CertiProf.CEHPC.v2026-06-10.q54

Exam Code:	CEHPC
Exam Name:	Ethical Hacking Professional Certification Exam
Certification Provider:	CertiProf
Free Question Number:	54
Version:	v2026-06-10
# of views:	155
# of Questions views:	540
https://www.freepdfdumps.com/CertiProf.CEHPC.v2026-06-10.q54.html	

NEW QUESTION: 1
Which of the following is a network security protocol designed to authenticate and authorize remote users to securely access network resources?
A. SSL (Secure Sockets Layer).
B. FTP (File Transfer Protocol).
C. SSH (Secure Shell).
Answer: C (LEAVE A REPLY)
Secure Shell (SSH) is a robust cryptographic network protocol utilized for operating network services securely over an unsecured network. Its primary application is the secure remote login to computer systems by administrators and users. Unlike earlier protocols such as Telnet or rlogin, which transmitted data (including passwords) in plain text, SSH provides a secure, encrypted channel. It achieves this through a suite of cryptographic techniques that ensure theconfidentiality,integrity, andauthenticityof the data being transmitted between the client and the server.
The protocol operates using a client-server architecture, where an SSH client initiates a connection to an SSH server. SSH facilitates both authentication and authorization. Authentication is typically performed using either a password or, more securely, a public-private key pair. Once the user's identity is verified, the protocol authorizes the level of access based on the server's configuration. Beyond simple terminal access, SSH supports secure file transfers (SFTP) and port forwarding, allowing other network protocols to be "tunneled" through its encrypted connection. From a security standpoint, while SSH is highly secure, it can be breached if misconfigured-such as by allowing weak passwords or failing to disable root login. Consequently, ethical hackers prioritize hardening SSH services as a fundamental control in protecting organizational assets.

NEW QUESTION: 2
Can Kali Linux only be used by criminals?

A. YES, criminal acts are carried out with it.
B. YES, it is a prohibited system.
C. NO, it can be used by cybersecurity enthusiasts.
Answer: C (LEAVE A REPLY)
Kali Linux is a specialized, Debian-derived Linux distribution designed specifically for digital forensics and penetration testing. While it is true that the tools included in Kali Linux can be used for criminal activities (Option A), the operating system itself is a legitimate professional tool used worldwide by cybersecurity enthusiasts, ethical hackers, and security researchers. Its primary purpose is to provide a comprehensive environment pre-loaded with hundreds of security tools for tasks like vulnerability analysis, wireless attacks, and web application testing.
The distinction between a criminal act and ethical hacking lies in "authorization" and "intent" rather than the tools used. Ethical hackers use Kali Linux to perform authorized security audits to help organizations identify and fix vulnerabilities before they are exploited by real-world attackers. For example, tools like Nmap or Metasploit are essential for a penetration tester to map a network and verify the effectiveness of existing security controls.
Furthermore, Kali Linux is an essential educational resource. It allows students to learn about the "phases of hacking"-reconnaissance, scanning, and gaining access-in a controlled, legal environment. Many cybersecurity certifications, such as the OSCP (Offensive Security Certified Professional), are built around the proficiency of using this system. Claiming it is a "prohibited system" (Option B) is factually incorrect; it is an open-source project maintained by Offensive Security and is legal to download and use for legitimate security research and defense. By mastering Kali Linux, security professionals can better understand the techniques used by adversaries, allowing them to build more resilient and secure digital infrastructures.

