A future-focused security audit discusses risks where attackers collect encrypted data now, anticipating that they can decrypt it later with quantum computers. What is this threat known as?
A. Saving data today for future quantum decryption
B. Replaying intercepted quantum messages
C. Breaking RSA using quantum algorithms
D. Flipping qubit values to corrupt the output
Answer: (SHOW ANSWER)
In CEH v13 Cryptography, this threat is formally referred to as "Harvest Now, Decrypt Later" (HNDL). It describes a long-term cryptographic risk where adversaries intercept and store encrypted communications today, even though they cannot decrypt them with current computational capabilities. The expectation is that future quantum computers will be powerful enough to break widely used public-key cryptographic algorithms.
CEH v13 emphasizes that quantum algorithms such as Shor's Algorithm can theoretically break RSA, DSA, and ECC by efficiently solving integer factorization and discrete logarithm problems. However, the defining feature of this threat is not the act of breaking encryption itself, but rather the strategic collection and storage of encrypted data in advance.
Option C is incomplete because it focuses only on the cryptographic mechanism rather than the threat model.
Options B and D are unrelated to the scenario described and refer to quantum communication integrity issues, not long-term cryptographic exposure.
CEH v13 highlights that sensitive data with long confidentiality lifetimes-such as government records, financial data, healthcare information, and intellectual property-is especially vulnerable to this threat. As a result, organizations are encouraged to adopt quantum-resistant (post-quantum) cryptographic algorithms proactively.
Thus, Option A accurately describes the threat model and aligns with CEH v13's treatment of future cryptographic risks.

NEW QUESTION: 70
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: (SHOW ANSWER)

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: 71

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: 72
During a penetration test at Triangle FinTech in Raleigh, North Carolina, ethical hacker Ethan attempts to bypass the company ' s perimeter firewall. Instead of sending obvious malicious payloads, he encapsulates his traffic inside standard web requests on port 80, blending in with normal browsing activity. This method allows his packets to slip past perimeter defenses that are not performing deep application inspection.
Which firewall evasion technique is Ethan most likely using?
A. HTTP Tunneling
B. Source Routing
C. Tiny Fragments
D. DNS Tunneling
Answer: A (LEAVE A REPLY)
The described technique is HTTP tunneling because Ethan is encapsulating his traffic inside standard web requests on port 80 to blend with normal browsing activity and bypass perimeter defenses that only perform basic port/protocol filtering. HTTP tunneling leverages the fact that many organizations allow outbound (and sometimes inbound) HTTP/HTTPS traffic through firewalls for business needs. If a firewall is not doing deep inspection (such as application-layer proxying, WAF inspection, or strict egress controls), encapsulated traffic can traverse allowed ports while carrying non-HTTP payloads inside the HTTP structure.
The scenario's core clues are: (1) "encapsulates his traffic inside standard web requests," (2) uses port 80, and (3) success depends on the firewall "not performing deep application inspection." These are exactly the conditions where HTTP tunneling is effective: the traffic appears as ordinary HTTP sessions, so the firewall treats it as permitted web traffic even though the content is being used as a carrier for another protocol or command channel.
Why the other options don't fit:
DNS tunneling (D) also encapsulates traffic, but it uses DNS queries/responses (typically UDP/TCP 53), not HTTP requests on port 80.
Tiny fragments (C) is an evasion method that breaks packets into very small fragments to confuse filtering
/IDS reassembly; the scenario is about encapsulation in web requests, not fragmentation.
Source routing (B) attempts to influence packet path using IP options; it is not described here and is commonly blocked/ignored in modern networks.
Therefore, the firewall evasion technique is A. HTTP Tunneling.

NEW QUESTION: 73

A regional e-commerce company in Dallas, Texas operates an Apache-based web server to manage product catalogs and promotional campaigns. During an authorized assessment, a security consultant analyzes how the platform processes a referral parameter embedded in product-sharing links. While reviewing responses through an intercepting proxy, he observes that values supplied in the referral parameter are incorporated into metadata returned to the browser. By introducing carefully crafted delimiter characters into the parameter, he notices that the structure of the server's outbound response changes in an unexpected manner. Further testing shows that the manipulated input causes the server to generate multiple logically distinct response segments within what should have been a single transaction. When the crafted link is accessed through a standard browser, the client interprets the injected portion as a separate directive, resulting in redirection behavior influenced by the attacker-controlled input. Identify the web server attack technique being demonstrated in this scenario.

A. Web Cache Poisoning Attack

B. Directory Traversal Attack

C. HTTP Response-Splitting Attack

D. Frontjacking Attack

Answer: C (LEAVE A REPLY)

The correct answer is HTTP Response-Splitting Attack. CEH web server coverage explains that HTTP response splitting occurs when attacker-controlled input is inserted into HTTP headers or response metadata in a way that allows the server to split one intended response into two separate responses or response segments. The question specifically describes crafted delimiter characters changing the structure of the outbound response and causing the browser to interpret the injected content as a separate directive, including attacker-influenced redirection. That is the classic behavior of response splitting. Directory traversal would involve unauthorized path navigation to restricted files or directories. Web cache poisoning focuses on corrupting cached responses so later users receive malicious or altered content, which is related conceptually but not the direct mechanism described here. CEH materials present HTTP response splitting as a means to an end, often used to trigger redirect behavior or facilitate secondary attacks by controlling the second response or header content. Because the attacker manipulates server output into multiple response components within a single transaction, HTTP Response-Splitting is the most precise answer.

NEW QUESTION: 74

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: (SHOW ANSWER)
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: 75
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: 76
Which encryption method supports secure key distribution?
A. Disk encryption
B. Symmetric encryption
C. Hash functions
D. Asymmetric encryption
Answer: (SHOW ANSWER)
Asymmetric encryption, as defined in CEH v13 Cryptography, uses a public-private key pair, solving the key distribution problem inherent in symmetric encryption.
Public keys can be freely shared, enabling secure communication initiation without prior shared secrets. Disk encryption and hashes do not address key exchange.

Therefore, Option D is correct.

NEW QUESTION: 77
While auditing legacy network devices at a public hospital in Miami, Jason, a penetration tester, needs to verify what SNMP traffic is leaking across the internal segment. Instead of running structured queries, he decides to capture live network traffic and manually review the protocol fields. This method allows him to see SNMP requests and responses in transit but requires manual parsing of OIDs, community strings, and variable bindings.
Which method should Jason use in this situation?
A. Nmap
B. Wireshark
C. SnmpWalk
D. SoftPerfect Network Scanner
Answer: B (LEAVE A REPLY)
Jason's goal is to capture live SNMP traffic on the wire and manually inspect protocol fields such as community strings, OIDs, and variable bindings within requests and responses. The method described is packet capture and protocol dissection, which is exactly what Wireshark is designed for. Wireshark can capture traffic from an interface (or from a mirrored/SPAN port) and decode SNMP at the protocol level, presenting SNMP PDUs in a human-readable structure. This enables an assessor to view SNMP GET /GETNEXT/GETBULK requests, SET operations (if present), and responses, including the transmitted identifiers and values-useful for verifying whether sensitive SNMP data is exposed in transit.
The scenario explicitly states Jason is not running structured queries and instead wants to observe "SNMP requests and responses in transit," which rules out tools that actively query devices. SnmpWalk (C) is an active enumeration tool that queries SNMP agents using a community string and walks a subtree of the MIB; that is the opposite of passive traffic inspection. Nmap (A) can scan ports and perform some SNMP-related scripts, but it still operates as an active probing tool rather than a live traffic capture and manual field review platform. SoftPerfect Network Scanner (D) is a network discovery tool for identifying hosts and services; it is not a packet-level sniffer intended for dissecting SNMP messages on the wire.

Additionally, the mention of "manual parsing" is consistent with packet analysis workflows: even though Wireshark decodes SNMP, the analyst still needs to interpret what OIDs and values mean, correlate requests to responses, and assess sensitivity (e.g., community strings in SNMPv1/v2c are not encrypted, and captured traffic may reveal them).
Therefore, the correct method is B. Wireshark.

NEW QUESTION: 78
In the crisp mountain air of Denver, Colorado, ethical hacker Lila Chen investigates the security framework of MedVault, a US-based healthcare platform used by regional clinics to manage patient data. During her assessment, Lila manipulates session parameters while navigating the patient portal's dashboard. Her tests reveal a critical flaw: the system allows users to access sensitive medical records not associated with their own account, enabling unauthorized changes to private health data. Upon deeper inspection, Lila determines that the issue stems from the application allowing users to perform actions beyond their assigned roles rather than failures in encryption, unsafe object handling, or server configuration.
Which OWASP Top 10 2021 vulnerability is Lila most likely exploiting in MedVault's web application?
A. Security Misconfiguration
B. Insecure Deserialization
C. Cryptographic Failures
D. Broken Access Control
Answer: D (LEAVE A REPLY)
Broken Access Control is the correct choice because the scenario describes a user being able to access and modify resources that should be restricted to other users or roles. In CEH-aligned web testing, access control flaws occur when an application fails to enforce authorization checks consistently on the server side.
Manipulating session parameters and then retrieving "sensitive medical records not associated with their own account" is a classic indicator of an authorization bypass, often seen as insecure direct object references, parameter tampering, or horizontal and vertical privilege escalation. Horizontal escalation is when one user accesses another user's data at the same privilege level, while vertical escalation is when a user performs actions reserved for higher-privileged roles. The prompt explicitly states users can perform actions beyond assigned roles, which is the definition of broken authorization enforcement.
The other options do not align with the described root cause. Cryptographic Failures focuses on weak or missing encryption and does not explain why authenticated users can reach unauthorized records. Insecure Deserialization involves unsafe deserialization leading to remote code execution or data tampering via serialized objects, which is not indicated here. Security Misconfiguration is broader and can contribute to exposure, but the scenario emphasizes role and resource permission bypass rather than mis-set server headers, default accounts, or exposed admin interfaces.

Mitigation in CEH best practices includes enforcing server-side authorization on every request, using deny-by- default policies, validating that the authenticated user is allowed to access the specific record identifier, implementing robust role-based access control, logging access denials, and adding automated tests to prevent IDOR and privilege escalation regressions.

NEW QUESTION: 79
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: D (LEAVE A REPLY)
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: 80
At Apex Financial Services in Houston, Texas, ethical hacker Javier Ruiz evaluates mobile security practices under the company ' s BYOD policy. He demonstrates that employees often install applications that request access to contact lists, cameras, and messaging services, even though these functions are unrelated to the apps
' intended purpose. This behavior allows a malicious program to harvest sensitive corporate information.
Which security guideline would most directly prevent this issue?
A. Use encryption mechanisms to store data
B. Enforce automatic device locking or implement biometric authentication
C. Review permissions requested by apps before installing them
D. Set passwords for apps to restrict others from accessing them
Answer: (SHOW ANSWER)
The issue described is excessive or inappropriate application permission granting in a BYOD environment.

Employees install apps that request access to sensitive device resources-contacts, camera, messaging- despite those permissions not being necessary for the app's stated purpose. This creates a risk of data harvesting and corporate information leakage if a malicious or overly intrusive app is installed. The most direct guideline to prevent this behavior is to review the permissions requested by apps before installing them.
Mobile operating systems rely heavily on permission models to control access to sensitive data and device capabilities. When users approve broad permissions without scrutiny, they effectively authorize the app to collect and transmit sensitive information. Enforcing a culture and policy of checking permissions (and denying or uninstalling apps that request unnecessary access) directly addresses the root cause in the scenario:
user consent enabling excessive privilege at the app level. In a corporate BYOD program, this guideline is often paired with mobile security controls such as enterprise app stores, allowlists/denylists, MDM/MAM policies, and user awareness training, but the question asks for the most direct preventive guideline.
Why the other options are less direct:
Encryption at rest (A) helps protect stored data if the device is lost or compromised, but it does not stop an authorized app from accessing data via granted permissions.
Automatic locking/biometrics (B) reduces unauthorized physical access, but it does not constrain what a permitted app can access while the device is in use.
App passwords (D) can help restrict casual access to an app, but they do not solve the problem of an app legitimately being granted invasive permissions.
Therefore, the best answer is C. Review permissions requested by apps before installing them.

NEW QUESTION: 81
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: (SHOW ANSWER)
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: 82
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: 83
An attacker places a malicious VM on the same physical server as a target VM in a multi-tenant cloud environment. The attacker then extracts cryptographic keys using CPU timing analysis. What type of attack was conducted?
A. Side-channel attack
B. Cloud cryptojacking
C. Cache poisoned denial of service (CPDoS)
D. Metadata spoofing
Answer: A (LEAVE A REPLY)
CEH cloud modules explain that side-channel attacks exploit indirect information leakage based on hardware characteristics-such as CPU timing, power usage, cache access patterns, or electromagnetic emissions. In virtualized cloud environments, multiple tenants share the same physical hardware, creating opportunities for attackers to extract sensitive data from neighboring virtual machines. By placing a malicious VM on the same host as the victim, an attacker can measure minute differences in timing during cryptographic

operations, allowing them to infer private keys or sensitive computations. This aligns precisely with CEH's definition of a side-channel attack. Cryptojacking involves unauthorized cryptocurrency mining, CPDoS targets caching layers rather than key extraction, and metadata spoofing manipulates cloud metadata endpoints. Only side-channel analysis matches the described attack behavior.

NEW QUESTION: 84
During an external assessment of a regional retail company ' s digital infrastructure, security analyst Joe is assigned to map internal services without active intrusion. While testing the behavior of a publicly exposed resolution system, he discovers that a secondary system responds unusually to structured queries. When he issues a specific request format, the server replies with a full list of internal mappings, including subdomains, mail hosts, and system aliases without requiring credentials or triggering alerts.
Which technique was most likely used to obtain this information?
A. LDAP Enumeration
B. NTP Enumeration
C. DNS Zone Transfer Enumeration
D. NetBIOS Enumeration
Answer: C (LEAVE A REPLY)
The described behavior matches DNS Zone Transfer Enumeration. In CEH reconnaissance, DNS enumeration aims to discover hosts and services by querying DNS records. A zone transfer is a special DNS operation intended for legitimate replication between an authoritative primary DNS server and its secondary DNS servers. When misconfigured, a DNS server may allow an unauthorized requester to perform a zone transfer, returning the entire DNS zone database. This can reveal extensive internal naming information such as subdomains, hostnames, mail exchangers, service records, and aliases, exactly like the "full list of internal mappings, including subdomains, mail hosts, and system aliases" described in the question. The clue
"secondary system responds unusually" is especially telling, because secondary DNS servers are commonly the ones configured for replication and may be mistakenly left open to transfers from any host.
The other options do not fit the output. LDAP enumeration targets directory services and would not yield DNS-style mappings unless you already had directory access and queries. NTP enumeration relates to time synchronization services and can reveal time/server details, not comprehensive host/subdomain lists.
NetBIOS enumeration focuses on Windows networking (names, shares, workgroups) typically on internal networks and would not produce a DNS zone's record set.
CEH-recommended mitigations include restricting zone transfers to authorized secondary server IPs only, using TSIG keys for authenticated transfers, minimizing publicly exposed DNS data, splitting internal and external DNS (split-horizon), and continuously auditing DNS configurations to prevent inadvertent information leakage.

NEW QUESTION: 85
You are Maya, a security engineer at HarborPoint Cloud Services in Chicago, Illinois, performing a post- incident hardening review after an internal audit flagged multiple services that rely on legacy public-key algorithms. The engineering team must prioritize actions company-wide to reduce long-term risk from future quantum-capable adversaries while development continues on a large refactor of several services. Which proactive control should Maya recommend as the highest-priority change to embed into the organization ' s development lifecycle to improve future resistance to quantum-based attacks?
A. Include quantum-resistance checks in SDLC and code review processes
B. Encrypt stored data with quantum-resistant algorithms
C. Use quantum-specific firewalls to protect quantum communication channels
D. Break data into fragments and distribute it across multiple locations
Answer: A (LEAVE A REPLY)
The highest-priority proactive control "to embed into the organization's development lifecycle" is including quantum-resistance checks in the SDLC and code review processes. The scenario emphasizes a company- wide, long-term risk reduction strategy while development continues on a major refactor. In that context, the most scalable and durable control is governance and engineering hygiene: ensuring that new features and refactored components do not reintroduce weak or legacy cryptography and that teams consistently select algorithms and key sizes aligned with modern guidance and future migration plans. Embedding checks into the SDLC means instituting standards and guardrails such as approved cryptographic libraries, banned algorithm lists (e.g., legacy RSA key sizes, deprecated curves, weak hashes), cryptography design reviews, automated dependency scanning for crypto usage, and CI/CD policy gates that flag noncompliant implementations. This approach reduces "crypto sprawl," prevents new technical debt, and creates a structured path to transition toward post-quantum or quantum-resistant approaches as the organization modernizes systems.
Why the other choices are not the best "highest priority" SDLC-embedded control:
Encrypt stored data with quantum-resistant algorithms (B) may be appropriate for protecting long-lived sensitive data ("harvest now, decrypt later"), but it is a targeted technical control and may not be feasible immediately across many services during refactoring. It also does not by itself prevent developers from continuing to implement legacy public-key schemes elsewhere.
Quantum-specific firewalls (C) is not a realistic or standard control for post-quantum readiness in typical enterprise environments.
Fragmenting data across locations (D) can help resilience/confidentiality in some designs but does not address the core issue: preventing continued reliance on weak public-key cryptography.

Therefore, the best answer is A. Include quantum-resistance checks in SDLC and code review processes.

NEW QUESTION: 86
In Miami, Florida, cybersecurity analyst Laura Bennett is responding to a series of unauthorized access attempts targeting Sunshine Credit Union's online banking platform. She observes unusual network activity that suggests attackers may be intercepting session IDs transmitted over unsecured connections to hijack active user sessions. To prevent further compromise, Laura works with the network team to apply a control that secures session-related communications throughout the entire portal, ensuring sensitive tokens are no longer exposed to interception during user interactions.
What countermeasure should Laura implement to prevent session hijacking in this scenario?
A. Regenerate the session ID after a successful login
B. Implement SSL to encrypt all information in transit via the network
C. Use restrictive cache directives such as Cache-Control no-cache
D. Do not create sessions for unauthenticated users
Answer: (SHOW ANSWER)
The scenario clearly indicates session hijacking risk caused by interception of session IDs over unsecured connections. In CEH-aligned web security, when session tokens are transmitted without strong transport encryption, an attacker positioned on the same network path can sniff traffic and capture cookies or URL- based session IDs, then reuse them to impersonate the victim. The most effective control that directly addresses interception in transit across the entire portal is enforcing SSL/TLS for all session-related communications, meaning every page and request that could carry authentication state is protected by HTTPS.
This prevents passive eavesdropping and significantly reduces the feasibility of man-in-the-middle capture of session identifiers during normal user interactions.
Option A, regenerating the session ID after login, is an important defense against session fixation, but it does not stop an attacker from stealing the new session token if it is later transmitted over plaintext HTTP. Option C, cache-control directives, helps prevent sensitive pages from being stored in shared caches or browser history, but it does not protect session IDs from network sniffing. Option D, avoiding sessions for unauthenticated users, can reduce some tracking exposure, yet the core issue here is hijacking of authenticated sessions due to unencrypted transport.
Therefore, implementing SSL/TLS across the portal, typically combined with secure cookie flags and strict HTTPS enforcement, is the correct countermeasure for the described interception-based session hijacking.

NEW QUESTION: 87

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: 88
Encrypted session tokens vary in length, indicating inconsistent encryption strength. What is the best mitigation?
A. Rotate keys frequently
B. Enforce MFA for privileged users
C. Implement uniform encryption strength
D. Centralized logging
Answer: C (LEAVE A REPLY)
CEH v13 explains that cryptographic consistency is essential for secure session management. Variable token lengths can leak information about encryption methods, key sizes, or user privilege levels, making sessions vulnerable to cryptanalysis or targeted attacks.
The most effective mitigation is implementing uniform encryption strength across all roles, ensuring consistent key sizes, algorithms, and token formats. While MFA improves

authentication and key rotation improves lifecycle management, neither directly resolves cryptographic inconsistency.
CEH v13 stresses that encryption should be role-agnostic and standardized. Therefore, Option C is correct.

NEW QUESTION: 89
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: 90
You are a cybersecurity analyst at a global banking corporation and suspect a backdoor attack due to abnormal outbound traffic during non-working hours, unexplained reboots, and modified system files. Which combination of measures would be most effective to accurately identify and neutralize the backdoor while ensuring system integrity?
A. Review firewall logs, analyze traffic, and immediately reboot systems
B. Monitor system and file activity, apply anomaly detection, and use advanced anti-malware tools
C. Enforce strong passwords, MFA, and regular vulnerability assessments
D. Apply ACLs, patch systems, and audit user privileges
Answer: B (LEAVE A REPLY)
According to CEH v13 Security Operations and Incident Response, backdoors are stealth mechanisms that allow attackers persistent access. Indicators such as unexplained outbound traffic, unauthorized file modifications, and irregular reboots strongly suggest post-compromise persistence mechanisms.
CEH v13 recommends a behavioral and host-based detection approach for backdoor identification.
Continuous monitoring of system and file activity helps detect unauthorized binaries, registry changes, and scheduled tasks. Anomaly detection identifies deviations from

normal system behavior, which is critical for uncovering hidden backdoors that evade signature-based detection.
Additionally, advanced anti-malware tools with heuristic and memory analysis capabilities are essential to identify sophisticated backdoors that traditional antivirus may miss. These tools can detect rootkits, fileless persistence, and covert communication channels.
The other options are preventative but not investigative. Immediate reboots may destroy volatile evidence, while password policies and ACLs do not detect existing compromises.
Therefore, option B provides the most effective and CEH-aligned response.

NEW QUESTION: 91
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: (SHOW ANSWER)
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: 92
During a red team exercise, a Certified Ethical Hacker (CEH) is attempting to exploit a potential vulnerability in a target organization's web server. The CEH has completed the information gathering and footprinting phases and has mirrored the website for offline analysis. It has also been discovered that the server is vulnerable to session hijacking. Which of the following steps is most likely to be part of a successful attack methodology while minimizing the possibility of detection?
A. Hijack an active session and immediately modify server configuration files.
B. Attempt SQL injection to extract sensitive database information.
C. Perform vulnerability scanning using automated tools to identify additional weaknesses.
D. Launch a direct brute-force attack to crack the server's administrative password.
Answer: B (LEAVE A REPLY)
According to the Certified Ethical Hacker (CEH) attack methodology, once reconnaissance, footprinting, and website mirroring have been completed, the attacker proceeds cautiously to exploitation while maintaining stealth. CEH documentation emphasizes that low-noise, application-layer attacks are preferable when the objective is to minimize detection.
Option B, attempting SQL Injection, aligns directly with CEH's Web Application Hacking module. SQL Injection is a server-side attack that can often be executed through normal-looking HTTP requests, making it less likely to trigger intrusion detection systems (IDS) or security alerts. CEH materials highlight SQL injection as a common and effective technique for extracting sensitive data such as usernames, passwords, and business-critical information without disrupting server operations.
Option A is incorrect because immediately modifying server configuration files after session hijacking significantly increases the risk of detection. CEH guidelines stress post-exploitation restraint, especially during red team operations.
Option C is not ideal at this stage because automated vulnerability scanners generate substantial traffic and are highly detectable. CEH explicitly notes that vulnerability scanning is noisy and often logged.
Option D is the least stealthy option. Brute-force attacks generate numerous failed authentication attempts, triggering security alerts and account lockouts. CEH classifies brute-force attacks as high-risk and easily detectable.
Therefore, SQL Injection represents the most effective and stealthy next step in accordance with CEH's structured attack lifecycle.

NEW QUESTION: 93
During a strategic security briefing at Meridian Global Analytics in Washington, D.C., executives review a series of coordinated activities targeting national infrastructure. These activities include manipulating digital media to influence public perception, disrupting communication networks, and degrading critical systems to weaken institutional stability without direct conventional military engagement. What form of conflict best describes this type of coordinated activity?

A. Cyberterrorism
B. Hacktivism
C. Cyber espionage
D. Information warfare
Answer: D (LEAVE A REPLY)
The correct answer is Information warfare. CEH introductory security coverage explains that information warfare involves coordinated use of information systems, influence operations, disruption, deception, and attacks on digital infrastructure to affect perception, decision-making, and institutional stability. The question includes manipulation of digital media, disruption of communications, and degradation of critical systems, all aimed at weakening a target without traditional military confrontation. That broad strategic combination goes beyond cyber espionage, which focuses on covert intelligence collection, and beyond hacktivism, which is typically ideologically motivated digital protest or disruption. Cyberterrorism can involve fear and critical infrastructure attacks, but the scenario is framed more comprehensively around coordinated influence and infrastructure effects as part of a broader conflict model. CEH materials use information warfare to describe conflict conducted through control, corruption, disruption, or weaponization of information and information systems. Because the activities target both perception and operational capability at a national scale, the most accurate classification is Information Warfare.

NEW QUESTION: 94
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: 95
A digital publishing firm in Charlotte, North Carolina, noticed suspicious probing activity against its public website. To proactively assess exposure, the security team initiated a focused scan of the company ' s HTTP servers. The chosen tool examined server headers,

identified installed web server software through file signatures and favicon analysis, checked for outdated components, and searched for potentially dangerous files and misconfigurations. The scan also supported SSL connections and generated exportable reports in multiple formats for documentation. Which vulnerability assessment tool most closely aligns with the capabilities described?

A. OpenVAS

B. Nessus

C. Qualys VM

D. Nikto

Answer: D (LEAVE A REPLY)

The correct answer is Nikto. CEH web server security coverage identifies Nikto as a specialized open-source web server vulnerability scanner designed to assess HTTP and HTTPS services for dangerous files, insecure default content, outdated server versions, and version-specific problems. The scenario mentions examination of server headers, detection of installed web server software, checks for outdated components, identification of dangerous files and misconfigurations, SSL support, and exportable reporting. Those characteristics align closely with Nikto's typical use in CEH-style web server assessments. OpenVAS, Nessus, and Qualys VM are broad vulnerability management platforms with much wider enterprise coverage, but the question describes a focused HTTP-server scanner rather than a full-spectrum infrastructure scanner. CEH materials frequently present Nikto in the context of web server enumeration and vulnerability discovery after the tester has identified the target web platform. It is especially useful for quickly checking internet-facing servers for known risky files, weak configurations, and outdated software. Because the assessment is centered on the specific exposure of web servers and matches the recognized feature set of Nikto, option D is the best answer.

NEW QUESTION: 96

A penetration tester evaluates a company ' s secure web application, which uses HTTPS, secure cookie flags, and strict session management to prevent session hijacking. To bypass these protections and hijack a legitimate user ' s session without detection, which advanced technique should the tester employ?

A. Utilize a session fixation attack by forcing a known session ID during login

B. Perform a Cross-Site Scripting (XSS) attack to steal the session token

C. Exploit a timing side-channel vulnerability to predict session tokens

D. Implement a Man-in-the-Middle (MitM) attack by compromising a trusted certificate authority

Answer: D (LEAVE A REPLY)

CEH materials explain that modern web applications deploy multiple layers of security-HTTPS, secure cookies, HttpOnly flags, and strict session regeneration-to defend against standard hijacking methods such as token theft through XSS or fixation. When these protections are properly implemented, attackers must compromise the underlying trust

relationship between the client and server to successfully intercept or manipulate session tokens. One of the most advanced techniques described in CEH is compromising a trusted certificate authority or injecting a forged certificate into the victim's trust store. This enables the attacker to perform a transparent MITM attack despite HTTPS protections. Because the victim's browser trusts the forged certificate, encrypted traffic-including session tokens-is exposed to the attacker without generating browser warnings or IDS alerts. Timing side-channel attacks are not considered session hijacking methods; XSS is mitigated by secure flags; and session fixation is ineffective when session regeneration occurs.
Therefore, compromising a trusted certificate authority to enable an undetectable MITM attack is the most viable method.

NEW QUESTION: 97
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: A (LEAVE A REPLY)
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: 98
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: 99
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: (SHOW ANSWER)
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: 100
As an Ethical Hacker, you have been asked to test an application's vulnerability to SQL injection. During testing, you discover an entry field that appears susceptible. However, the backend database is unknown, and regular SQL injection techniques have failed to produce useful information. Which advanced SQL injection technique should you apply next?
A. Content-Based Blind SQL Injection
B. Time-Based Blind SQL Injection
C. Union-Based SQL Injection

D. Error-Based SQL Injection

Answer: (SHOW ANSWER)

This scenario clearly describes the need for Time-Based Blind SQL Injection, an advanced SQL injection technique covered in the CEH v13 Web Application Hacking module. Blind SQL injection is used when an application does not return database errors or visible output, making traditional techniques ineffective.

According to CEH v13, Time-Based Blind SQL Injection is particularly useful when:

* The backend database type is unknown
* Error messages are suppressed
* UNION queries fail
* No direct data is returned in responses

In this technique, attackers inject SQL statements that deliberately introduce time delays using database- specific functions such as SLEEP(), WAITFOR DELAY, or BENCHMARK(). The ethical hacker then observes the application's response time to determine whether the injected condition is true or false.

For example:

' OR IF(1=1, SLEEP(5), 0) --

If the application response is delayed, it confirms that the injected SQL statement was executed successfully.

CEH v13 categorizes this method as behavioral-based inference, where the attacker extracts information one bit at a time by analyzing timing differences.

Other options are incorrect because:

* Content-Based Blind SQL Injection relies on visible differences in responses, which the question states are unavailable.
* Union-Based SQL Injection requires knowing column count and data types.
* Error-Based SQL Injection depends on database error messages being displayed.

CEH v13 emphasizes Time-Based Blind SQL Injection as a last-resort yet highly effective technique when dealing with hardened applications that suppress output, making it a frequent exam-tested concept.

NEW QUESTION: 101

During a security audit, a penetration tester observes abnormal redirection of all traffic for a financial institution's primary domain. Users are being redirected to a phishing clone of the website. Investigation shows the authoritative DNS server was compromised and its zone records modified to point to the attacker's server. This demonstrates total manipulation of domain-level resolution, not cache poisoning or client-side attacks. Which technique is being used in this scenario?

A. Establish covert communication using DNS tunneling over standard DNS queries

B. Perform DNS rebinding to manipulate browser-origin interactions

C. Carry out DNS server hijacking by tampering with the legitimate name-resolution infrastructure

D. Initiate a DNS amplification attack using recursive servers

Answer: C (LEAVE A REPLY)

CEH v13 states that DNS server hijacking occurs when attackers compromise the authoritative DNS infrastructure and alter DNS zone records to redirect all legitimate queries to malicious destinations. Unlike DNS cache poisoning, which affects specific resolvers temporarily, server hijacking manipulates the core DNS authority controlling the domain. This results in a complete redirect for all users, regardless of geographic location or device configuration. CEH emphasizes that such attacks can lead to large-scale credential theft, phishing, financial fraud, and session compromise because the attacker presents an identical clone site while retaining full control of DNS routing. DNS tunneling is used for covert data exfiltration and does not redirect traffic. DNS rebinding targets browser policies, not global DNS redirection. DNS amplification is a volumetric DDoS technique unrelated to zone manipulation. The scenario matches DNS server hijacking exactly.

NEW QUESTION: 102

As a Certified Ethical Hacker assessing session management vulnerabilities in a secure web application using MFA, encrypted cookies, and a WAF, which technique would most effectively exploit a session management weakness while bypassing these defenses?

A. Utilizing Session Fixation to force a victim to use a known session ID

B. Executing a Cross-Site Request Forgery (CSRF) attack

C. Exploiting insecure deserialization vulnerabilities for code execution

D. Conducting Session Sidejacking using captured session tokens

Answer: A (LEAVE A REPLY)

The CEH Web Application Hacking module identifies Session Fixation as a powerful session management attack that can bypass advanced authentication controls, including MFA.

In session fixation, the attacker forces the victim to authenticate using a session ID already known to the attacker. Once authentication completes, the attacker hijacks the valid session without needing credentials.

Option A directly targets session management logic.

Option B exploits authorization logic, not session handling.

Option C is unrelated to session management.

Option D is mitigated by encrypted cookies and HTTPS.

CEH explicitly warns that applications must regenerate session IDs after authentication.

NEW QUESTION: 103

During a security assessment of a metropolitan public transportation terminal, a penetration tester examines a network-connected IoT surveillance camera system used for 24/7 video monitoring. The camera uses outdated SSLv2 encryption to transmit video data. The tester intercepts and decrypts video streams due to the weak encryption and absence

of authentication mechanisms. What IoT vulnerability is most likely being exploited in this scenario?

A. Insecure data transfer and storage

B. Jamming attack on RF communication

C. Credential theft via web application

D. Replay attack on wireless signals

Answer: A (LEAVE A REPLY)

CEH identifies insecure data transfer as a critical IoT weakness. Outdated encryption protocols such as SSLv2 fail to protect confidentiality or integrity. Without strong encryption and authentication, attackers can intercept, decrypt, and manipulate video feeds.

NEW QUESTION: 104

A digital forensics consultant in Portland, Oregon examines an iPhone seized as part of a corporate data leakage investigation. The device contains third-party extensions and system modifications not typically permitted by the operating system vendor. The owner explains that whenever the device is powered off and restarted, it boots normally and remains fully functional for everyday tasks such as calls and messaging.

However, the custom extensions and system-level tweaks do not function until a specific jailbreak application installed on the device is manually executed. No external computer is required during this reactivation process. Determine the type of jailbreaking technique implemented on this device.

A. Tethered Jailbreaking

B. Semi-Tethered Jailbreaking

C. Untethered Jailbreaking

D. Semi-Untethered Jailbreaking

Answer: D (LEAVE A REPLY)

The correct answer is Semi-Untethered Jailbreaking. CEH mobile platform material distinguishes jailbreak persistence based on what happens after a reboot. In this scenario, the iPhone restarts normally and remains usable for ordinary functions, but the jailbreak-specific capabilities are inactive until the user manually runs a jailbreak application on the device. No computer is needed for that reactivation. That is the defining behavior of semi-untethered jailbreaking. Tethered jailbreaking would require connection to a computer during reboot.

Untethered jailbreaking would remain fully active across restarts with no manual reactivation step. Semi- tethered wording is sometimes used in older materials to describe normal boot without an immediate computer dependency, but in CEH-style modern exam phrasing, the specific indicator that an on-device app must be launched to reapply the jailbreak points to semi-untethered. CEH mobile security guidance uses these distinctions to help analysts recognize persistence, forensic artifacts, and operational risk on compromised iOS devices. Because the system boots normally, loses jailbreak

functionality after restart, and regains it only when the local jailbreak app is executed, the most accurate classification is Semi-Untethered Jailbreaking.

NEW QUESTION: 105
During a red team operation for XYZ Financial Services, security analyst Lily Jensen is assigned to scan a critical subnet that is protected by an IDS. Her initial scan attempt is immediately flagged and blocked. To evade detection while continuing reconnaissance, she adjusts the scanning configuration to include multiple spoofed IP addresses alongside her own. This makes it difficult for network defenses to isolate her real scanning activity, while still allowing her to receive accurate results.
Which scanning technique is Lily using?
A. SYN FIN Scanning
B. Source Routing
C. IP Spoofing
D. Decoy Scanning
Answer: D (LEAVE A REPLY)
The technique described is decoy scanning. In CEH network scanning methodology, decoy scanning is used to make IDS and logging systems attribute scan traffic to multiple apparent sources instead of the attacker's true IP address. The attacker configures the scanner to generate additional probe packets that appear to originate from several spoofed decoy IP addresses, mixed with the real attacker's probes. This creates ambiguity for defenders because IDS alerts and firewall logs show many potential "scanners," complicating attribution and response actions such as blocking a single source.
A key detail in the prompt is that Lily "includes multiple spoofed IP addresses alongside her own" and still
"receives accurate results." That matches how decoy scanning works in tools like Nmap: the attacker's real IP must remain in the mix so that replies from the target return to the attacker, enabling accurate interpretation of port states. The decoys mainly exist to confuse monitoring and incident response teams by polluting the log trail.
Option C, IP spoofing, is too general and, by itself, typically prevents the attacker from receiving responses because return traffic goes to the spoofed address. Decoy scanning is a specific, structured use of spoofing combined with the real source to preserve results. Option A refers to stealth flag scans, which reduce handshake visibility but do not involve multiple spoofed sources. Option B, source routing, attempts to control packet paths and is not the described behavior. Therefore, the correct answer is Decoy Scanning.

NEW QUESTION: 106
A defense contractor in Arlington, Virginia, initiated an internal awareness exercise to test employee susceptibility to human-based manipulation. During the assessment, an individual posing as an external recruitment consultant began casually engaging several engineers at a nearby industry networking event. Over multiple conversations, the

individual gradually steered discussions toward current research initiatives, development timelines, and internal project code names. No direct requests for credentials or system access were made. Instead, the information was obtained incrementally through carefully crafted questions embedded within informal dialogue. Which social engineering technique is most accurately demonstrated in this scenario?

A. Quid Pro Quo

B. Baiting

C. Elicitation

D. Honey Trap

Answer: C (LEAVE A REPLY)

The technique demonstrated is Elicitation. CEH social engineering coverage explains elicitation as the art of drawing out information from a target through conversation without making direct or obviously suspicious requests. The attacker carefully guides dialogue so the victim voluntarily reveals sensitive details, often believing the discussion is normal, harmless, or professionally relevant. That is exactly what happens here: the person poses as a recruitment consultant, builds rapport through multiple informal interactions, and gradually obtains information about research, timelines, and internal code names. No credentials are requested and no overt trade or reward is offered, so this is not quid pro quo. It is also not baiting, which typically relies on an enticing object or opportunity, nor a honey trap, which usually involves romantic or intimate manipulation.

CEH materials emphasize that elicitation is especially dangerous because the victim often does not realize that the attacker's questions are strategically sequenced to extract valuable intelligence piece by piece. The gradual, conversational, non-confrontational harvesting of sensitive project details in this scenario is the defining pattern of elicitation.

NEW QUESTION: 107

During a penetration test at a financial services firm in Boston, ethical hacker Daniel simulates a DDoS against the customer portal. To handle the surge, the IT team sets a rule that caps the number of requests a single user can make per second; aggressive connections are delayed or dropped while most legitimate customers continue to use the service.

Which countermeasure strategy is the IT team primarily using?