NEW QUESTION: 3
What is netcat?
A. It is a versatile, open-source network tool used for reading and writing data over network connections.
B. It is a hacking tool for Linux.
C. It is a hacking tool for Windows.
Answer: A (LEAVE A REPLY)
Netcat, often referred to as the "Swiss Army Knife" of networking, is a powerful and versatile utility that uses TCP or UDP protocols to read and write data across network connections. It is a foundational tool for both system administrators and security professionals because of its ability to perform a wide variety of tasks with minimal overhead. While it is natively a Linux tool, versions like ncat (distributed with Nmap) make it available across all major operating systems.
In the context of ethical hacking, Netcat is used for:

* Port Scanning: It can be used as a lightweight port scanner to check for open services on a target.
* Banner Grabbing: By connecting to a specific port, testers can capture the "banner" or header sent by a service to identify its software version.
* File Transfer: It can push files from one machine to another without needing FTP or SMB protocols.
* Creating Backdoors and Shells: Netcat is the primary tool used to establishBind ShellsorReverse Shellsduring the exploitation phase of a pentest. An attacker can set Netcat to "listen" on a port and execute a shell (like /bin/bash or cmd.exe) whenever someone connects to it.
Its simplicity is its greatest strength; it can be scripted into complex automated tasks or used manually for quick troubleshooting. Because Netcat can be used to bypass security controls and establish unauthorized access, security teams often monitor for its presence or execution on sensitive servers. Understanding how to use and defend against Netcat is a core requirement for any information security expert.

NEW QUESTION: 4
What tool would you use to search for hidden directories or files?
A. Dirb
B. Shodan
C. Ping
Answer: A (LEAVE A REPLY)
DIRB is a specializedweb content scanning toolused in ethical hacking and penetration testing to discoverhidden directories and fileson web servers. It operates by performing adictionary-based brute-force attackagainst a target website, attempting to access directories and files that are not publicly linked but may still be accessible. This makes option A the correct answer.
DIRB is typically used during theweb application reconnaissance and enumeration phasesof penetration testing. Ethical hackers rely on it to uncover misconfigurations such as exposed admin panels, backup files, configuration files, or outdated directories that could lead to further compromise. These hidden resources often exist due to poor security practices or improper cleanup during development.
Option B, Shodan, is incorrect because Shodan is a search engine used to discover internet-connected devices and services, not hidden directories within a specific website.
Option C, Ping, is also incorrect because it is a network utility used only to test host reachability and does not interact with web servers at the application layer.
From a defensive security perspective, DIRB helps organizations identify unnecessary exposure in web environments. Discovering hidden directories allows administrators to remove, restrict, or secure them before attackers exploit them. When used ethically and with authorization, DIRB is a powerful tool for improving web application security and reducing attack surfaces.

NEW QUESTION: 5
What is the most vulnerable within an organization?
A. Servers.
B. Wi-Fi network.
C. Individuals.
Answer: (SHOW ANSWER)
In the field of cybersecurity, it is a well-established axiom thatindividuals(the human element) represent the most vulnerable link in an organization's security chain. While a company can invest millions of dollars in sophisticated firewalls, encryption, and endpoint protection, these technical controls can be completely bypassed if a human is manipulated into granting access.
The vulnerability of individuals stems from several psychological factors:
* Trust and Cooperation: Humans are naturally inclined to be helpful, which attackers exploit through social engineering.
* Lack of Awareness: Employees who are not trained in security hygiene may use weak passwords, reuse credentials across multiple sites, or fail to recognize phishing attempts.
* Fatigue and Urgency: Attackers often create a false sense of crisis (e.g., "Your account will be deleted in 1 hour") to trick users into bypassing their better judgment.
* Physical Security Risks: Common vulnerabilities include "tailgating" (following someone through a secure door) or leaving sensitive documents on a desk.
Ethical hacking documents emphasize that a "Defense in Depth" strategy must include the "Human Firewall." This involves continuous security awareness training, phishing simulations, and clearAcceptable Use Policies (AUP). Organizations that ignore the human element often find themselves victims of ransomware or data breaches despite having state-of-the-art technical defenses. Strengthening the human link through education is the most effective way to reduce the overall attack surface of an organization.