A. Rate Limiting
B. Shutting Down Services
C. Absorb the Attack
D. Degrading Services
Answer: A (LEAVE A REPLY)
The IT team's action-capping how many requests a single user can make per second and then delaying or dropping aggressive connections-is the defining behavior of rate limiting. In DDoS conditions, especially when the portal is under a surge of automated or abusive traffic, rate limiting enforces a policy that restricts request frequency from a source (such as an IP address, session, API key, or user identifier). This helps preserve availability by preventing any one client (or a small set of clients) from consuming a disproportionate share of application and infrastructure resources.
The key wording in the scenario is that "aggressive connections are delayed or dropped while most legitimate customers continue to use the service." Rate limiting is designed for precisely this outcome: it introduces friction for abusive traffic patterns while allowing typical user behavior through. Depending on implementation, controls can respond with delays (throttling), temporary blocks, connection resets, or HTTP error responses (for example, "too many requests") when limits are exceeded. This is commonly applied at the edge (reverse proxy/CDN), load balancer, WAF, or application gateway to reduce pressure on backend services.
Why the other options are not the best match:
Shutting Down Services (B) is an extreme measure that sacrifices availability to stop an attack; the scenario explicitly states service largely continues.
Absorb the Attack (C) refers to scaling capacity or using scrubbing centers/CDNs to handle volume without necessarily restricting individual requester behavior; the described control is specifically per-user request caps.
Degrading Services (D) generally means intentionally reducing functionality or quality (e.g., disabling non- essential features) to keep core services alive; here, the main technique is enforcing request-rate thresholds.
Thus, the countermeasure strategy being used is A. Rate Limiting.

NEW QUESTION: 108
As a network administrator, you explain to your team that a recent DDoS attack targeted the application layer of your company's web server. Which type of DDoS attack was most likely used?
A. HTTP flood attack
B. UDP flood attack
C. ICMP flood attack
D. SYN flood attack
Answer: (SHOW ANSWER)

According to the CEH Denial-of-Service (DoS/DDoS) module, application-layer DDoS attacks specifically target services such as HTTP, HTTPS, DNS, or APIs by sending requests that appear legitimate but overwhelm server resources.
An HTTP flood attack sends a massive number of HTTP GET or POST requests, consuming CPU, memory, and application threads. CEH highlights that these attacks are particularly dangerous because they:
* Mimic normal user behavior
* Are difficult to distinguish from legitimate traffic
* Bypass traditional network-layer defenses
Option A is correct.
Options B, C, and D operate primarily at the network or transport layers, not the application layer.
CEH stresses that HTTP floods are among the most challenging DDoS attacks to mitigate due to their stealthy nature.

NEW QUESTION: 109
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: 110
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: (SHOW ANSWER)
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: 111
A penetration tester is attacking a wireless network running WPA3 encryption. Since WPA3 handshake protections prevent offline brute-force cracking, what is the most effective approach?
A. Downgrade the connection to WPA2 and capture the handshake to crack the key
B. Execute a dictionary attack on the WPA3 handshake using common passwords

C. Perform a brute-force attack directly on the WPA3 handshake
D. Perform a SQL injection attack on the router ' s login page
Answer: (SHOW ANSWER)
CEH v13 explains that WPA3 introduces SAE (Simultaneous Authentication of Equals), which resists traditional offline dictionary and brute-force attacks by removing crackable handshake material. Because WPA3 prevents attackers from capturing a reusable handshake, the most practical offensive method is to force a downgrade attack, tricking clients into associating using WPA2 instead of WPA3. Once the victim reconnects under WPA2-PSK, the attacker captures the standard 4-way handshake, which can then be cracked offline using dictionary or GPU-accelerated brute-force methods. CEH discusses downgrade attacks as a significant real-world threat when mixed-mode configurations are enabled or when access points fail to enforce strict WPA3-only operation. Options B and C are ineffective because WPA3 handshake materials cannot be brute-forced offline. Option D is unrelated to Wi-Fi encryption. Downgrading to WPA2 is the most effective and widely documented attack path.

NEW QUESTION: 112
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: 113
During a red team assessment of an enterprise LAN environment, the tester discovers an access switch that connects multiple internal workstations. The switch has no port security measures in place. To silently intercept communication between different hosts without deploying ARP poisoning or modifying the routing table, the tester launches a MAC flooding attack using the macof utility from the dsniff suite. This command sends thousands of Ethernet frames per minute, each with random, spoofed source MAC addresses. Soon after the flooding begins, the tester puts their network interface into promiscuous mode and starts capturing packets. They observe unicast traffic between internal machines appearing in their packet sniffer-traffic that should have been isolated. What internal switch behavior is responsible for this sudden exposure of isolated traffic?
A. The switch performed ARP spoofing to misroute packets.
B. The switch entered hub-like behavior due to a full CAM table.
C. The interface performed DHCP starvation to capture broadcasts.
D. The switch disabled MAC filtering due to duplicate address conflicts.
Answer: B (LEAVE A REPLY)
CEH explains that MAC flooding overwhelms a switch's CAM table, causing it to fail open. When the table fills, the switch broadcasts frames out all ports, behaving like a hub. This exposes unicast traffic to attackers operating in promiscuous mode.

NEW QUESTION: 114
During an internal security assessment of a medium-sized enterprise network, a security analyst notices an unusual spike in ARP traffic. Closer inspection reveals that one particular MAC address is associated with multiple IP addresses across different subnets. The ARP packets were unsolicited replies rather than requests, and several employees from different departments have reported intermittent connection drops, failed logins, and broken intranet sessions. The analyst suspects an intentional interference on the local network segment.

What is the most likely cause of this abnormal behavior?
A. ARP poisoning causing routing inconsistencies
B. DHCP snooping improperly configured
C. Legitimate ARP table refresh on all clients
D. Port security restricting all outbound MAC responses
Answer: A (LEAVE A REPLY)
CEH v13 explains that ARP poisoning (also known as ARP spoofing) occurs when an attacker sends forged ARP replies across the network to associate their MAC address with multiple IP addresses, tricking hosts into sending traffic through the attacker's machine. This results in routing inconsistencies, intermittent connectivity, failed logins, and degraded intranet performance-exactly the symptoms described. ARP poisoning typically involves unsolicited ARP replies, which overwrite legitimate ARP cache entries. CEH emphasizes that ARP-based attacks are common on LANs because ARP lacks authentication, allowing attackers to impersonate gateways or key hosts. DHCP snooping misconfigurations (Option B) affect IP allocation, not ARP mappings. Legitimate ARP refreshes (Option C) are request-based and do not involve flooding unsolicited replies. Port security restrictions (Option D) block MAC anomalies, not create them.
Therefore, ARP poisoning is the correct root cause.

NEW QUESTION: 115
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: (SHOW ANSWER)
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: 116

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.

NEW QUESTION: 117
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: 118

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: 119
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: 120
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: D (LEAVE A REPLY)

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: 121
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. Metasploit
B. Nmap
C. Colasoft Packet Builder
D. Traffic IQ Professional
Answer: D (LEAVE A REPLY)

NEW QUESTION: 122
During a penetration test at a technology startup in Austin, Texas, an ethical hacker is tasked with evaluating defenses against stealthy scanning techniques. She selects an approach that involves sending TCP packets with no flags, relying on the way target systems respond to infer whether ports are open or closed. This allows her to remain less visible to intrusion detection systems compared to a full handshake. Which scanning method is she using?
A. TCP Connect Scan
B. FIN Scan
C. NULL Scan
D. ACK Scan
Answer: C (LEAVE A REPLY)
The method described-sending TCP packets with no flags set-is a NULL scan. In TCP header terminology, a NULL packet has all control flags cleared (no SYN, ACK, FIN, RST, PSH, URG). The scanner then interprets the target's response behavior to infer port state. Traditionally, for many TCP/IP stacks, a closed port responds with RST, while an open port may respond with no reply (silence) because the packet does not correspond to any valid state in the TCP state machine. This behavior can vary by OS and filtering devices, but the defining characteristic is the "no flags" probe.
The scenario also highlights stealth: compared to a TCP connect scan, which completes a full three-way handshake and is easily logged, NULL scans can be less conspicuous because they avoid a normal connection setup. Some intrusion detection systems focus heavily on repeated SYN handshakes or completed connections; unusual flag scans may slip through weak detection, though modern IDS/IPS can still detect them.
Why the other options are incorrect:
TCP Connect Scan (A) uses the operating system's connect() call to establish a full TCP connection; it is not a "no flags" technique and is generally noisier.
FIN Scan (B) sends packets with the FIN flag set; it is a different "stealth" scan type, but not "no flags." ACK Scan (D) sends packets with the ACK flag set and is typically used to map firewall rules (filtered vs unfiltered), not to determine open vs closed ports in the same way, and again it is not "no flags." Therefore, the scanning method is C. NULL Scan.

NEW QUESTION: 123
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: (SHOW ANSWER)
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: 124
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: D (LEAVE A REPLY)
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: 125
During a penetration test at Pacific Shipping Co. in Seattle, ethical hacker Mia Chen evaluates the defenses protecting the company ' s web-facing servers. She observes that the security system is not only checking basic packet headers but also validating session

state and performing some application-level analysis. This multilayer approach makes it more difficult for Mia to bypass the firewall using simple fragmentation or tunneling attacks. Which type of firewall is Mia most likely facing?

A. Packet Filtering Firewall

B. Stateful Multilayer Inspection Firewall

C. Application-Level Firewall

D. Circuit-Level Gateway Firewall

Answer: B (LEAVE A REPLY)

The firewall described is doing more than simple header checks: it is validating session state and also performing some application-level analysis. That combination is characteristic of a Stateful Multilayer Inspection Firewall. This firewall type expands beyond traditional packet filtering by tracking the state of network connections (e.g., TCP handshake progression, established sessions, expected flags and sequence behavior) and applying inspection across multiple OSI layers. Because it understands whether traffic belongs to a legitimate, established session, it can block many spoofed or out-of-context packets that might pass a stateless filter.

The mention of being harder to bypass with fragmentation or tunneling attacks further supports this. Stateless packet-filtering firewalls mainly rely on source/destination IP, port, and protocol fields. Attackers may attempt fragmentation to split payloads across packets and evade simplistic inspection, or use tunneling to encapsulate traffic to hide prohibited content. A stateful multilayer firewall, by maintaining connection tables and reassembling or correlating traffic with session context, is better equipped to detect anomalies that do not align with valid session behavior and to apply deeper inspection policies.

Why the other choices are less fitting:

A Packet Filtering Firewall (A) focuses on basic header fields and is typically stateless, matching the opposite of what Mia observed.

An Application-Level Firewall (C) (proxy firewall) can do deep application inspection, but the scenario emphasizes a multilayer approach combining state tracking with application-level checks-more aligned with stateful multilayer inspection than a pure application proxy model.

A Circuit-Level Gateway Firewall (D) validates session establishment (e.g., TCP handshakes) and creates virtual circuits, but it generally does not perform meaningful application-level analysis of the content.

Therefore, the best match is B. Stateful Multilayer Inspection Firewall.

NEW QUESTION: 126

During a controlled red team engagement at a financial institution in New Jersey, ethical hacker Ryan tests the bank ' s resilience against stealth-based malware. He plants a custom malicious program on an employee workstation. After execution, he observes that the infected files continue to function normally, but his malware conceals its modifications by intercepting operating system calls. Antivirus scans repeatedly return

"no threats detected," even though the malicious code remains active and hidden on the system.
Which type of virus did Ryan most likely deploy in this assessment?
A. Cavity Virus
B. Stealth Virus
C. Polymorphic Virus
D. Macro Virus
Answer: (SHOW ANSWER)
The correct answer is B. Stealth Virus because the defining characteristic described is hiding malicious presence by intercepting operating system calls and masking changes so that normal tools (including antivirus scans) do not observe the infection. In CEH-aligned malware concepts, stealth viruses are designed to evade detection by concealing modifications to files, boot records, or system areas. They commonly do this by hooking system functions or APIs so that when the OS or a security product requests file contents, sizes, checksums, directory listings, or other metadata, the virus returns clean-looking or original data instead of the infected/modified version. This makes infected files appear to "function normally," while the malware remains active in memory and persists on disk.
The scenario explicitly mentions that "infected files continue to function normally" and that the malware
"conceals its modifications by intercepting operating system calls." That is the classic behavior of stealth techniques: manipulate what the system reports, not necessarily change the outward behavior of the application. The repeated "no threats detected" results also align: signature-based or basic scanning can be blinded when the malware controls the interface through which the scanner reads target files or system structures.
Why the other options are less correct: a polymorphic virus focuses on changing its code/signature between infections to evade signature-based detection, but the key clue here is OS call interception and hiding modifications, not code mutation. A macro virus targets macro-enabled documents and spreads through macro execution in office applications; it is not primarily defined by OS-level call hooking. A cavity virus (spacefiller) hides by inserting itself into unused areas of a file without changing the file size, but the scenario' s emphasis is on intercepting OS calls to conceal changes, which is more directly the stealth-virus behavior.
Therefore, Ryan most likely deployed a stealth virus.

NEW QUESTION: 127
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: 128
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: (SHOW ANSWER)
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: 129
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: C (LEAVE A REPLY)
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: 130
During a security assessment, a consultant investigates how the application handles requests from authenticated users. They discover that once a user logs in, the application does not verify the origin of subsequent requests. To exploit this, the consultant creates a web page containing a malicious form that submits a funds transfer request to the application. A logged-in user, believing the page is part of a promotional campaign, fills out the form and submits it. The application processes the request successfully without any reauthentication or user confirmation, completing the transaction under the victim's session.
Which session hijacking technique is being used in this scenario?
A. Hijacking a user session using a session fixation attack
B. Hijacking a user session using a session replay attack
C. Hijacking a user session using a cross-site request forgery attack
D. Hijacking a user session using a cross-site script attack
Answer: (SHOW ANSWER)
CEH v13 describes Cross-Site Request Forgery (CSRF) as an attack in which an authenticated user ' s browser is tricked into submitting unauthorized actions to a trusted application without the user ' s intent.
CSRF exploits the fact that browsers automatically include stored session cookies when sending requests to a domain the user is logged into. In this scenario, the attacker creates a malicious form that triggers an unwanted funds transfer. Since the application does not validate request origin, enforce CSRF tokens, or require secondary verification, it processes the attacker ' s forged request as if it came legitimately from the victim. CEH emphasizes that CSRF differs from XSS because no malicious script executes on the target website; instead, the attacker leverages the victim's authenticated session. This is

distinct from session fixation (Option A), replay attacks (Option B), and XSS (Option D). The described behavior aligns precisely with CSRF exploitation.

NEW QUESTION: 131
You are an ethical hacker at Nexus Cybersecurity, contracted to perform a penetration test for BlueRidge Retail, a US-based e-commerce company in Atlanta, Georgia. While testing their online store's product search page, you attempt to inject a malicious query into the URL to extract customer data. The application is protected by a web application firewall WAF that blocks standard SQL injection attempts. To bypass this, you modify your input to split the query into multiple parts, ensuring the malicious instructions are not detected as a single signature. For example, you craft the URL as products.php?id=1+UNION+SE+LECT +1,2, which successfully retrieves unauthorized data. Based on the observed behavior, which SQL injection evasion technique are you employing?
A. Hex Encoding
B. String Concatenation
C. In-line Comment
D. Null Byte
Answer: B (LEAVE A REPLY)
String concatenation is the best match because the technique described is breaking a recognizable SQL keyword or payload into separate pieces so a signature-based WAF rule does not see the full malicious token in one continuous pattern. In CEH-aligned web application testing, many WAF detections rely on matching known strings such as UNION SELECT, OR 1=1, and other classic patterns. If an attacker can cause the database parser to interpret the same meaning while the input appears different at the inspection layer, the WAF may fail to match its rule and the payload can reach the backend.
The prompt explicitly says you "split the query into multiple parts" to avoid detection as "a single signature." That is the core idea of concatenation-based evasion: represent the same instruction through separated fragments that are recombined or tolerated by the SQL parser, depending on the database and application behavior. This differs from in-line comments, which would typically insert comment markers inside keywords to break signatures while preserving parsing, and differs from hex encoding, which replaces characters or strings with hexadecimal representations. A null byte technique is usually associated with string-termination tricks in older contexts and does not align with splitting SQL keywords for WAF bypass.
Defensively, CEH guidance emphasizes that relying on WAF signatures alone is insufficient. Strong prevention requires parameterized queries, strict server-side input validation, least-privilege database accounts, and monitoring for anomalous query patterns and error behaviors even when obvious signatures are not present.

NEW QUESTION: 132

A system analyst wants to implement an encryption solution that allows secure key distribution between communicating parties. Which encryption method should the analyst consider?

A. Disk encryption

B. Symmetric encryption

C. Hash functions

D. Asymmetric encryption

Answer: D (LEAVE A REPLY)

The Certified Ethical Hacker (CEH) Cryptography module explains that one of the primary challenges in encryption is secure key distribution. Asymmetric encryption, also known as public-key cryptography, was specifically designed to address this issue.

In asymmetric encryption, each entity possesses a public key and a private key. The public key can be shared openly, allowing anyone to encrypt data securely, while only the corresponding private key can decrypt it.

CEH documentation highlights that this model eliminates the need to transmit secret keys over insecure channels.

Option D is correct because asymmetric encryption enables secure key exchange without prior trust.

Option B (symmetric encryption) requires a shared secret key and suffers from key distribution challenges.

Option A refers to data-at-rest protection, not key exchange.

Option C provides integrity verification, not encryption.

CEH emphasizes that asymmetric encryption underpins secure protocols such as TLS and digital certificates.

NEW QUESTION: 133

A government agency trains a group of cybersecurity experts to carry out covert cyber missions against foreign threats and gather intelligence without being detected. These experts work exclusively for national interests. What classification best describes them?

A. Organized hackers

B. State-sponsored hackers

C. Hacktivists

D. Gray hat hackers

Answer: B (LEAVE A REPLY)

CEH courseware categorizes hackers based on intent, authorization, and affiliation. State-sponsored hackers are defined as individuals or teams who conduct cyber operations on behalf of a government to advance national interests. These operations often include espionage, cyber warfare, intelligence gathering, and covert offensive actions. Unlike organized hackers or cybercriminal groups, whose motivations may include financial gain or ideological activism, state-sponsored units follow strategic directives issued by government agencies. CEH materials explain that such groups operate with access to

advanced tools, long-term funding, and classified intelligence, enabling them to execute highly sophisticated and covert operations targeting foreign governments, corporations, or critical infrastructure. Hacktivists pursue political or social causes, while gray-hat hackers operate without explicit permission but without malicious intent. Only state-sponsored hackers match the scenario where cyber experts are formally trained, resourced, and authorized by a national government to conduct operations that remain undetected. Therefore, the correct classification is state- sponsored hackers.

NEW QUESTION: 134
Using nbtstat -A < IP > , NetBIOS names including < 20 > and < 03 > are retrieved, but shared folders cannot be listed. Why?
A. File and printer sharing is disabled
B. NetBIOS runs on a non-standard port
C. nbtstat cannot enumerate shared folders
D. The host is not in an AD domain
Answer: (SHOW ANSWER)
CEH v13 clarifies that nbtstat is used only for NetBIOS name table enumeration, not for listing shared resources. Tags such as < 20 > indicate file server services, but share enumeration requires tools like net view or SMB enumeration utilities.
Thus, the inability to list shares is due to tool limitation, not service configuration. Option C is correct.

NEW QUESTION: 135
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: 136
A penetration tester is assessing a web application that does not properly sanitize user input in the search field. The tester suspects the application is vulnerable to a SQL injection attack. Which approach should the tester take to confirm the vulnerability?
A. Use directory traversal in the search field to access sensitive files on the server
B. Input a SQL query such as 1 OR 1=1 - into the search field to check for SQL injection
C. Perform a brute-force attack on the login page to identify weak passwords
D. Inject JavaScript into the search field to perform a Cross-Site Scripting (XSS) attack
Answer: B (LEAVE A REPLY)
SQL injection is one of the most common and dangerous vulnerabilities covered in CEH training. It occurs when an application accepts unsanitized input and directly passes it to a backend SQL query. To confirm the presence of SQL injection, the tester must insert a payload that alters the logic of the SQL query executed by the application. A classic test payload such as "1 OR 1=1 -" is widely used because it forces the database to return all rows instead of filtering based on the intended search value. This verifies whether the input field is being concatenated directly into a SQL command. The CEH methodology emphasizes starting with simple, non-destructive boolean-based payloads to safely evaluate the vulnerability without causing harm to the database or impacting server availability. Since directory traversal, brute-force login attempts, and XSS attacks target entirely different weaknesses, they are not appropriate for confirming SQL injection. The selected option aligns with proper CEH testing methodology for identifying insecure input handling and improper query construction.

NEW QUESTION: 137
An ethical hacker needs to gather sensitive information about a company's internal network without engaging directly with the organization's systems to avoid detection. Which method should be employed to obtain this information discreetly?
A. Analyze the organization's job postings for technical details
B. Exploit a public vulnerability in the company's web server
C. Perform a WHOIS lookup on the company's domain registrar

D. Use port scanning tools to probe the company's firewall

Answer: (SHOW ANSWER)

CEH v13 stresses the importance of passive reconnaissance when the goal is to avoid any interaction with the target's systems. Job postings frequently reveal detailed information such as internal technologies, OS platforms, security tools, IDS brands, virtualization environments, scripting languages, and cloud services.

CEH explicitly notes job ads as one of the richest passive intelligence sources because organizations inadvertently disclose their tech stack, often mentioning required experience with specific network components, databases, protocols, or internal tools. Options B and D involve direct interaction, violating the passive reconnaissance requirement. WHOIS lookups (Option C) provide DNS registrar information but do not reveal internal network details. Job postings, social media recruitment materials, and HR documentation are discussed in CEH as critical OSINT resources used during the footprinting phase to gather actionable intelligence while maintaining complete stealth. Thus, analyzing job postings is the correct method.

NEW QUESTION: 138

During a security assessment at Apex Technologies in Austin, Texas, the cybersecurity team identifies a high risk of social engineering attacks, including phishing, vishing, and baiting, targeting employees across departments. To strengthen defenses, the team plans to implement a countermeasure to reduce the likelihood of employees disclosing sensitive information. Which of the following countermeasures should Apex Technologies prioritize to mitigate the risk of social engineering attacks?

A. Conduct security awareness and training programs

B. Employees must verify the identity of individuals requesting information

C. Use two-factor authentication

D. Establish policies and procedures for handling sensitive information

Answer: A (LEAVE A REPLY)

Security awareness and training is the most effective primary countermeasure against social engineering because these attacks exploit human trust, curiosity, urgency, and lack of familiarity with deception tactics rather than purely technical weaknesses. In CEH guidance, phishing, vishing, and baiting succeed when users fail to recognize red flags such as unexpected requests, pressure to act quickly, suspicious links or attachments, caller spoofing, or offers that seem too good to be true. A structured awareness program directly reduces the chance of disclosure by teaching employees how to identify common pretexts, verify unusual requests, and follow safe reporting procedures.

While identity verification (option B) is an important practice, employees typically perform it correctly only when they have been trained on verification steps, escalation paths, and what "good verification" looks like under pressure. Two-factor authentication (option C) helps protect accounts even if credentials are stolen, but it does not prevent employees from sharing sensitive information such as customer data, internal documents, OTP codes,

or approving fraudulent requests-many social engineering campaigns aim beyond passwords.
Policies and procedures (option D) are necessary, but policies alone are often ignored or misunderstood without ongoing training, reinforcement, and real-world simulations.
CEH-aligned best practice is a layered approach: start with awareness training, reinforce it with clear handling policies, require verification for sensitive requests, conduct phishing simulations, and ensure employees know how to report suspicious emails/calls immediately. This combination reduces both successful compromise and the impact of attempts, but training is the foundational priority because it directly targets the human element being attacked.

NEW QUESTION: 139
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: 140
During a social engineering simulation at BrightPath Consulting in Denver, ethical hacker Liam emails employees a message that appears to come from the company's security team. The email urgently warns that
"all systems will shut down within 24 hours" unless staff download a patch from a provided link. The message is deliberately false and contains no actual malware, but it causes confusion and prompts several employees to call IT for clarification. Which social engineering technique is Liam demonstrating?
A. CThe correct answer is Hoax. CEH social engineering guidance explains that a hoax is a false warning or fabricated message intended to deceive users into believing that an urgent threat or unusual condition exists. The attacker's goal is often to provoke confusion, influence behavior, or trigger unnecessary responses even when the message does not contain actual malware or a working exploit. In this scenario, Liam sends a false security alert claiming that all systems will shut down unless employees download a patch. The message is intentionally deceptive, creates alarm, and causes staff to contact IT, which is

consistent with a hoax. Spam is merely unsolicited bulk messaging and does not specifically capture the false-warning element. Baiting relies on an enticing offer or object, and pretexting centers on a fabricated scenario used to obtain information or access. CEH materials emphasize that hoaxes are effective because they exploit fear, urgency, and trust in authority. Since the message is a deliberately false operational warning designed to manipulate employee behavior, the best classification is Hoax.

B. Baiting

C. Hoax

D. Spam

E. Pretexting

Answer: (SHOW ANSWER)

NEW QUESTION: 141

During an external assessment of a healthcare insurance company in Houston, a penetration tester identifies a service running on TCP port 389. When queried, the service accepts anonymous binds and reveals directory data. By structuring his search filter, the tester is able to obtain usernames, departmental details, and organizational units. This information could potentially be used for targeted password attacks or privilege escalation. Which classification best describes this enumeration activity?

A. SMTP Enumeration

B. DNS Enumeration

C. LDAP Enumeration

D. NTP Enumeration

Answer: C (LEAVE A REPLY)

TCP port 389 is the default port for LDAP (Lightweight Directory Access Protocol). The tester's actions- performing an anonymous bind and querying directory contents with structured search filters to extract usernames and organizational information-are definitive indicators of LDAP enumeration. LDAP is commonly used for centralized directory services (including environments integrated with Active Directory via LDAP interfaces). If misconfigured to allow anonymous binds or overly permissive searches, an attacker can retrieve valuable identity and structure data.

The scenario describes obtaining usernames, departmental details, and organizational units (OUs). Those are typical LDAP directory attributes and containers. Enumerating them can directly support follow-on attack paths: building targeted password-spraying lists, crafting spear-phishing that references accurate internal roles, identifying privileged groups, and mapping the organization's structure to prioritize high-value targets.

Even without direct credential compromise, directory disclosure increases attacker effectiveness.

Why the other options are incorrect:

SMTP enumeration (A) focuses on email systems (e.g., VRFY/EXPN/RCPT TO behaviors) and typically uses TCP/25 or related mail ports, not 389.

DNS enumeration (B) involves querying DNS records (A/AAAA, MX, NS, TXT, zone transfers) and does not involve directory binds or LDAP filters.
NTP enumeration (D) relates to time services (UDP/123) and provides timing/monlist-style information, not user/OU directory attributes.
Because the service is on TCP/389 and the technique involves binds and directory searches, the correct classification is C. LDAP Enumeration.

NEW QUESTION: 142
A penetration tester discovers that a web application is vulnerable to Local File Inclusion (LFI) due to improper input validation in a URL parameter. Which approach should the tester take to exploit this vulnerability?
A. Conduct a brute-force attack on the admin login page to gain access
B. Inject SQL commands into the URL parameter to test for database vulnerabilities
C. Perform a Cross-Site Scripting (XSS) attack by injecting malicious scripts into the URL
D. Use directory traversal to access sensitive files on the server, such as /etc/passwd
Answer: D (LEAVE A REPLY)
Local File Inclusion vulnerabilities arise when a web application incorporates user-supplied input into file- handling functions without proper sanitization. CEH courseware emphasizes that attackers can leverage directory traversal sequences (such as ../../) to escape the intended directory structure and access sensitive local files. An LFI payload commonly targets system files like /etc/passwd on Linux to extract user information or escalate the attack further.

NEW QUESTION: 143
During an investigation, an ethical hacker discovers that a web application's API has been compromised, leading to unauthorized access and data manipulation. The attacker is using webhooks and a webshell. To prevent further exploitation, which of the following actions should be taken?
A. Implement a Web Application Firewall (WAF) with rules to block webshell traffic and increase the logging verbosity of webhooks.
B. Perform regular code reviews for the webhooks and modify the API to block connections from unknown IP addresses.
C. Harden the web server security, add multi-factor authentication for API users, and restrict the execution of scripts server-side.
D. Implement input validation on all API endpoints, review webhook payloads, and schedule regular scanning for webshells.
Answer: D (LEAVE A REPLY)
This question focuses on API Security, Webhooks abuse, and Webshell mitigation, all of which are addressed in the CEH v13 Web Application Hacking and Security Operations modules. The most appropriate corrective action is Option D, as it directly addresses the root causes and persistence mechanisms of the compromise.

According to CEH v13, attackers frequently exploit improper input validation in APIs and insecure webhook implementations to inject malicious payloads or gain remote command execution. Webhooks, when not properly validated, can accept malicious requests that trigger backend processes, making them a common vector for API abuse.
Input validation on all API endpoints is critical to prevent injection attacks, including command injection and SQL injection. CEH v13 explicitly emphasizes validating request parameters, headers, and payload structures to prevent malicious manipulation.
Reviewing webhook payloads ensures that only trusted sources can trigger automated actions, preventing attackers from abusing webhook functionality. This includes validating signatures, enforcing authentication, and restricting allowed payload formats.
Finally, regular scanning for webshells is essential because webshells provide persistent backdoor access.
CEH v13 identifies webshell detection as a key defensive measure during incident response and post- exploitation containment.
Other options are incomplete:
A WAF alone cannot detect all webshells.
IP blocking is ineffective against spoofed or cloud-based attacks.
MFA and server hardening are valuable but do not directly address webhook abuse or existing webshells.
Therefore, Option D provides the most comprehensive, CEH v13-aligned mitigation strategy.

NEW QUESTION: 144
A penetration tester discovers that a system is infected with malware that encrypts all files and demands payment for decryption. What type of malware is this?
A. Worm
B. Spyware
C. Keylogger
D. Ransomware
Answer: (SHOW ANSWER)
Ransomware encrypts user data and extorts payment for restoration. CEH covers ransomware as a major threat in system hacking, highlighting encryption-based extortion as its defining behavior.

NEW QUESTION: 145
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: 146

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: D (LEAVE A REPLY)

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: 147
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: 148
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: 149
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: B (LEAVE A REPLY)
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: 150
Why explore the Deep Web during reconnaissance?
A. Insider threats
B. Physical attacker locations
C. Learning hacking techniques
D. Non-indexed company data exposure
Answer: D (LEAVE A REPLY)
CEH v13 explains that the Deep Web contains content not indexed by search engines, including exposed databases, misconfigured portals, leaked credentials, and internal documents.
This makes it a critical area to assess unintended data exposure. The Deep Web is not primarily for attacker profiling or insider detection.
Thus, Option D is correct.

NEW QUESTION: 151

A penetration tester suspects that a web application's product search feature is vulnerable to SQL injection.
The tester needs to confirm this by manipulating the SQL query. What is the best technique to test for SQL injection?
A. Inject a malicious script into the search field to test for Cross-Site Scripting (XSS)
B. Use directory traversal syntax in the search field to access server files
C. Input 1 OR 1=1 in the search field to retrieve all products from the database
D. Insert admin'- in the search field to attempt bypassing authentication
Answer: C (LEAVE A REPLY)
SQL injection testing commonly involves using tautology-based payloads such as 1 OR 1=1, which force SQL queries to evaluate as true. CEH explains that this confirms improper input sanitization and exposes whether user-supplied fields directly influence database queries. The result often returns all records, indicating successful injection.

NEW QUESTION: 152
You are a security analyst conducting a footprinting exercise for a new client to gather information without direct interaction. After using search engines and public databases, you consider using Google Hacking (Google Dorking) techniques to uncover further vulnerabilities. Which option best justifies this decision?
A. Google Hacking can help locate phishing websites that mimic the client's website.
B. Google Hacking can help discover hidden organizational data from the Deep Web.
C. Google Hacking can help identify weaknesses in the client's website code.
D. Google Hacking can assist in mapping the client's internal network structure.
Answer: C (LEAVE A REPLY)
The Certified Ethical Hacker (CEH) Footprinting and Reconnaissance module defines Google Hacking, also known as Google Dorking, as the use of advanced search operators to uncover sensitive information unintentionally exposed on the public internet. This technique remains passive, making it ideal during early reconnaissance.
Google Hacking can reveal:
Exposed configuration files
Backup files (.bak, .old, .zip)
Error messages and stack traces

Source code fragments and scripting errors
These findings often indicate coding weaknesses or insecure configurations within a web application. CEH explicitly highlights Google Dorking as an effective way to identify web application weaknesses without scanning or exploiting the target directly.
Option C is correct because Google Hacking is commonly used to identify coding and configuration weaknesses exposed through indexed files.
Option A may be possible indirectly but is not the primary justification.
Option B is incorrect because Google does not index the Deep Web.
Option D involves internal network discovery, which Google Hacking cannot directly achieve.
CEH emphasizes Google Hacking as a powerful passive reconnaissance technique for discovering exposed vulnerabilities.

NEW QUESTION: 153
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: (SHOW ANSWER)
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: 154
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: 155
Why explore the Deep Web during reconnaissance?
A. Insider threats
B. Non-indexed company data exposure
C. Physical attacker locations
D. Learning hacking techniques
Answer: B (LEAVE A REPLY)

NEW QUESTION: 156
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: 157

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: 158

Malware adapts behavior, changes code dynamically, and exfiltrates data stealthily. What is it?

A. AI-powered malware

B. Worm

C. Rootkit

D. Polymorphic virus

Answer: A (LEAVE A REPLY)

CEH v13 identifies AI-powered malware as an emerging advanced threat that adapts its execution based on environmental cues and user behavior. Unlike traditional polymorphic malware, AI-driven malware can dynamically decide when and how to execute actions to avoid detection.

The described traits-behavioral adaptation, idle-time exfiltration, encrypted communication-are hallmarks of AI-assisted malware.

Polymorphic viruses change signatures but do not adapt behavior intelligently. Rootkits focus on hiding presence. Worms propagate aggressively.

Therefore, Option A is correct.

NEW QUESTION: 159

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: C (LEAVE A REPLY)

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: 160
While conducting a covert penetration test on a UNIX-based infrastructure, the tester decides to bypass intrusion detection systems by sending specially crafted TCP packets with an unusual set of flags enabled.
These packets do not initiate or complete any TCP handshake. During the scan, the tester notices that when certain ports are probed, there is no response from the target, but for others, a TCP RST (reset) packet is received. The tester notes that this behavior consistently aligns with open and closed ports. Based on these observations, which scanning technique is most likely being used?
A. ACK flag scan to evaluate firewall behavior
B. TCP Connect scan to complete the three-way handshake
C. Xmas scan leveraging RFC 793 quirks
D. FIN scan using stealthy flag combinations
Answer: D (LEAVE A REPLY)
CEH describes FIN scans as stealthy scans that send packets with the FIN flag without initiating a TCP handshake. According to TCP RFC behavior, closed ports respond with RST packets while open ports ignore the probe, producing no response. This allows enumeration of port states while evading IDS systems that typically monitor SYN-based scans.

NEW QUESTION: 161
At Pinnacle Financial Services in Chicago, Illinois, ethical hacker Sarah Thompson is conducting a penetration test to evaluate the security of the company ' s online banking portal. During her assessment, Sarah positions herself on the internal network and uses a sniffer to capture traffic between a user's browser and the banking server. She quietly collects session data, including user IDs and authentication tokens, without interfering with the ongoing communication. Later, she plans to use this information to impersonate a legitimate user in a controlled test environment to demonstrate potential risk to the bank's IT team.
What type of session hijacking is Sarah performing during this phase of her penetration test?
A. Session Fixation Attack
B. Active Session Hijacking
C. Man-in-the-browser Attack
D. Passive Session Hijacking
Answer: D (LEAVE A REPLY)
The activity described is passive session hijacking because Sarah is only observing and capturing session- related information without altering, injecting, or disrupting the live client

server communication. In CEH coverage of session hijacking, the key distinction is whether the attacker merely eavesdrops to obtain session identifiers or actively takes control of the session in real time. Passive hijacking focuses on sniffing traffic to collect authentication material such as session IDs, cookies, bearer tokens, or other credentials transmitted in cleartext or exposed through weak transport protections. The prompt explicitly says she "quietly collects session data" and does so "without interfering," which is the hallmark of passive hijacking.
This is commonly feasible when applications use unencrypted HTTP, weak TLS configurations, or when tokens are exposed in ways that can be captured on the network. Once obtained, the attacker can replay or reuse the stolen token to impersonate the victim, which matches Sarah's plan to later use the captured tokens to demonstrate risk in a controlled environment. CEH emphasizes that session tokens effectively become the user's identity after authentication; if an attacker can steal them, they can often bypass login entirely.
Option B, active session hijacking, would involve manipulating the connection, injecting packets, desynchronizing the client, or taking over the session live. Option A, session fixation, involves forcing a victim to use a session ID chosen by the attacker, not sniffing. Option C, man-in-the-browser, requires malware within the browser to intercept or modify transactions, which is not described. Therefore, Passive Session Hijacking is correct.

NEW QUESTION: 162
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: 163
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: 164
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: C (LEAVE A REPLY)
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: 165
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: B (LEAVE A REPLY)
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: 166
During a penetration test at a regional bank in Richmond, ethical hacker Thomas is tasked with identifying weaknesses in how employee credentials are transmitted. He sets up Wireshark on a mirrored port and captures HTTP login sessions from the customer services VLAN. To quickly reconstruct entire conversations between browsers and the server, Thomas uses a feature that reassembles packet data into a readable stream, allowing him to view usernames and passwords directly in plain text.
Which Wireshark feature is Thomas most likely using in this case?
A. Filtering by IP Address
B. Display Filtering by Protocol
C. Monitoring the Specific Ports

D. Follow TCP Stream

Answer: D (LEAVE A REPLY)

Thomas is most likely using Follow TCP Stream. This Wireshark feature reconstructs the bidirectional application data carried over a TCP connection by reassembling packets in sequence into a readable conversation view. When traffic is unencrypted HTTP, the reassembled stream can reveal full request
/response content, including URLs, headers, form parameters, and-critically in this scenario-usernames and passwords transmitted in clear text (for example, within POST body parameters).

The scenario's language is a direct match: "reconstruct entire conversations between browsers and the server" and "reassembles packet data into a readable stream." That is exactly what Follow TCP Stream does: it groups packets that belong to the same TCP session and displays the payload as contiguous data, making it far easier than manually inspecting individual packets. This is commonly used during assessments and investigations to understand what data was exchanged, validate whether sensitive data is exposed, and confirm whether protections like TLS are properly applied.

Why the other options are not correct:

Filtering by IP Address (A) helps narrow the packet list to specific hosts but does not reconstruct conversations.

Display Filtering by Protocol (B) can isolate HTTP packets but still leaves the analyst to interpret individual packets without full reassembly.

Monitoring the Specific Ports (C) similarly narrows traffic (e.g., TCP/80 for HTTP) but does not present a reassembled readable session.

Because the goal is quick, readable reconstruction of HTTP login sessions over TCP, the correct answer is D.

Follow TCP Stream.

NEW QUESTION: 167

A penetration tester is hired to legally assess the security of a company ' s network by identifying vulnerabilities and attempting to exploit them. What type of hacker is this?