NEW QUESTION: 6
Do all hackers always carry out criminal activities?
A. Yes, all hackers commit crimes such as hacking banks or social media accounts.
B. No, ethical hackers responsibly report discovered vulnerabilities to the appropriate organization for remediation.
C. Yes, hackers always sell stolen information to the highest bidder.
Answer: B (LEAVE A REPLY)
Not all hackers engage in criminal activity, making option B the correct answer. The term "hacker" broadly refers to individuals with technical skills to understand and manipulate systems. Their intent determines whether their actions are ethical or malicious.
Ethical hackers, also known as White Hat hackers, work legally and with authorization to identify vulnerabilities in systems, networks, and applications. When they discover security

weaknesses, they follow responsible disclosure practices by reporting findings to the affected organization so issues can be fixed promptly.
Option A is incorrect because it incorrectly generalizes all hackers as criminals. Option C is incorrect because selling stolen information describes malicious actors, often referred to as Black Hat hackers.
Understanding this distinction is important when analyzingcurrent security trends, as ethical hacking has become a legitimate profession. Many organizations now rely on penetration testers, bug bounty programs, and internal security teams to proactively defend against cyber threats.
Ethical hacking contributes to safer digital environments by helping organizations strengthen defenses before attackers exploit vulnerabilities. Recognizing that hacking skills can be used constructively supports responsible security practices and professional cybersecurity development.

NEW QUESTION: 7
What is a firewall?
A. A device or software that monitors and filters network traffic to help prevent unauthorized access.
B. Software that only protects against viruses.
C. A method for hacking systems remotely.
Answer: A (LEAVE A REPLY)
A firewall is a fundamental information security control designed to monitor, filter, and control incoming and outgoing network traffic based on predefined security rules. This makes option A the correct answer.
Firewalls act as a barrier between trusted internal networks and untrusted external networks, such as the internet. They can be implemented as hardware devices, software applications, or cloud-based services.
Ethical hackers must understand firewall behavior because it directly affects reconnaissance, exploitation techniques, and attack surface visibility.
Option B is incorrect because antivirus software focuses on malware detection, not traffic filtering. Option C is incorrect because a firewall is a defensive security mechanism, not an attack method.
From an ethical hacking perspective, firewalls are evaluated during security assessments to identify misconfigurations, overly permissive rules, or exposed services. Poorly configured firewalls may allow unauthorized access, while overly restrictive ones may disrupt legitimate business operations.
Firewalls play a critical role in enforcing network segmentation, access control, and defense-in-depth strategies. When combined with intrusion detection systems, endpoint security, and proper monitoring, they significantly reduce the risk of unauthorized access.
Understanding firewall concepts enables ethical hackers and defenders to design stronger network architectures and respond effectively to modern cyber threats.

NEW QUESTION: 8
What is XSS (Cross-Site Scripting)?
A. It is a security vulnerability that occurs in web applications when user-supplied input is not properly validated or sanitized, allowing malicious scripts to execute in a user's web browser.
B. It is a type of cloned website created with malicious intent.
C. It is a security vulnerability that occurs in mobile applications to steal balances or contacts.
Answer: A (LEAVE A REPLY)
Cross-Site Scripting (XSS) is aweb application security vulnerabilitythat allows attackers to inject malicious client-side scripts into trusted web pages. This makes option A the correct answer. XSS occurs when applications fail to properly validate, sanitize, or encode user input before displaying it to other users.
When an XSS vulnerability is exploited, the injected script runs in the victim's browser within the security context of the vulnerable website. This can lead to session hijacking, cookie theft, credential harvesting, keylogging, or redirection to malicious websites. XSS is commonly categorized intostored XSS, reflected XSS, and DOM-based XSS, all of which ethical hackers test during web application assessments.
Option B is incorrect because cloned websites are typically associated with phishing attacks, not XSS vulnerabilities. Option C is incorrect because XSS is primarily a web-based vulnerability, not a mobile- specific issue involving balance or contact theft.
From a defensive perspective, understanding XSS is critical for implementing secure coding practices such as input validation, output encoding, Content Security Policy (CSP), and proper use of modern frameworks.
Ethical hackers test for XSS to help organizations prevent client-side attacks and protect user data.