A. Black Hat

B. Grey Hat

C. Script Kiddie
D. White Hat
Answer: D (LEAVE A REPLY)
CEH v13 defines a white hat hacker as a security professional with explicit authorization to perform penetration testing, vulnerability assessments, and exploitation attempts within legal and contractual boundaries. Their objective is to strengthen security, not compromise it. White hats follow structured methodologies, document findings, and provide remediation recommendations. A black hat (Option A) acts maliciously and without permission. A grey hat (Option B) operates without authorization but without harmful intent, which is not compliant with corporate penetration testing procedures. Script kiddies (Option C) rely on pre-built tools without deep knowledge and are not employed for legitimate engagements. Therefore, the individual described is a white hat, operating under legal and ethical guidelines with organizational consent.

NEW QUESTION: 168
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: A (LEAVE A REPLY)
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: 169
A global fintech company receives extortion emails threatening a severe DDoS attack unless ransom is paid.
The attacker briefly launches an HTTP flood to demonstrate capability. The attack uses incomplete POST requests that overload application-layer resources, causing performance degradation. The attacker reinforces their demand with a second threat email. What type of DDoS attack is being carried out?
A. RDDoS attack combining threat and extortion
B. DRDoS attack using intermediaries
C. Recursive GET flood disguised as crawling
D. Pulse wave attack with burst patterns
Answer: A (LEAVE A REPLY)
CEH materials describe RDDoS (Ransom DDoS) attacks as threat-driven extortion campaigns where attackers demand payment and demonstrate capability by launching a short-lived DDoS burst. The purpose is to intimidate the victim into paying before a larger, sustained attack begins. The attack described uses HTTP floods with incomplete POST requests-an application-layer DDoS technique that consumes server resources by forcing the target to hold open connections. This kind of demonstration followed by an extortion email aligns precisely with RDDoS behavior. DRDoS attacks involve reflection/amplification through third-party servers, which is not occurring here. Pulse wave attacks use timed bursts and do not involve extortion, while recursive GET floods do not match the incomplete POST behavior. Therefore, the correct classification is RDDoS.

NEW QUESTION: 170
Attackers persisted by modifying legitimate system utilities and services. What key step helps prevent similar threats?
A. Weekly off-site backups
B. Monitor file hashes of sensitive executables

C. Update antivirus and firewalls
D. Disable unused ports
Answer: B (LEAVE A REPLY)
This scenario describes Living-off-the-Land (LotL) malware techniques, where attackers modify or abuse legitimate system binaries and services to evade detection. CEH v13 identifies this as a highly stealthy persistence mechanism commonly used in advanced persistent threats (APTs).
The most effective countermeasure is file integrity monitoring (FIM), specifically by tracking cryptographic hashes of critical system executables. CEH v13 emphasizes that monitoring file hashes enables early detection of unauthorized modifications to binaries such as PowerShell, cmd.exe, or Windows services.
Backups (Option A) aid recovery but do not prevent or detect compromise. Antivirus updates (Option C) often fail against modified legitimate tools. Firewall hardening (Option D) reduces attack surface but does not detect tampering of trusted binaries.
CEH v13 explicitly recommends hash-based integrity verification as a core defense against stealthy persistence mechanisms. Therefore, option B is correct.

NEW QUESTION: 171
Which advanced mobile hacking technique is the hardest to detect and mitigate in a healthcare environment?
A. Zero-day mobile exploits
B. App spoofing
C. Bluejacking
D. Side-channel attacks
Answer: A (LEAVE A REPLY)
Zero-day exploits are considered the most dangerous mobile attack vector in CEH v13 Mobile Platform Hacking. These exploits abuse previously unknown vulnerabilities, meaning no patches, signatures, or defenses exist at the time of attack.
In healthcare environments, mobile devices access sensitive EHR systems and operate under strict compliance requirements. Zero-day exploits can bypass mobile OS security, sandboxing, and antivirus controls entirely.
App spoofing and Bluejacking are easier to detect and mitigate through user awareness and Bluetooth controls. Side-channel attacks are highly specialized and rare in enterprise mobile environments.
CEH v13 stresses that zero-day attacks pose the greatest risk due to lack of detection mechanisms, making Option A correct.

NEW QUESTION: 172
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: (SHOW ANSWER)
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: 173
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: 174
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: A (LEAVE A REPLY)
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: 175
After installing a backdoor on a web server, what action best ensures it remains undetected?
A. Embed it in a frequently updated web file
B. Increase the backdoor code size
C. Install it on a non-web file referenced in a URL
D. Place it in a file type excluded from resource maps
Answer: D (LEAVE A REPLY)
In CEH v13 Maintaining Access, stealth and persistence are key goals after compromise. Placing a backdoor in a file type excluded from resource maps (such as image metadata, configuration files, or uncommon extensions) reduces the likelihood of discovery by automated scanners and integrity checks.
Option D is correct because many security tools focus on executable or commonly accessed web files. Files excluded from resource maps are less likely to be scanned or monitored.
Option A increases detection risk due to frequent changes. Option B increases signature visibility. Option C still exposes the file to access logs and monitoring.

CEH v13 highlights that attackers often hide backdoors in non-obvious locations to avoid detection.
Therefore, Option D is correct.

NEW QUESTION: 176
Maya Patel from SecureHorizon Consulting is investigating a breach at Dallas General Hospital in Texas after a nurse misplaced a smartphone containing patient management software. Although the device remained active on the network, administrators had no way to identify its physical whereabouts, delaying incident response and allowing sensitive medical records to be exposed for hours. Which mobile security guideline would have most directly reduced the impact of this incident?
A. Use anti-virus and data loss prevention (DLP) solutions
B. Utilize a secure VPN connection while accessing public Wi-Fi networks
C. Install device tracking software that allows the device to be located remotely
D. Register devices with a remote locate and wipe facility
Answer: D (LEAVE A REPLY)
The most direct guideline is D. Register devices with a remote locate and wipe facility because the incident's core impact came from two factors: loss of physical control of the device and continued exposure of sensitive records while the device remained active. A remote locate-and-wipe capability (commonly delivered through Mobile Device Management (MDM) / Enterprise Mobility Management (EMM) platforms) addresses both problems immediately: it enables administrators to identify the device's last known location (or trigger location reporting) and, critically, to remotely lock or wipe the device to prevent ongoing unauthorized access to patient data.
In healthcare environments handling regulated data, the priority during a lost-device event is rapid containment. Even if device tracking alone can help find the phone, it does not guarantee that sensitive information stops being accessed during the search. Remote wipe (often paired with remote lock, enforced encryption, and policy-based access control) reduces exposure time by allowing responders to remove protected data and invalidate application access. This is particularly important when the device is still connected to the network, because an attacker (or unauthorized holder) could continue using cached sessions, stored tokens, or locally available records until access is cut off.
Why the other options are less direct: A (anti-virus/DLP) may help detect malware or control data movement, but it does not solve the immediate lost-device containment requirement. B (VPN on public Wi-Fi) is unrelated because the problem is physical loss and inability to control the endpoint. C (install tracking software) helps locate the device, but the scenario highlights that sensitive records were exposed for hours; the most direct impact reduction is achieved when the organization can both locate and wipe/lock the device through an enrolled, centrally managed capability.
Therefore, enrolling devices in a remote locate and wipe facility would have most directly reduced the breach impact.

NEW QUESTION: 177
A security researcher reviewing an organization's website source code finds references to Amazon S3 file locations. What is the most effective way to identify additional publicly accessible S3 bucket URLs used by the target?
A. Exploit XSS to force the page to reveal the S3 links
B. Use Google advanced search operators to enumerate S3 bucket URLs
C. Use SQL injection to extract internal file paths from the database
D. Perform packet sniffing to intercept internal S3 bucket names
Answer: B (LEAVE A REPLY)
OSINT-based reconnaissance includes using search engines to identify publicly exposed cloud assets. CEH highlights Google dorking as a passive method to reveal S3 buckets indexed in search engines through patterns such as site:s3.amazonaws.com or keyword-based queries.

NEW QUESTION: 178
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: 179
A penetration tester is assessing a company's vulnerability to advanced social engineering attacks targeting its legal department. Using detailed knowledge of mergers and legal proceedings, the tester crafts a highly credible pretext to deceive legal employees into sharing confidential case documents. What is the most effective technique?
A. Send a spear-phishing email referencing specific merger details and requesting document access
B. Create a fake LinkedIn profile to connect with legal employees and request document sharing
C. Visit the office in person posing as a new legal intern to request document access
D. Conduct a mass phishing campaign with generic legal templates attached
Answer: A (LEAVE A REPLY)
CEH identifies spear-phishing as a targeted, context-rich social engineering method tailored to specific individuals or departments. By incorporating accurate insider details, attackers significantly increase trust and likelihood of disclosure.

NEW QUESTION: 180
You are an ethical hacker at Northpoint Assessments, engaged to map the wireless footprint around Harborview Plaza in San Francisco, California. To enumerate nearby networks and prompt devices to reveal SSIDs and capabilities, you actively send crafted management frames from your laptop and log each AP ' s immediate responses (including probe responses and capability information), rather than only listening for broadcasts.
Based on the described activity, which Wi-Fi discovery technique are you performing?
A. Network Discovery Software
B. Passive Footprinting
C. Wash Command
D. Active Footprinting
Answer: (SHOW ANSWER)
The activity described is active footprinting because you are not merely listening for wireless broadcasts; you are transmitting crafted 802.11 management frames to elicit

responses and gather information. In Wi-Fi reconnaissance, passive methods rely on monitoring beacon frames and other naturally occurring traffic.
Active methods, by contrast, deliberately interact with the environment-often by sending probe requests or other management frames-to prompt access points or client devices to respond with details such as SSID, supported data rates, security capabilities, and other parameters.
The scenario explicitly states you "actively send crafted management frames" and then log "immediate responses (including probe responses and capability information)." That is the defining difference between active and passive wireless footprinting. Active footprinting can reveal SSIDs that may not be visible through beacons alone (for example, networks that do not broadcast SSID in beacons may still respond under certain conditions), and it can speed discovery by forcing responses rather than waiting for periodic broadcasts or client activity.
Why the other options are less accurate:
Passive footprinting (B) contradicts the scenario because passive recon involves no transmissions from the auditor's device.
Wash command (C) refers to a specific tool/command typically associated with WPS enumeration workflows, not the general technique classification being asked here.
Network discovery software (A) is too generic; the question is asking for the technique (active vs passive), and the described behavior is clearly active.
Therefore, the correct answer is D. Active Footprinting.

NEW QUESTION: 181
During a penetration test at Horizon Tech in Austin, ethical hacker Michael sets up a man-in-the-middle attack to intercept traffic between employees and the company ' s internal web applications. He uses a lightweight tool capable of performing ARP spoofing, DNS manipulation, and packet injection while providing an interactive interface for real-time monitoring. This allows him to capture and manipulate session tokens in transit, which he later presents to the security team as proof of risk.
Which tool is Michael most likely using in this exercise?
A. Wireshark
B. Hetty
C. Caido
D. Bettercap
Answer: (SHOW ANSWER)
The tool described is most consistent with Bettercap. Bettercap is a lightweight, extensible framework commonly used in controlled security testing for man-in-the-middle (MITM) operations on local networks. It supports ARP spoofing/ARP poisoning to position the attacker between victims and gateways, enabling interception of traffic. It also supports DNS manipulation/spoofing (e.g., redirecting domain lookups to attacker-controlled destinations) and packet injection capabilities for modifying or inserting traffic.

Importantly, it provides an interactive interface that allows real-time session visibility and control, which matches the scenario's emphasis on interactive monitoring while intercepting internal web application traffic.
The objective described-capturing and manipulating session tokens in transit-is consistent with a MITM platform that can observe HTTP traffic (or influence traffic where TLS is not properly enforced or where testing includes trusted certificates in a lab). Bettercap's design as an "all-in-one" local network attack and monitoring tool makes it a typical choice for demonstrating risks from weak network segmentation, insecure DNS, lack of HTTPS/HSTS, or insufficient endpoint protections against ARP spoofing.
Why the other options are less suitable:
Wireshark (A) is primarily a packet analyzer/sniffer; it does not inherently perform ARP spoofing, DNS manipulation, or injection as an active MITM tool.
Hetty (B) and Caido (C) are web-focused interception/testing tools (proxy-style workflows). They can intercept HTTP/S when configured as a proxy, but they do not natively specialize in LAN-layer ARP spoofing and DNS manipulation for transparent MITM in the same way as Bettercap.
Therefore, the most likely tool is D. Bettercap.

NEW QUESTION: 182
A kernel-level rootkit is discovered. What is the safest remediation strategy?
A. Power down immediately
B. Deploy honeypots
C. Full system format and reinstall
D. Use rootkit scanners and tailored removal
Answer: (SHOW ANSWER)
CEH v13 identifies kernel-level rootkits as among the most dangerous malware types. Because they operate at the lowest OS level, they can hide processes, files, and system calls.
CEH v13 states that the only guaranteed remediation is a complete system wipe and clean OS reinstallation from a trusted source. Attempting removal risks incomplete eradication. Powering down alone does not remove the rootkit. Honeypots are for detection, not remediation. Tailored removal tools may fail at kernel depth.

Thus, Option C is correct.

NEW QUESTION: 183
A tester evaluates a login form that constructs SQL queries using unsanitized user input. By submitting ' C 'll- 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: A (LEAVE A REPLY)
This question describes a classic example of Tautology-Based SQL Injection, a subcategory of SQL Injection attacks which fall under Web Application Hacking in the CEH curriculum.
In a tautology-based SQL injection, the attacker injects a SQL fragment that always evaluates to true, thus bypassing the authentication mechanism. The string ' C 'll-T; - is a malformed variant, possibly meant to represent ' OR '1'='1'; --, which is one of the most basic and widely recognized tautology-based injection payloads. When injected into a vulnerable SQL query, this kind of input manipulates the WHERE clause of the query so that it always evaluates to true, regardless of the original conditions.
Here's how it works:
If the SQL query is:
SELECT * FROM users WHERE username = '$username' AND password = '$password';
And the attacker inputs:
' OR '1'='1'; --
The query becomes:
SELECT * FROM users WHERE username = '' OR '1'='1'; --' AND password = ''; This results in the execution of:
SELECT * FROM users WHERE '1'='1';
Which always evaluates to true, thereby bypassing authentication and allowing unauthorized access.
This method does not rely on error messages (Error-Based), timing delays (Time-Based Blind), or UNION statements (Union-Based). Its goal is to exploit logic within the query structure itself using boolean-based manipulation.
According to EC-Council's CEH v13 Module: Web Application Hacking, understanding tautology-based injection is critical because it's one of the most common ways attackers bypass login forms on poorly secured web applications.

NEW QUESTION: 184
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: 185
As a cybersecurity professional at XYZ Corporation, you are tasked with investigating anomalies in system logs that suggest potential unauthorized activity. System administrators have detected repeated failed login attempts on a critical server, followed by a sudden surge in outbound data traffic. These indicators suggest a possible compromise.

Given the sensitive nature of the system and the sophistication of the threat, what should be your initial course of action?
A. Conduct real-time monitoring of the server, analyze logs for abnormal patterns, and identify the nature of the activity to formulate immediate countermeasures.
B. Conduct a comprehensive audit of all outbound traffic and analyze destination IP addresses to map the attacker's network.
C. Immediately reset all server credentials and instruct all users to change their passwords.
D. Immediately disconnect the affected server from the network to prevent further data exfiltration.
Answer: (SHOW ANSWER)
The Certified Ethical Hacker (CEH) Incident Response lifecycle begins with Identification, followed by containment, eradication, recovery, and lessons learned. CEH documentation stresses that understanding the scope and nature of an incident is critical before taking disruptive action.
Option A is the correct initial response because it focuses on real-time monitoring and log analysis, which are essential during the identification phase. CEH materials emphasize analyzing logs, authentication failures, and traffic anomalies to confirm whether an incident has occurred and determine the attacker's techniques, persistence level, and impact.
Option B, while valuable, is more appropriate after initial identification. Conducting deep outbound traffic audits without first understanding the attack vector can delay containment decisions.
Option C is premature. CEH warns that changing credentials too early may alert the attacker and cause them to escalate or destroy evidence.
Option D represents a containment strategy, not an initial response. CEH guidelines advise against immediately disconnecting systems unless there is confirmed active data exfiltration that cannot be otherwise controlled, as this may disrupt business operations and erase volatile forensic evidence.
Therefore, the CEH-approved approach is to monitor, analyze, and identify the incident before moving to containment and eradication.

NEW QUESTION: 186
An Android device has an unpatched permission-handling flaw and updated antivirus. What is the most effective undetected exploitation approach?
A. SMS phishing
B. Rootkit installation
C. Custom exploit with obfuscation
D. Metasploit payload
Answer: (SHOW ANSWER)
CEH v13 explains that mobile antivirus solutions rely heavily on signatures and known exploit patterns. A custom exploit using obfuscation is far more likely to evade detection.

Metasploit payloads and rootkits are commonly flagged, and SMS phishing relies on user interaction.
Therefore, custom obfuscated exploit code is the most stealthy and effective method.

NEW QUESTION: 187
You are an ethical hacker at Titan Cyber Defense, hired by BrightWave Publishing in New York City to assess the security of their content management system (CMS). While testing the article search function, you input malformed strings such as multiple single quotes. The application responds with system feedback that unexpectedly reveals the database type and internal query structure, including table and column information.
You use these disclosures to better understand how the backend query is built.
Which of the following methods to detect SQL injection are you employing?
A. Function Testing
B. Testing String
C. Dynamic Testing
D. Fuzz Testing
Answer: B (LEAVE A REPLY)
The correct answer is B. Testing String because the scenario describes a classic SQL injection detection approach where the tester submits special characters and malformed input strings-most notably single quotes (')-to observe how the application processes them and whether it produces database error feedback. In SQL injection discovery, inserting a single quote (or multiple quotes) into a parameter commonly breaks the intended SQL syntax if the input is concatenated into a query without proper validation/escaping or parameterization. When this happens, the backend database often returns error messages that may disclose critical information such as the DBMS type (e.g., MySQL, Microsoft SQL Server, Oracle), query fragments, and sometimes references to table/column names. That is exactly what you observed: "system feedback that unexpectedly reveals the database type and internal query structure." This method is specifically called "testing strings" in CEH-style SQL injection identification: using quote characters, delimiters, comment markers, and other metacharacters to see whether the application is vulnerable and whether errors or abnormal behavior occur. The goal is not to fully exploit the injection immediately, but to confirm whether input is being interpreted as part of an SQL statement and to collect clues that help the tester model the backend query and proceed with safe, authorized validation steps.
Why the other options are less accurate: Function testing is a broader web-testing concept and is not the specific SQLi detection tactic shown. Dynamic testing generally refers to testing an application while it is running to observe behavior, but it does not name this specific SQLi discovery technique. Fuzz testing involves sending large volumes of random or semi-random unexpected inputs to trigger crashes or errors; while multiple quotes could be part of fuzzing, the described method is the targeted, well-known SQLi testing string approach used to elicit informative SQL errors.

Therefore, the method being employed is Testing String.

NEW QUESTION: 188
You perform a FIN scan and observe that many ports do not respond to FIN packets. How should these results be interpreted?
A. Conclude the ports are closed
B. Escalate as an active breach
C. Attribute it to network congestion
D. Suspect firewall filtering and investigate further
Answer: D (LEAVE A REPLY)
According to CEH v13 Network Scanning Techniques, a FIN scan is a stealth scanning method that sends TCP packets with only the FIN flag set. Its behavior relies on RFC 793, which specifies that closed ports must respond with a TCP RST, while open ports should silently drop the packet.
However, modern firewalls, IDS/IPS systems, and hardened TCP/IP stacks often filter or silently drop FIN packets regardless of port state. Therefore, when a FIN scan results in no response from a large number of ports, it does not conclusively indicate that the ports are open. Instead, CEH v13 stresses that this behavior commonly points to packet filtering by firewalls or security controls.
Option A is incorrect because a lack of response does not definitively mean ports are closed. Option B is an overreaction; stealth scan anomalies alone do not indicate a breach. Option C is unlikely because congestion would impact multiple protocols, not selectively suppress FIN responses.
CEH v13 recommends that when FIN scans produce ambiguous results, analysts should correlate findings using additional scan types (such as SYN scans) and investigate firewall rules and filtering behavior. Thus, option D is the most accurate interpretation and aligns with CEH guidance.

NEW QUESTION: 189
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: 190
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: (SHOW ANSWER)
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: 191
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: 192
During testing against a network protected by a signature-based IDS, the tester notices that standard scans are blocked. To evade detection, the tester sends TCP headers split into multiple small IP fragments so the IDS cannot reassemble or interpret them, but the destination host can. What technique is being used?
A. IP decoying with randomized address positions
B. SYN scan with spoofed MAC address
C. Packet crafting with randomized window size
D. Packet fragmentation to bypass filtering logic
Answer: D (LEAVE A REPLY)
CEH v13 details that fragmentation attacks are a common IDS evasion strategy. Signature-based IDS systems depend on reassembling packets to detect malicious patterns. When attackers fragment TCP headers into smaller segments, the IDS may be unable to reconstruct the original packet sequence, especially if the fragments are intentionally crafted to confuse reassembly buffers. Meanwhile, the target host typically recombines the fragments correctly, allowing the scan or payload to pass undetected. This technique is specifically discussed under IDS evasion methods, where fragmentation prevents complete packet inspection.

Options A and B describe unrelated evasion mechanisms such as IP spoofing and MAC spoofing, and Option C does not fundamentally affect IDS reconstruction. The tester is clearly using packet fragmentation to evade detection while still mapping open ports successfully.

NEW QUESTION: 193
During a security penetration test at ABC Financial Services in Miami, Florida, on July 9, 2025, ethical hacker Javier Morales targets the company's online banking portal to assess its resilience. Over several hours, the portal's web server begins to falter, with legitimate users reporting inability to log in or complete transactions. The IT team notices the server is struggling to accept new connections, as its maximum connection limit is nearly reached, despite no significant spike in overall network traffic. Javier's controlled test, run from a secure system, logs interactions to simulate a real attack, aiming to evaluate the IT team's ability to identify the threat.
What DoS or DDoS attack technique is Javier's exercise primarily simulating?
A. Slowloris Attack
B. UDP Flood Attack
C. Peer-to-Peer Attack
D. SYN Flood Attack
Answer: A (LEAVE A REPLY)
The symptoms point directly to a Slowloris attack, which CEH materials classify as an application-layer denial-of-service technique that targets web servers by exhausting their available concurrent connection slots rather than saturating bandwidth. In a Slowloris attack, the attacker opens many HTTP or HTTPS connections to the server and then keeps them alive as long as possible by sending partial, incomplete HTTP requests or very slow header transmissions at timed intervals. Because the requests are never fully completed, the server keeps the connections open, waiting for the remainder of the request. Over time, the server's maximum connection limit is consumed, and legitimate users cannot establish new sessions, even though overall network traffic may remain relatively low.
That exact pattern is described in the scenario: the server is "struggling to accept new connections," the
"maximum connection limit is nearly reached," and there is "no significant spike in overall network traffic." This is a classic indicator of low-and-slow DoS behavior, which can be harder to detect because it does not resemble a high-volume flood.
A SYN Flood attack can also exhaust connection resources, but it typically creates a large number of half- open TCP connections and is usually more apparent in network-level telemetry and SYN backlog behavior. A UDP Flood generally causes a noticeable traffic spike. "Peer-to-Peer Attack" describes a botnet architecture style, not the specific technique used here. Therefore, the attack being simulated is Slowloris.

NEW QUESTION: 194
A technology consulting firm in Denver, Colorado, recently experienced a wave of suspicious account compromise incidents. Several employees reported receiving an email that appeared identical to a legitimate cloud storage notification they had received earlier that week. The message reused the original branding, formatting, sender display name, and subject line. However, it informed recipients that the previously shared document had been "updated due to synchronization errors" and instructed them to reauthenticate using the embedded link. The link directed users to a convincing replica of the organization's authentication portal.
Investigation revealed that the attacker had reused content from a genuine prior communication and modified only the embedded hyperlink. Which type of social engineering attack does this scenario most accurately represent?
A. Clone Phishing
B. Consent Phishing
C. Search Engine Phishing
D. Tabnabbing
Answer: A (LEAVE A REPLY)
The correct answer is Clone Phishing. CEH social engineering material explains that clone phishing occurs when an attacker takes a legitimate message previously received by the victim, duplicates its appearance and content, and modifies a malicious element such as a link or attachment. That matches this scenario exactly:
the attacker reused genuine branding, the original format, sender display style, and subject line, then changed the embedded hyperlink so users would reauthenticate on a fake portal. Consent phishing is a different cloud- focused technique involving malicious OAuth authorization requests. Search engine phishing relies on manipulating search results so victims voluntarily navigate to a fake site. Tabnabbing involves changing the content of an inactive browser tab to a phishing page. None of those fit as closely as clone phishing. CEH guidance stresses that clone phishing is highly convincing because the message is based on a real prior communication that the victim may remember and trust. Since the attacker preserved almost everything from a legitimate message and altered only the actionable malicious link, the scenario is a textbook example of Clone Phishing.

NEW QUESTION: 195
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: 196
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: 197
A penetration tester is investigating a web server that allows unrestricted file uploads without validating file types. Which technique should be used to exploit this vulnerability and potentially gain control of the server?
A. Perform a SQL injection attack to extract sensitive database information
B. Upload a shell script disguised as an image file to execute commands on the server
C. Conduct a brute-force attack on the server's FTP service to gain access
D. Use a Cross-Site Scripting (XSS) attack to steal user session cookies
Answer: B (LEAVE A REPLY)
CEH teaches that unrestricted file upload vulnerabilities are among the most dangerous in web applications because they allow attackers to bypass extension checks and upload malicious executable files. When the server fails to validate MIME types, file extensions, or execution permissions, an attacker can upload a web shell disguised as a harmless file, such as "image.php.jpg," which may pass superficial validation and still be executed by the server's interpreter. Once executed, the shell provides the attacker with command execution capabilities, allowing full control over the system. CEH emphasizes that web shells can enable privilege escalation, database compromise, lateral movement, or full server takeover. Unlike SQL injection or XSS, file upload exploitation directly affects server-side execution, making it significantly more severe. Unrestricted upload flaws are commonly tested in CEH labs with tools like Burp Suite to alter content-type headers or bypass client-side filters. This is a high-impact vulnerability requiring strict validation and sandboxing controls.

NEW QUESTION: 198
A cybersecurity team at a cloud infrastructure provider in San Jose, California, initiated a structured vulnerability evaluation across its production environment. The scanning process began by identifying communication protocols active on each host. Once the protocols were cataloged, the platform analyzed which services were associated with those ports and dynamically selected only the vulnerability tests relevant to those detected services. The scanning logic adjusted automatically based on discoveries made during execution. Which vulnerability assessment approach is illustrated in this scenario?
A. Inference-Based Assessment
B. Service-Based Solutions

C. Product-Based Solutions
D. Tree-Based Assessment
Answer: A (LEAVE A REPLY)
The correct answer is Inference-Based Assessment. CEH vulnerability assessment material explains that some scanning approaches do not blindly run every possible test against a host. Instead, they infer what checks are appropriate by first identifying protocols, ports, and services, then dynamically selecting tests that are relevant to those discoveries. The scenario describes exactly that behavior: the platform catalogs communication protocols, determines which services are associated with the observed ports, and automatically adjusts the vulnerability tests during execution. This inference-driven logic improves efficiency and reduces unnecessary probing because the scanner tailors its checks to the environment it discovers. Service-based and product- based phrasing may sound plausible, but the question is specifically about the scanning logic and decision model rather than the type of vendor offering. Tree-based assessment does not best describe the sequence presented. CEH guidance uses inference-based assessment to describe scanners that progressively refine their actions using information learned during earlier scanning stages. Because the selection of tests depends on discovered service characteristics and adapts as the scan proceeds, Inference-Based Assessment is the most accurate answer.

NEW QUESTION: 199
One customer's malicious activity impacts other tenants. Which control would best prevent this?
A. Strong encryption
B. Secure log management
C. Multi-tenant isolation
D. Strong authentication
Answer: C (LEAVE A REPLY)
In CEH v13 Cloud Computing, multi-tenancy is a core cloud characteristic-but also a major risk if isolation controls are weak. When one tenant's actions affect others, the issue is almost always insufficient isolation between tenants.
Multi-tenant isolation ensures that compute, storage, memory, and network resources are strictly separated.
Without proper isolation, a malicious tenant can:
Exhaust shared resources
Access neighboring virtual machines
Damage the provider's reputation
Encryption and authentication protect data access but do not stop cross-tenant impact.
Logging helps detect incidents but does not prevent them.

CEH v13 emphasizes strong logical isolation mechanisms-such as hypervisor hardening and tenant segmentation-as essential cloud security controls. Therefore, Option C is the correct answer.

NEW QUESTION: 200
Which technique best exploits session management despite MFA, encrypted cookies, and WAFs?
A. CSRF
B. Side jacking
C. Session fixation
D. Insecure deserialization
Answer: (SHOW ANSWER)
CEH v13 emphasizes that insecure deserialization is one of the most dangerous application vulnerabilities because it can lead to arbitrary code execution, bypassing authentication, authorization, and session protections entirely.
Even with MFA, encrypted cookies, and WAFs, deserialization flaws allow attackers to manipulate serialized objects used in session handling. When deserialized without validation, these objects may execute attacker- controlled code.
CSRF relies on authenticated users. Side jacking is mitigated by encryption. Session fixation is ineffective if session regeneration and MFA are implemented. Insecure deserialization, however, attacks the application logic itself, making it the most effective option.
Thus, Option D is correct.

NEW QUESTION: 201
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: 202
You are Emma Rodriguez, an ethical hacker at SecurePath Solutions, hired to test the mobile application security of Sterling & Associates, a law firm in New York City. During a covert assessment, your objective is to simulate an attacker attempting to exploit vulnerabilities in the firm's client case management app. You discover that the app stores user credentials in plain text on the device, enabling you to extract sensitive client login information using a rooted device. Based on this finding, which OWASP Top 10 Mobile Risk are you identifying in the app?
A. Insecure Communication
B. Improper Credential Usage
C. Inadequate Privacy Controls
D. Insecure Data Storage
Answer: (SHOW ANSWER)
The finding described maps directly to Insecure Data Storage. In CEH-aligned mobile security guidance and OWASP Mobile risk discussions, insecure data storage occurs when a mobile application saves sensitive information locally in a way that can be easily recovered by an attacker, especially on a rooted or jailbroken device where sandbox protections can be bypassed. Storing usernames and passwords in plain text is a high-severity example because it allows immediate account takeover and enables access to protected client records, case notes, and other confidential material.
Mobile devices routinely store app data in local file systems, shared preferences, databases, logs, or cached content. If sensitive data is stored without proper protections, an attacker with physical access, malware, backup extraction capability, or root access can read it directly. CEH materials emphasize that rooting dramatically increases attacker capability by permitting access to app directories and system areas that would otherwise be restricted. That is exactly what the scenario shows: credentials are recovered from the device once root access is available.
The best practice mitigation is to never store credentials in plain text. Use secure, OS-provided storage such as Android Keystore or iOS Keychain, apply strong encryption with keys protected by hardware-backed mechanisms when available, minimize what is stored locally, and ensure secrets are not written to logs or debug artifacts. Insecure Communication would involve weak transport protections, and Improper Credential Usage can include hardcoded credentials or poor authentication handling, but the specific issue here is plainly unsafe local storage of credentials, so Insecure Data Storage is the correct choice.

NEW QUESTION: 203

A competing technology firm begins releasing products that closely mirror the design, pricing strategy, and feature roadmap of ApexDynamics Inc. An internal review reveals that detailed information about ApexDynamics ' s upcoming initiatives had been gradually collected through publicly available sources and external disclosures before product launch. Which footprinting-related threat does this scenario best represent?

A. Corporate Espionage

B. Business Loss

C. Information Leakage

D. Social Engineering

Answer: A (LEAVE A REPLY)

The best answer is Corporate Espionage. CEH reconnaissance coverage explains that footprinting can be used not only for technical attack preparation but also for competitive intelligence gathering against organizations.

In this scenario, a rival company appears to have derived meaningful strategic information about product design, pricing, and roadmap decisions from publicly available data and external disclosures before launch.

The resulting harm is not just accidental exposure in the abstract; it is the use of collected intelligence to gain a business advantage over the target organization. That makes corporate espionage the most accurate classification. Information leakage is certainly part of the pathway, because some information had to be exposed or inferable from public sources, but the threat asked for is the footprinting-related consequence represented by the competitor's behavior. Business loss describes an impact, not the threat category itself. Social engineering would require manipulative interaction with people, which is not stated here. CEH materials note that careless public disclosures, metadata, career postings, partner information, and strategic announcements can all support footprinting by competitors or adversaries. When such data is systematically collected to mirror or undermine business strategy, the activity is best described as corporate espionage.

NEW QUESTION: 204

Cyber experts conducting covert missions exclusively for national interests are best classified as:

A. State-sponsored hackers

B. Organized hackers

C. Gray hat hackers

D. Hacktivists

Answer: A (LEAVE A REPLY)

CEH v13 classifies state-sponsored hackers as highly skilled professionals who operate under government direction to conduct espionage, intelligence gathering, sabotage, or cyber warfare. These attackers often target foreign governments, critical infrastructure, and strategic industries.

The defining characteristics are:

Government backing
National or geopolitical objectives
Advanced resources and long-term campaigns
Options B, C, and D do not fit. Organized hackers are typically financially motivated cybercriminal groups.
Gray hats operate without authorization but not for national interests. Hacktivists pursue ideological or political causes independently.
CEH v13 explicitly associates covert intelligence operations with state-sponsored actors, making Option A correct.

NEW QUESTION: 205
During a penetration test at a healthcare provider in Phoenix, ethical hacker Sofia crafts a stream of IP packets with manipulated offset fields and overlapping payload offsets so that the records server ' s protocol stack repeatedly attempts to reconstruct the original datagrams. The repeated reconstruction attempts consume CPU and memory, causing the system to crash intermittently and disrupt patient portal access, even though overall bandwidth remains normal. Packet analysis shows deliberately malformed offsets that trigger processing errors rather than a simple flood of traffic.
Which type of attack is Sofia most likely simulating?
A. Fragmentation Attack
B. ICMP Flood
C. Teardrop Attack
D. Ping of Death
Answer: C (LEAVE A REPLY)
This scenario matches a Teardrop attack, which exploits IP fragmentation reassembly weaknesses by sending fragments with overlapping or inconsistent offset fields. In a teardrop attack, the attacker crafts IP fragments so that when the target attempts to reassemble them into the original datagram, the fragment offsets and sizes do not align correctly (often overlapping). Vulnerable systems can experience errors in the reassembly process, leading to CPU/memory exhaustion, crashes, or instability in the network stack.
The question highlights "manipulated offset fields and overlapping payload offsets," "repeated attempts to reconstruct," and
"deliberately malformed offsets that trigger processing errors rather than a simple flood," which are all core teardrop characteristics.
The impact described-system crashes and service disruption without abnormal bandwidth usage-also fits.
This is not a volumetric DoS (like ICMP flood); it's a malformed-packet attack that targets protocol stack processing. The key is that the attacker is exploiting how the target handles fragmented packets, causing excessive processing and failure during reassembly.
Why the other options are less accurate:

Fragmentation attack (A) is a broader category and could include many fragmentation-based manipulations, but "overlapping offsets causing reassembly failure" is the classic teardrop pattern.
ICMP flood (B) is bandwidth/packet-rate driven and does not involve IP fragment offset manipulation.
Ping of Death (D) involves oversized ICMP packets (often via fragmentation) exceeding maximum IP size, causing crashes on vulnerable stacks; the scenario instead emphasizes overlapping offsets and reassembly logic errors rather than oversized packet size.
Therefore, Sofia is most likely simulating C. Teardrop Attack.

NEW QUESTION: 206
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: 207
You are Noah Kim, an ethical hacker at Quantum Cyber Solutions, hired to test the mobile device security of TechTrend Innovations, a tech firm in Austin, Texas. During a covert assessment, your objective is to simulate an attacker attempting to gain privileged access to an iPhone 12 running iOS 14.5 used for proprietary app development. You apply a jailbreaking technique that allows the device to fully restart without requiring a computer,

maintaining a patched kernel and enabling access to sensitive app data in the file system. Based on this method, which iOS jailbreaking technique are you using?

A. Semi-tethered jailbreaking

B. Untethered jailbreaking

C. Semi-untethered jailbreaking

D. Tethered jailbreaking

Answer: B (LEAVE A REPLY)

Untethered jailbreaking is the only option that matches all key characteristics described: the device can reboot normally without needing a computer, and the jailbreak remains active after the restart with kernel-level modifications still in effect. In CEH-aligned mobile security concepts, the main difference among jailbreak types is what happens after a reboot.

A tethered jailbreak requires a computer to boot the device at all. If the phone restarts without being connected to a computer, it will not complete the boot process. That contradicts the scenario, which explicitly says the device can fully restart without requiring a computer. A semi-tethered jailbreak allows the phone to reboot without a computer, but it boots into a non-jailbroken state, meaning elevated privileges and kernel patching are not active until re-enabled through a tool. A semi-untethered jailbreak is similar in that it can boot normally without a computer, but the jailbreak does not persist automatically; it typically requires re- activating the jailbreak after each reboot to regain kernel patching and privileged access.

The scenario states the restart occurs while still "maintaining a patched kernel" and continuing access to protected filesystem data, which indicates persistence across reboot. That persistence is the defining feature of an untethered jailbreak. From a defensive and assessment perspective, this is considered higher risk because it provides continuous post-reboot privileged access, increasing the window for data access, tampering, and persistence mechanisms compared with reboot-reset jailbreak states.

NEW QUESTION: 208

During a red team assessment at New England Insurance in Boston, ethical hacker Daniel sends a series of spoofed TCP packets carrying the reset flag to a server hosting client applications. As a result, several active sessions between employees and the server are abruptly terminated, causing temporary disruption of legitimate work. Daniel uses this demonstration to highlight how attackers can forcibly tear down sessions without completing a full hijack.

Which type of network-level session hijacking technique is Daniel simulating?