NEW QUESTION: 9
What is a "Reverse Shell?
A. It refers to a process in which the victim's machine connects to the attacker's machine to receive commands.
B. It refers to when the terminal is run with root.
C. A common Linux command console.
Answer: A (LEAVE A REPLY)
A reverse shell is a fundamental technique used during the exploitation phase of a penetration test to gain interactive access to a target system. In a standard shell connection (Bind Shell), the attacker initiates a connection to a specific port on the victim's machine. However, modern network security controls, such as firewalls and Network Address Translation (NAT), almost always block unsolicited inbound connections. To bypass these restrictions, ethical hackers utilize a "reverse shell." In this scenario, the

attacker first sets up a listener on their own machine (using a tool like Netcat or Metasploit) on a common outbound port, such as 80 (HTTP) or 443 (HTTPS). The attacker then executes a payload on the victim's machine that instructs it to initiate an outbound connection back to the attacker's listener.
Since most firewalls are configured to be permissive with outbound traffic (to allow users to browse the web), the connection from the victim to the attacker is often successful. Once the connection is established, the victim's machine hands over control of its command-line interface to the attacker. This allows the attacker to execute commands as if they were sitting at the victim's keyboard. The power of a reverse shell lies in its ability to circumvent perimeter defenses and provide a stable platform for post-exploitation activities, such as privilege escalation or lateral movement. From a defensive standpoint, organizations can mitigate this threat by implementing strict egress (outbound) filtering, which limits the ports and IP addresses that internal servers can communicate with. Monitoring for unusual outbound traffic patterns and using EDR (Endpoint Detection and Response) tools to identify unauthorized shell processes are also critical components of a robust security strategy designed to detect and terminate active reverse shell connections.

NEW QUESTION: 10
What is active reconnaissance?
A. Recognizes the target but does nothing.
B. Observes the target without performing any direct actions.
C. Gathers information by directly interacting with the target.
Answer: (SHOW ANSWER)
Active reconnaissance is a phase of ethical hacking in which information is gathered bydirectly interacting with the target system. This makes option C the correct answer.
Unlike passive reconnaissance, active reconnaissance involves sending requests, probes, or packets to the target to elicit responses that reveal useful technical details.
Common active reconnaissance techniques includeport scanning,service enumeration,banner grabbing,DNS queries, andnetwork mapping. These methods help ethical hackers identify open ports, running services, operating systems, and potential vulnerabilities. Active reconnaissance is typically conducted after passive techniques have provided initial intelligence.
Option A is incorrect because recognizing a target without action does not describe reconnaissance behavior.
Option B is also incorrect because observing without interaction definespassive reconnaissance, not active reconnaissance.
From an ethical hacking perspective, active reconnaissance is more intrusive and therefore more likely to be detected by intrusion detection systems or firewalls. Because of this, it must always be performed withexplicit authorization. Despite the increased risk of detection, active reconnaissance provides far more accurate and actionable information, making it essential for effective penetration testing.

Understanding the distinction between active and passive reconnaissance helps security professionals choose the correct techniques based on scope, authorization, and risk tolerance. Properly managed, active reconnaissance enables organizations to identify weaknesses early and strengthen their defensive security posture.

NEW QUESTION: 11
What is an "exploit" in the hacking world?
A. A malicious program that spreads through social networks.
B. A code designed to exploit a specific vulnerability in a system.
C. A technique for removing malware.
Answer: B (LEAVE A REPLY)
In the hacking world, an "exploit" is a specialized piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in a system to cause unintended or unanticipated behavior. The primary goal of an exploit is to gain unauthorized access to a computer system, escalate privileges, or trigger a denial-of-service condition. Exploits are the "keys" used by hackers to unlock the doors found during the scanning and vulnerability analysis phases.
Exploits are typically categorized into two types based on where they are launched:Remote Exploits, which work over a network without prior access to the target, andLocal Exploits, which require prior access to the system to increase privileges. Within the ethical hacking lifecycle, the "Exploitation" phase occurs after a vulnerability has been identified and verified. An ethical hacker uses a specific exploit code to demonstrate the real-world impact of a flaw, proving to the stakeholders that the vulnerability is not just a theoretical risk but a practical entry point for an attacker.
It is important to differentiate an exploit from malware (Option A); while an exploit is themethodused to get in, malware is thepayloaddelivered once the door is open. Understanding exploits is fundamental for security professionals, as it allows them to develop "signatures" for intrusion detection systems and provides the justification needed for urgent patch management. By mastering the use of exploits in a controlled environment, such as with the Metasploit Framework, ethical hackers can better defend systems by anticipating how a malicious actor would attempt to break through technical barriers.