A. UDP Hijacking

B. RST Hijacking

C. Blind Hijacking

D. TCP/IP Hijacking

Answer: B (LEAVE A REPLY)

The technique described is RST hijacking because the attacker sends spoofed TCP packets with the RST (reset) flag to forcibly terminate established TCP sessions. In TCP, an RST packet is used to immediately abort a connection. If an attacker can craft packets that appear to belong to an existing session (matching the 4- tuple and using plausible sequence/acknowledgment values), the receiving endpoint may accept the reset and tear down the connection. This creates disruption-sessions drop, users are disconnected, and applications experience errors-without the attacker needing to fully take over the session or inject meaningful application data.
The scenario matches this exactly: "spoofed TCP packets carrying the reset flag," followed by "active sessions...abruptly terminated." That is the hallmark outcome of RST-based session disruption. It is often used as a demonstration of how fragile sessions can be when attackers can spoof traffic within a path (or on the same network segment) and when defensive controls do not validate or protect sessions adequately.
Why the other options are incorrect:
UDP hijacking (A) doesn't apply because UDP is connectionless and has no RST flag or session teardown mechanism like TCP.
Blind hijacking (C) refers to injecting traffic without seeing responses (guessing sequence numbers), but the specific mechanism asked here is the reset-flag termination; "blind" could be a property of how it's done, not the named technique.
TCP/IP hijacking (D) is a broader category that includes multiple methods of taking over or manipulating TCP sessions. The question is specifically about using RST packets to kill sessions, which is most precisely called RST hijacking.
Therefore, the correct answer is B. RST Hijacking.

NEW QUESTION: 209
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: 210
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: 211
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: C (LEAVE A REPLY)

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: 212
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: B (LEAVE A REPLY)
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: 213
Justin Fletcher is conducting an authorized assessment for EverSafe Technologies in Las Vegas. During the active reconnaissance phase, he interacts directly with the organization ' s infrastructure to retrieve structural details about how its public-facing systems are logically organized. His activity generates entries within the target environment ' s monitoring systems. Which type of active footprinting technique is Justin performing?
A. Network/port scanning
B. DNS interrogation
C. Social engineering
D. User and service enumeration
Answer: B (LEAVE A REPLY)
The correct answer is DNS interrogation. CEH reconnaissance guidance explains that active footprinting involves direct interaction with the target environment, which can generate logs or alerts. DNS interrogation is an active technique used to query name servers for information about domain structure, hostnames, mail servers, subdomains, and other records that reveal how public-facing systems are logically arranged. The question specifically says Justin is retrieving structural details about the organization's public-facing systems and that his activity is logged by the target, which is consistent with active DNS queries. Network or port scanning is also active, but it focuses on discovering open ports and reachable services rather than the logical naming and organizational structure of public systems. Social engineering is human-focused, and user and service enumeration typically aims at accounts or system services rather than domain structure. CEH materials repeatedly emphasize DNS as a rich reconnaissance source because records such as A, MX, NS, TXT, and SOA can reveal infrastructure relationships and naming conventions.

Since the goal is to understand how the organization's internet-facing systems are organized and represented, DNS interrogation is the best fit.

NEW QUESTION: 214
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: 215
At a digital marketing firm in Atlanta, Georgia, employees began reporting that access to a widely used cloud collaboration portal was intermittently redirecting them to a counterfeit interface hosted on an unfamiliar IP address. Security engineers observed that when multiple users across different departments attempted to access the legitimate domain, they consistently received the same incorrect IP resolution. The anomalous behavior persisted across sessions and affected numerous internal clients until the organization ' s name resolution service was restarted, after which normal resolution resumed. What DNS manipulation technique best explains this scenario?
A. Performing Intranet DNS Spoofing within the local network
B. Injecting malicious records through DNS Cache Poisoning
C. Executing Proxy Server DNS Poisoning to alter resolution paths
D. Conducting Internet DNS Spoofing from a remote network
Answer: (SHOW ANSWER)
The correct answer is DNS Cache Poisoning. CEH network security material explains that cache poisoning occurs when a DNS server is tricked into storing fraudulent name-to-IP mappings in its cache. Once the poisoned entry is cached, many users querying that DNS service receive the same false resolution until the cache is flushed, expires, or the service is restarted. That maps directly to the scenario: multiple internal clients receive the same incorrect IP address for a legitimate domain, and the issue disappears after the organization's name resolution service is restarted. Intranet DNS spoofing typically involves local interception and very fast forged replies on a LAN, while proxy server DNS poisoning changes browser-side proxy behavior, and internet DNS spoofing usually

involves altering a host's DNS configuration or redirecting it to a malicious resolver. The persistence across many users and the recovery after DNS service restart are the most important clues, because they indicate poisoned cached records on the resolver itself rather than isolated endpoint tampering. CEH guidance highlights that DNS cache poisoning can silently redirect users to counterfeit systems while appearing to resolve legitimate domain names normally.

NEW QUESTION: 216
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: 217
At TechTrend Innovations in Silicon Valley, network administrator Jake Henderson reviews the configuration of their web infrastructure. While inspecting the web server setup, he identifies the directory that stores the publicly accessible website content such as HTML files, images, and client-side scripts. Jake highlights this area as a frequent target for attackers, since improper permissions could expose sensitive files to unauthorized users.
Which web server component is Jake analyzing in this scenario?
A. Application Server
B. Document Root
C. HTTP Server (Core)
D. Virtual Document Tree
Answer: B (LEAVE A REPLY)
The directory that contains the publicly accessible web content-including HTML pages, images, JavaScript, CSS, and other client-side assets-is known as the Document Root. This is the base filesystem path that a web server maps to the "/" location of a website. When a user requests a resource (for example, https://site.
com/index.html), the web server typically resolves that URL path to a file under the configured document root and then serves it to the client (subject to access controls and server configuration).
The scenario's details match this precisely: Jake identifies "the directory that stores the publicly accessible website content," and notes that it is a frequent attacker target due to risks from improper permissions.
Document root security is critical because overly permissive read or browse access can expose files that were never intended to be public-such as backups, configuration files, temporary files, source code archives, or sensitive data accidentally placed in web-accessible paths. Misconfigurations can also enable directory listing, allowing attackers to enumerate and retrieve files directly. Attackers often probe for common filenames (e.g., old .zip backups, .bak files, exposed .env files, or test pages) precisely because document root is where such mistakes become externally reachable.
Why the other options are less accurate:
An Application Server (A) runs server-side application logic (e.g., Java/.NET app containers) and is not specifically the directory of static public web content.
The HTTP Server (Core) (C) refers to the web server software/service handling HTTP requests, not the content directory itself.

A Virtual Document Tree (D) describes the logical structure mapping URLs to resources (sometimes via aliases and virtual hosts), but the question asks for the directory that stores the publicly accessible content- this is the document root.
Therefore, Jake is analyzing B. Document Root.

NEW QUESTION: 218
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: 219
A penetration tester observes that traceroutes to various internal devices always show 10.10.10.1 as the second-to-last hop, regardless of the destination subnet. What does this pattern most likely indicate?
A. DNS poisoning at the local resolver used by the compromised host
B. Loopback misconfiguration at the destination endpoints
C. A core router facilitating communication across multiple internal subnets
D. Presence of a transparent proxy device acting as a forwarder
Answer: C (LEAVE A REPLY)

CEH v13 highlights the importance of route tracing during internal reconnaissance to identify key infrastructure devices such as distribution switches, firewalls, and core routers. When a single IP address consistently appears as the penultimate hop across multiple network paths, this typically indicates that the device serves as a core router responsible for inter-VLAN or inter-subnet routing. Core routers aggregate traffic from various segments before forwarding to endpoint subnets, explaining why it appears before diverse destinations. CEH emphasizes recognizing core infrastructure because compromising such devices provides attackers with significant visibility and potential control over network-wide communications. DNS poisoning would affect name resolution, not hop patterns. Loopback misconfigurations would affect single hosts, not multiple segments. A transparent proxy would appear only for traffic routed through application-layer inspection, not all traceroute tests. The consistency across subnets strongly points to a centralized routing device.

NEW QUESTION: 220
During an internal audit at a financial services firm in Mumbai, ethical hacker Meera was tasked with assessing lateral movement risks within the Windows-based domain environment. While monitoring internal network traffic, she noticed a strange broadcast from a workstation trying to resolve a non-existent host.
Suspecting protocol-level weakness, she responded swiftly using a pre-configured system. A few minutes later, she captured NTLMv2 hashes from several authenticated sessions across multiple departments. Later, her team successfully cracked one of the hashes offline and used the credentials to gain access to a sensitive internal reporting server.
Which type of attack did Meera most likely execute?
A. Internal Monologue Attack
B. LLMNR/NBT-NS Poisoning
C. Kerberoasting
D. Pass-the-Ticket Attack
Answer: (SHOW ANSWER)
The correct answer is LLMNR/NBT-NS Poisoning. CEH system hacking coverage explains that when a Windows host cannot resolve a name through normal DNS, it may fall back to Link-Local Multicast Name Resolution or NetBIOS Name Service. An attacker on the local network can answer those broadcasts and falsely claim to be the requested resource. If the victim then attempts authentication, NTLM or NTLMv2 challenge-response data can be captured and later cracked offline. That is exactly what this question describes: a non-existent host lookup, a quick malicious response, capture of NTLMv2 hashes, and later credential cracking. Kerberoasting targets service tickets in Active Directory, not broadcast name resolution.
Pass-the-Ticket involves Kerberos tickets, and Internal Monologue abuse is a different authentication abuse pattern. CEH materials specifically connect LLMNR/NBT-NS poisoning with tools such as Responder and highlight that these protocols can be abused

to collect hashes for lateral movement or privilege escalation. The scenario's sequence of name-resolution spoofing followed by hash capture is the defining signature of an LLMNR/NBT-NS poisoning attack.

NEW QUESTION: 221
A penetration tester identifies malware on a system that hides its presence and gives an attacker access to administrative functions without being detected. What type of malware is this?
A. Virus
B. Keylogger
C. Ransomware
D. Rootkit
Answer: (SHOW ANSWER)
CEH courseware describes rootkits as specialized malware designed to conceal their presence while providing persistent, unauthorized access to system-level functions. Rootkits typically modify low-level components of the operating system-such as kernel modules, drivers, or system processes-to hide files, processes, registry keys, and network connections. Their primary purpose is to grant attackers administrative privileges without triggering alerts, making them extremely stealthy and dangerous. CEH emphasizes that rootkits often accompany other malware to maintain long-term control after initial compromise. In contrast, viruses replicate by attaching to files, keyloggers record keystrokes but do not hide system-level access, and ransomware encrypts data rather than conceals operations. The defining characteristics in this scenario- cloaking activity, providing admin-level control, persisting undetected-are directly aligned with rootkit behavior as described in CEH training material.

NEW QUESTION: 222
An energy infrastructure company in Tulsa, Oklahoma initiated a controlled phishing simulation targeting multiple operational departments. The test email claimed to originate from the corporate compliance office and instructed employees to "complete a mandatory regulatory update within the next 30 minutes to avoid account suspension." The message used a broad salutation instead of employee names and lacked the standard corporate signature footer normally appended to official communications. Additionally, security analysts observed that the embedded hyperlink displayed the organization ' s domain in the message body; however, when examined more closely, the actual destination resolved to a shortened external URL redirecting to an unrelated host. From a defensive analysis standpoint, which indicator provides the strongest technical validation that the message is malicious?
A. AThe strongest technical indicator is the hover mismatch URL. CEH social engineering and email- phishing guidance treats deceptive links as one of the clearest validation points because the visible text shown to the user can be made to look trustworthy while the actual

hyperlink target leads somewhere completely different. In this scenario, the email imitates an internal compliance notice and uses urgency, generic greetings, and a missing corporate signature, all of which are suspicious. However, those signals are still contextual and behavioral. The most technically reliable evidence is that the displayed organization domain does not match the true destination, which resolves through a shortened external URL to an unrelated host. CEH materials consistently explain that phishing messages frequently redirect victims to fake login pages or malicious sites through disguised links, and verifying the real destination is a core defensive step. This is more conclusive than style-based clues because branding mistakes or greetings alone may vary in legitimate communications. A mismatch between displayed and actual URL directly shows intentional deception in message construction, making it the best technical validation that the message is malicious.

B. Absence of a formal corporate signature

C. Use of generic greetings rather than individualized addressing

D. Identification of Hover Mismatch URLs in the embedded link

E. Presence of aggressive urgency language

Answer: A,B,C,D,E (LEAVE A REPLY)

NEW QUESTION: 223

As a Certified Ethical Hacker evaluating a smart city project (traffic lights, public Wi-Fi, and water management), you find anomalous IoT network logs showing high-volume data exchange between a specific traffic light and an external IP address. Further investigation reveals an unexpectedly open port on that traffic light. What should be your subsequent course of action?

A. Isolate the affected traffic light from the network and perform a detailed firmware investigation

B. Conduct an exhaustive penetration test across the entire network to uncover hidden vulnerabilities

C. Analyze and modify IoT firewall rules to block further interaction with the suspicious external IP

D. Attempt to orchestrate a reverse connection from the traffic light to the external IP to understand the transferred data

Answer: A (LEAVE A REPLY)

CEH's approach to suspected compromise aligns with an incident-handling mindset: containment first, then analysis and remediation. In IoT and OT-adjacent environments (smart city infrastructure, SCADA-like components, embedded controllers), CEH emphasizes that suspicious external communications and unexplained open ports may indicate compromise, misconfiguration, exposed management services, or implanted malware/backdoors. Because IoT endpoints often have limited logging and are difficult to reimage safely, the safest next step is to isolate the suspected device to prevent further data exfiltration, command-and- control activity, or lateral movement to other city systems.

Option A best matches CEH guidance: isolate the device and investigate its firmware, services, and configuration, including checking for unauthorized binaries, altered firmware images, insecure default services, and hardcoded credentials. This also preserves evidence and reduces the blast radius.
Option C (blocking the external IP) can be helpful, but it's a partial control: attackers can rotate infrastructure, and the device could still be compromised internally. Option B (full network pen test) is too broad and delays containment when a specific high-risk indicator is already present. Option D (attempting a reverse connection) crosses into active exploitation behavior and is not an appropriate "next step" in a defensive investigation; CEH methodology stresses authorized, controlled testing and prioritizes risk reduction over interacting with suspicious external hosts.
Thus, CEH-aligned best practice is immediate isolation and firmware-level investigation.

NEW QUESTION: 224
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: 225
During a penetration test at a logistics company in Atlanta, Georgia, you examine the configuration of network devices and discover that they rely on legacy communication mechanisms lacking encryption and integrity checks. These mechanisms allow

neighboring systems to exchange operational data without verification, exposing the infrastructure to potential manipulation. What type of vulnerability is most clearly present?

A. Firewall vulnerabilities

B. Lack of password protection

C. Lack of authentication

D. Insecure routing protocols

Answer: D (LEAVE A REPLY)

The best answer is D. Insecure routing protocols because the scenario describes legacy neighbor-to-neighbor device communications that lack encryption and integrity validation, allowing operational routing data to be exchanged without verification. In CEH-aligned network hacking concepts, this is a classic weakness of older or improperly secured routing protocols (and related network control-plane exchanges) where routers trust updates from neighbors and do not cryptographically validate the authenticity and integrity of routing information.

When routing updates are accepted without strong verification, an attacker who can position themselves on the same segment (or spoof a trusted neighbor) may inject or manipulate routing information. This can enable attacks such as route injection, route poisoning, man-in-the-middle (MITM) traffic redirection, blackholing traffic, or causing instability/denial of service by continuously advertising bad routes. The mention of "neighboring systems" and "operational data" strongly maps to routing adjacencies where devices exchange reachability and topology information. The absence of integrity checks makes it feasible to alter routing messages in transit or forge them, and the absence of encryption can expose routing details that further assists reconnaissance and targeted manipulation.

Why the other options are less accurate:

Firewall vulnerabilities relate to filtering and policy enforcement, but the core issue here is the trust model and protection of routing/control messages, not firewall rule flaws.

Lack of password protection is too generic and typically refers to weak/no credentials on management access, not unauthenticated routing exchanges.

Lack of authentication is conceptually related, but the question asks for the type of vulnerability most clearly present given "legacy communication mechanisms" between neighbors carrying operational data-this is most specifically categorized in CEH terms as insecure routing protocols (i.e., routing updates lacking authentication/integrity and sometimes encryption).

In practice, organizations mitigate this by enabling routing protocol authentication (where supported), using cryptographic integrity protections, restricting routing adjacencies, and segmenting or filtering routing/control- plane traffic to trusted peers only.

NEW QUESTION: 226

Which information CANNOT be directly obtained from DNS interrogation?

A. Usernames and passwords

B. Server geolocation (via IPs)
C. Subdomains of the organization
D. IP addresses of mail servers
Answer: A (LEAVE A REPLY)
DNS interrogation is a core passive and semi-active reconnaissance technique described in CEH v13 Reconnaissance Techniques. It allows ethical hackers to gather publicly available information about a target's domain infrastructure.
Through DNS queries, testers can retrieve:
Subdomains (via zone transfers, brute force, or DNS records)
Mail server IP addresses (via MX records)
Server IP addresses, which can then be mapped to approximate geographic locations
However, DNS does not store authentication credentials such as usernames and passwords. That information resides in authentication systems like Active Directory, LDAP, or application databases, not DNS.
Therefore, Option A is the only choice that cannot be obtained via DNS interrogation. CEH v13 clearly distinguishes between naming infrastructure data and credential-based information, reinforcing why DNS enumeration cannot reveal user credentials.
Thus, Option A is correct.

NEW QUESTION: 227
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: (SHOW ANSWER)

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: 228

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: 229
You are part of the red team assigned to evaluate the physical and social vulnerabilities of a government contractor ' s office located in a metropolitan business hub. During your pretexting phase, you decide to simulate the role of a third-party IT technician. Upon arrival, the receptionist allows you entry without verifying credentials, assuming you ' re there for scheduled printer maintenance. While moving through the workspace, you casually observe open terminals, unattended printouts, and discarded sticky notes at workstations. You later report several user credentials and partial access details acquired during this visit.
Which social engineering technique does this scenario best illustrate?
A. Shoulder Surfing
B. Eavesdropping
C. Impersonation
D. Dumpster Diving
Answer: C (LEAVE A REPLY)
This scenario best illustrates impersonation, which is a core social engineering technique emphasized in CEH under pretexting and physical security testing. Impersonation occurs when an attacker assumes a believable identity, such as an IT technician, vendor, maintenance worker, or delivery person, to gain trust and bypass access controls. In the prompt, the red team member adopts a third-party IT technician role and is granted entry because the receptionist assumes the visit is legitimate and does not verify credentials. That is the defining moment of impersonation: exploiting human trust and procedural gaps to obtain unauthorized physical access.

While the attacker later observes open terminals, unattended printouts, and sticky notes, those observations are opportunistic data collection that becomes possible only after successful impersonation. Shoulder surfing is specifically observing a user entering credentials or viewing a screen while standing nearby, typically during active use. Eavesdropping focuses on capturing spoken or transmitted information, such as listening to conversations or intercepting communications. Dumpster diving involves retrieving sensitive information from trash or discarded materials in waste bins, not simply seeing sticky notes left on desks.
CEH guidance highlights that impersonation often succeeds when organizations lack visitor verification, badge enforcement, escort policies, and security awareness training. Controls include validating work orders, requiring government-issued ID, issuing visitor badges, escorting visitors, enforcing clean desk practices, locking workstations, and secure printing to prevent exposure of credentials and sensitive data.

NEW QUESTION: 230
During a security assessment for an e-commerce company in Boston, Massachusetts, your team conducts a reconnaissance phase to identify potential entry points into the organization ' s communication infrastructure.
You focus on gathering details about the systems responsible for handling incoming email traffic, avoiding active network probing, and relying on passive DNS data collection. Given this objective, which DNS record type should you query to extract information about the target's mail server configuration?
A. SOA
B. TXT
C. NS
D. MX
Answer: D (LEAVE A REPLY)
The correct answer is MX. CEH reconnaissance material explains that MX, or Mail Exchange, records identify the mail servers responsible for receiving email for a domain. When a tester wants to understand how an organization handles incoming email traffic, MX records are the most relevant DNS data source because they reveal the designated mail infrastructure and often the priority order of mail servers. In this scenario, the objective is to gather passive intelligence about communication infrastructure without performing active network probing, so querying DNS records is appropriate. SOA records provide domain authority and zone administration information, TXT records often contain verification or policy-related text such as SPF details, and NS records identify authoritative name servers. While those can all contribute to broader reconnaissance, they do not directly answer which systems are responsible for receiving mail. CEH emphasizes that MX records are commonly used during footprinting to identify email infrastructure, support phishing simulations, analyze third-party mail providers, or map communication dependencies.

Because the question explicitly asks for the DNS record type that reveals mail server configuration, MX is the correct choice.

NEW QUESTION: 231
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: 232
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: 233
During a security penetration test at Sterling Manufacturing in Cleveland, Ohio, the ethical hacking team evaluates the company ' s physical security controls. On a chilly evening in July 2025, ethical hacker Priya Desai, posing as a facilities contractor, accesses the company ' s loading dock area after regular business hours. Behind the employee entrance, she comes across an unsecured maintenance container with discarded packaging, shipping labels, and shredded office material. Among the clutter, Priya retrieves a crumpled document listing temporary access codes for the employee break room, along with a partially shredded memo referencing an upcoming audit. The exercise tests whether sensitive information discarded improperly can be exploited. The next day, Priya uses the recovered access codes to enter the break room undetected during a shift change, logging her entry on a controlled test system to simulate a breach.
What social engineering technique is Priya ' s exercise primarily simulating?
A. Tailgating
B. Eavesdropping
C. Dumpster Diving
D. Shoulder Surfing
Answer: C (LEAVE A REPLY)
This scenario primarily simulates dumpster diving because the key action involves retrieving sensitive information from discarded materials and then using it to gain access. In CEH social engineering coverage, dumpster diving is a physical information-gathering technique where an attacker searches trash, recycling bins, unsecured disposal containers, or shredding waste to find documents and artifacts that can be exploited. Common targets include access codes, employee directories, printed emails, shipping labels, invoices, internal memos, and partially shredded documents-exactly what Priya finds in the unsecured maintenance container.
The question even emphasizes "discarded packaging," "shipping labels," "shredded office material," and a
"crumpled document listing temporary access codes," which are classic dumpster-diving indicators.
The later use of recovered access codes to enter the break room is the impact of the dumpster-diving phase, but the primary social engineering technique tested is how improper disposal leads to compromise. Tailgating would involve following an authorized person through a secure door without proper authentication.
Eavesdropping refers to listening in on conversations or communications to capture sensitive information.

Shoulder surfing involves visually observing someone's screen or keyboard while they enter credentials or view confidential data. None of those describe the initial method of obtaining the access codes.
CEH-aligned mitigations include enforcing clean-desk and secure disposal policies, using locked disposal bins, shredding sensitive documents properly with secure destruction processes, training staff on handling printed data, and restricting access to loading docks and waste areas. Regular audits of disposal practices and physical security checks reduce the likelihood that attackers can harvest usable access details from trash.

NEW QUESTION: 234
During a red team engagement at a retail company in Atlanta, ethical hacker James crafts a session with the company ' s shopping portal and deliberately shares that session ID with an unsuspecting employee by embedding it in a link. When the employee clicks and logs in, their activity is bound to the attacker ' s pre- assigned session. Later, James retrieves the employee ' s input from that same session to demonstrate the flaw to management.
Which session hijacking technique is James most likely using?
A. Session Donation Attack
B. Session Replay Attack
C. Session Prediction
D. Session Fixation Attack
Answer: D (LEAVE A REPLY)
This scenario is a classic session fixation attack. In session fixation, the attacker sets or "fixes" a known session identifier (session ID) for the victim before the victim authenticates. The attacker then persuades the victim to use that predetermined session-often by embedding the session ID into a URL, link, or cookie setting mechanism. Once the victim logs in, the application incorrectly continues using the same session ID (rather than issuing a new one upon authentication). As a result, the attacker can reuse that known session ID to access the victim's authenticated session context.
The described sequence matches session fixation exactly: James first crafts a session and obtains a session ID, then shares it with the victim via a link, the victim clicks and logs in, and "their activity is bound to the attacker's pre-assigned session." Later, James accesses the session and retrieves the victim's input- demonstrating that authentication was tied to an attacker-controlled session token.
Why the other options do not fit:
Session replay (B) involves capturing a valid session token (e.g., via sniffing, XSS, or leakage) and replaying it, but it does not require pre-setting the token before the victim logs in.
Session prediction (C) is about guessing or calculating valid session IDs due to weak randomness. Here the attacker does not guess; he deliberately provides a session ID he already controls.

"Session donation (A)" is not the standard classification for this well-known web session weakness in CEH- style taxonomy; the described behavior aligns with fixation.
Therefore, the correct answer is D. Session Fixation Attack.

NEW QUESTION: 235
An ethical hacker audits a hospital's wireless network secured with WPA using TKIP and successfully performs packet injection and decryption attacks. Which WPA vulnerability most likely enabled this?
A. Use of weak Initialization Vectors (IVs)
B. Dependence on weak passwords
C. Lack of AES-based encryption
D. Predictable Group Temporal Key (GTK)
Answer: (SHOW ANSWER)
CEH documentation explains that WPA-TKIP was a transitional security protocol and does not use AES encryption, relying instead on RC4-based mechanisms.
The lack of AES-based encryption makes WPA-TKIP vulnerable to injection and replay attacks.
Option C is correct.
Options A applies to WEP.
Option B affects authentication, not TKIP weakness.
Option D is not the primary TKIP flaw.
CEH recommends WPA2/WPA3 with AES.

NEW QUESTION: 236
During an authorized wireless security assessment, an ethical hacker captures traffic between client devices and a corporate access point to evaluate the strength of the implemented encryption mechanism. Packet analysis reveals that before protected data exchange begins, the client and access point complete a structured four-message key negotiation process. Subsequent traffic is encrypted using an AES-based counter mode protocol that integrates message authentication for integrity protection. Based on these observations, identify the wireless encryption standard deployed on the network.
A. WEP
B. WPA
C. WPA2
D. WPA3
Answer: (SHOW ANSWER)
The correct answer is WPA2. CEH wireless security material explains that WPA2 uses AES-based encryption together with CCMP, which provides confidentiality and message integrity protection. The scenario also mentions a structured four-message key negotiation process before protected traffic begins, which aligns with the well-known four-way handshake used in WPA and WPA2 environments. The deciding factor is the encryption

and integrity combination: AES with CCMP is strongly associated with WPA2 in CEH guidance.
WEP is far weaker and based on RC4, while WPA originally relied on TKIP as its hallmark improvement over WEP. WPA3 introduces newer protections and a different exam emphasis, but the classic CEH mapping for four-way handshake plus AES/CCMP is WPA2. CEH references also note that WPA2 was designed to improve enterprise-grade wireless security and that CCMP addresses integrity concerns more effectively than earlier approaches. Because the packet capture shows AES-based counter mode encryption with integrated integrity checks after the handshake sequence, the observed standard is best identified as WPA2.

NEW QUESTION: 237
While analyzing suspicious network activity, you observe a slow, stealthy scanning technique that is difficult to trace back to the attacker. Which scenario best describes the scanning technique being used?
A. The attacker sends FIN packets to infer port states based on responses
B. The attacker uses a "zombie" machine to perform scans, hiding their true identity
C. The attacker performs full TCP connect scans on all ports
D. The attacker sends packets with all TCP flags set
Answer: B (LEAVE A REPLY)
According to the CEH Network Scanning module, Idle Scanning (Zombie Scanning) is one of the most stealthy reconnaissance techniques. In this method, the attacker uses an idle third-party host (zombie) to probe the target indirectly.
Because all scan packets appear to originate from the zombie system, the true attacker remains hidden. CEH highlights that idle scans:
Are extremely stealthy
Generate minimal traffic from the attacker
Make attribution very difficult
Option B is correct.
Option A (FIN scan) is stealthy but still traceable.
Option C is noisy and easily detected.
Option D describes a Xmas scan, which is detectable.
CEH classifies idle scanning as one of the hardest scanning techniques to trace.

NEW QUESTION: 238
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: 239
A penetration tester is assessing a company's HR department for vulnerability to social engineering attacks using knowledge of recruitment and onboarding processes. What is the most effective technique to obtain network access credentials without raising suspicion?
A. Develop a fake social media profile to connect with HR employees and request sensitive information

B. Create a convincing fake onboarding portal that mimics the company's internal systems
C. Send a generic phishing email with a link to a fake HR policy document
D. Conduct a phone call posing as a new employee to request password resets
Answer: B (LEAVE A REPLY)
Social engineering attacks that target business processes are especially effective when they mimic legitimate workflows. CEH learning materials emphasize that attackers often exploit trust relationships and organizational procedures rather than attempting broad or generic phishing methods. In the context of HR operations, onboarding portals are highly trusted and frequently accessed by new employees who expect to enter personal information, submit documents, and receive initial network credentials. By creating a fake onboarding portal that closely resembles the organization's internal system, an attacker can collect credentials without triggering suspicion because the action being requested appears normal and expected. This method leverages procedural familiarity, brand consistency, and the implied authority of HR communications, making it far more effective than generic phishing emails or unsolicited social media messages. Phone calls, while sometimes useful, involve real-time interaction and increase the chance of detection. The fake portal, however, seamlessly integrates into existing processes, making it the most effective and lowest-profile approach for acquiring network credentials.

NEW QUESTION: 240
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: 241
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: 242
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: 243
An IDS generates alerts during normal user activity. What is the most likely cause?
A. Firewall failure
B. IDS outdated
C. Excessive IDS sensitivity causing false positives
D. Users triggering protocols
Answer: C (LEAVE A REPLY)
In CEH v13, IDS effectiveness is closely tied to proper signature tuning and sensitivity thresholds. When IDS alerts are triggered by legitimate user behavior, the most common cause is overly sensitive configuration, resulting in false positives.
False positives occur when normal traffic patterns match intrusion signatures. CEH v13 emphasizes that IDS systems must be calibrated to the organization's baseline traffic profile. Without tuning, IDS logs become noisy and reduce analyst effectiveness.

Firewall issues (Option A) and outdated IDS signatures (Option B) can cause missed detections, not excessive alerts. Users unintentionally triggering protocols (Option D) is not a root cause but a symptom of misconfiguration.
Thus, excessive IDS sensitivity is the correct explanation.

NEW QUESTION: 244
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: 245
During a red team exercise at a technology consulting firm in San Francisco, analyst Evelyn deploys a malicious payload disguised within a software update installer. When the target runs the installer, the main application functions normally, but behind the scenes, additional malware components are silently placed on the system without the user ' s knowledge. These hidden components later activate to establish remote access for the red team.
Which technique was most likely used to deliver the hidden malware?
A. Downloader
B. Wrapper
C. Injector
D. Dropper
Answer: D (LEAVE A REPLY)
The scenario describes a program that appears legitimate (a software update installer that "functions normally") while secretly placing additional malicious components onto the system, which later execute to establish remote access. That is the defining behavior of a dropper. A dropper's primary role is to deliver (drop) malware payloads onto a host-writing files to disk or unpacking embedded components-often while disguising itself as a benign application. The malicious components may then be executed immediately or staged for later activation to reduce suspicion and increase persistence.
This differs from a downloader, which typically contains minimal payload and focuses on contacting a remote server to fetch malware after initial execution. In this case, the description emphasizes that "additional malware components are silently placed on the system," implying the payload is being installed/deposited locally by the initial program rather than primarily downloaded. An injector focuses on injecting code into another running process (process injection) to evade detection or run under another process context; it does not inherently describe the act of placing additional components as separate hidden files. A wrapper is a technique where a malicious program is bound or "wrapped" with a legitimate one so that both run; while wrappers can be used in trojanized installers, the question emphasizes the behind-the-scenes placement of additional components for later activation, which is the classic dropper behavior.
The key indicators are: (1) user executes an installer that appears normal, (2) hidden malware components are deposited without the user's knowledge, and (3) those components later activate for remote access. That chain matches a dropper's purpose: stealthy malware delivery and staging.
Therefore, the correct answer is D. Dropper.

NEW QUESTION: 246
You discover multiple NetBIOS responses during an nbtscan, but only one host returns a <1B> entry. What does this indicate?
A. It is the local system
B. It is a rogue DHCP server
C. It is the domain master browser / Primary Domain Controller (PDC)
D. NetBIOS over TCP/IP is disabled
Answer: C (LEAVE A REPLY)
In CEH v13 Reconnaissance and Enumeration, NetBIOS name suffixes are used to identify the role of systems within a Windows network. The <1B> NetBIOS suffix is particularly significant because it uniquely identifies the Domain Master Browser, which in modern Windows environments corresponds to the Primary Domain Controller (PDC). When an nbtscan is performed, multiple systems may respond with NetBIOS names, but only one system per domain will register the <1B> suffix. This is because the PDC is responsible for maintaining the master browse list and coordinating authentication services across the domain.
Option C is correct because the <1B> entry is explicitly defined in CEH documentation as belonging to the domain controller.
Option A is incorrect because the local system does not advertise <1B>.
Option B is incorrect because DHCP servers use different identifiers and do not register <1B>.
Option D is incorrect because NetBIOS must be enabled for <1B> to appear at all.
CEH v13 highlights identifying <1B> during enumeration as a high-value discovery, since domain controllers are prime targets during privilege escalation and lateral movement phases.

NEW QUESTION: 247
As a Certified Ethical Hacker, you are assessing a corporation's serverless cloud architecture. The organization experienced an attack where a user manipulated a function-as-a-service (FaaS) component to execute malicious commands. The root cause was traced to an insecure third-party API used within a serverless function. What is the most effective countermeasure to strengthen the security posture?
A. Regularly updating serverless functions to reduce vulnerabilities.
B. Using a Cloud Access Security Broker (CASB) to enforce third-party policies.
C. Deploying a Cloud-Native Security Platform (CNSP) for full cloud protection.
D. Implementing function-level permissions and enforcing the principle of least privilege.
Answer: D (LEAVE A REPLY)
The Certified Ethical Hacker (CEH) Cloud Computing module emphasizes that serverless environments rely heavily on granular permission models. Attacks involving compromised APIs often succeed because functions are granted excessive privileges.

Option D is correct because enforcing function-level permissions and the principle of least privilege directly limits what a compromised function can execute. CEH documentation states this is the primary defense against serverless abuse.
Option A is beneficial but reactive.
Option B focuses on SaaS governance rather than FaaS execution control.
Option C provides visibility but does not directly prevent privilege misuse.
CEH highlights identity and access management (IAM) as critical in serverless security.

NEW QUESTION: 248
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: 249
A penetration tester evaluates an industrial control system (ICS) that manages critical infrastructure. The tester discovers that the system uses weak default passwords for remote access. What is the most effective method to exploit this vulnerability?
A. Perform a brute-force attack to guess the system's default passwords
B. Execute a Cross-Site Request Forgery (CSRF) attack to manipulate system settings
C. Conduct a denial-of-service (DoS) attack to disrupt the system temporarily
D. Use the default passwords to gain unauthorized access to the ICS and control system operations

Answer: D (LEAVE A REPLY)
Operational Technology and ICS environments often suffer from misconfigurations such as unchanged factory-default passwords. CEH identifies exploiting default credentials as a direct and effective method because ICS devices frequently lack strong authentication controls. Using these built-in credentials grants immediate unauthorized access to supervisory controls, enabling adversaries to manipulate configurations, disrupt processes, or escalate attacks across critical systems.

NEW QUESTION: 250
During a security assessment in San Francisco, an ethical hacker is tasked with evaluating a network ' s resilience against stealthy reconnaissance attempts. The hacker needs to employ a scanning technique that leverages TCP flags to evade detection by intrusion detection systems, relying on the target ' s response behavior to infer port states without completing a full connection. Which approach best aligns with this strategy, ensuring minimal visibility during the assessment?
A. TCP Connect Scan
B. Network Scanning
C. FIN Scan
D. NULL Scan
Answer: C (LEAVE A REPLY)
A FIN scan is a classic "stealth" TCP scan technique discussed in CEH network scanning methodology.
Unlike a TCP Connect scan, which completes the full three-way handshake and is highly visible in logs, a FIN scan sends a TCP packet with only the FIN flag set to a target port. The scan then interprets the target's response to infer whether the port is open or closed, without establishing a normal TCP session. This matches the scenario's requirement to "infer port states without completing a full connection" and to keep visibility low.
The logic relies on expected TCP behavior defined for many TCP/IP stacks. For a closed port, the target typically responds with an RST packet, indicating there is no service listening. For an open port, many systems do not respond at all to an unexpected FIN packet (because it does not correspond to an existing connection). That "no response" behavior becomes the signal the tester uses to suspect the port may be open or filtered.
CEH emphasizes that because FIN scans do not perform a handshake, they can be less likely to trigger certain basic connection-based logging, and they generate fewer obvious connection events than TCP Connect scans.
Option D, NULL scan, is also a stealth method, but it uses a packet with no flags set. The question specifically highlights leveraging TCP flags and is commonly mapped in CEH-style questions to FIN scanning as the representative "TCP flag stealth scan." Option B is too generic, and option A is the most detectable. Therefore, FIN scan best aligns with the described stealth reconnaissance strategy.

NEW QUESTION: 251
At a federal research agency, cybersecurity officer Nikhil is drafting a vulnerability assessment report. In this section, he documents the scanning methodology used, the information about the targets, the type and scope of scans performed, and the tools involved. He does not yet include specific vulnerabilities or affected assets, as this portion of the report is meant to provide context for how the assessment was conducted.
Which section of the vulnerability assessment report is Nikhil working on?
A. Supporting Information
B. Risk Assessment
C. Assessment Overview
D. Findings
Answer: (SHOW ANSWER)
The described content matches the Assessment Overview section because it focuses on how the vulnerability assessment was executed rather than what was found. An assessment report typically includes a part that explains the methodology and approach used to perform scanning so stakeholders can understand the process, validate coverage, and interpret results correctly. In this scenario, Nikhil is documenting the scanning methodology, target information, type and scope of scans, and the tools used. These elements provide context and transparency about the assessment process, assumptions, and boundaries-exactly what an overview is meant to capture.
This section is also intentionally not listing specific vulnerabilities or affected assets, which further confirms it is not the Findings section. Findings is where the report enumerates discovered vulnerabilities, affected systems, evidence, severity, and recommendations. Similarly, it is not the Risk Assessment section because that portion generally interprets the findings to determine likelihood and impact, prioritizes risks, and may map issues to business impact or compliance requirements. Since Nikhil is only describing the scanning approach and scope, risk analysis is premature and out of place.
Why not Supporting Information? Supporting information usually contains appendices or reference material that supplements the core report-such as raw scan outputs, detailed configuration data, asset inventories, screenshots, logs, tool configurations, or glossary/definitions. While tool names and technical details can appear there, the narrative about methodology, targets, scope, and scan types is more appropriately part of the main body's overview so readers understand the assessment context before reviewing results.
Therefore, the section Nikhil is working on is C. Assessment Overview, which establishes the assessment context and explains the scanning approach prior to presenting findings and risk conclusions.

NEW QUESTION: 252
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: 253

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: 254
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.

Valid 312-50v13 Dumps shared by Actual4test.com for Helping Passing 312-50v13 Exam! Actual4test.com now offer the **newest 312-50v13 exam dumps**, the Actual4test.com 312-50v13 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 312-50v13 dumps with Test Engine here: https://www.actual4test.com/312-50v13_examcollection.html (**787** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)