NEW QUESTION: 12
What is Rhost in metasploit?
A. Remote host.
B. Local root variable.
C. Root host.
Answer: A (LEAVE A REPLY)
In the context of the Metasploit Framework, RHOSTS (often referred to in its singular form RHOST) is one of the most fundamental variables a penetration tester must configure. It

stands forRemote Hostand represents the target IP address or hostname that the exploit or auxiliary module will attempt to interact with. Metasploit is designed around a modular architecture where users select an exploit, configure the necessary payloads, and then set the specific variables required for the module to execute successfully.
When a tester identifies a vulnerability on a target machine, they use the command set RHOSTS [Target_IP] within the msfconsole to direct the attack. This variable can take a single IP address (e.g., 192.168.1.10), a range of IP addresses (e.g., 192.168.1.1-192.168.1.50), or a CIDR notation (e.g., 192.168.1.0/24). Unlike LHOST (Local Host), which identifies the attacker's machine for receiving incoming connections, RHOSTS defines the destination.
Understanding these variables is critical for the "Exploitation" phase of a penetration test. If RHOSTS is set incorrectly, the exploit will be sent to the wrong machine, potentially causing unintended system crashes or alerts on non-target systems. Furthermore, modern versions of Metasploit use the plural RHOSTS even for single targets to maintain consistency across modules that support scanning entire networks. Mastering the configuration of these parameters ensures that an ethical hacker can efficiently deploy modules against specific vulnerabilities while maintaining precise control over the scope of the engagement.

NEW QUESTION: 13
What is Nmap?
A. It is an open-source command-line tool used to scan IP addresses and ports on a network and to detect services, operating systems, and running applications.
B. It is a Linux-based tool that works specifically to exploit computer vulnerabilities.
C. It is a program used only for pinging computers within a network or work environment.
Answer: A (LEAVE A REPLY)
Nmap, also known asNetwork Mapper, is a widely used open-source tool in ethical hacking and penetration testing. It plays a critical role during thereconnaissance and scanning phasesof ethical hacking, where the primary goal is to collect information about target systems in a legal and authorized manner. Ethical hackers rely on Nmap to understand the structure and exposure of a network before moving forward with deeper security testing.
The tool works by sending various types of packets to target hosts and analyzing the responses. Based on these responses, Nmap can identifyactive hosts,open and closed ports,running services,service versions, operating systems, and even certainfirewall and intrusion detection configurations. This information is essential for identifying potential weaknesses such as unnecessary open ports, misconfigured services, or outdated software.
Option A correctly defines Nmap because it accurately reflects its purpose as a scanning and discovery tool rather than an exploitation utility. Option B is incorrect because Nmap does not exploit vulnerabilities; exploitation is typically performed using specialized frameworks such as vulnerability scanners or exploitation platforms. Option C is also

incorrect because although Nmap can perform host discovery similar to ping, it offers far more advanced capabilities than simple network reachability checks.
From an ethical hacking perspective, Nmap supportspreventive and defensive security objectives. By revealing network visibility issues and configuration flaws, it enables organizations to harden systems, reduce attack surfaces, and comply with security best practices. When used ethically and with proper authorization, Nmap is a foundational tool for strengthening information security.

NEW QUESTION: 14
Is it possible to perform geolocation phishing?
A. Yes, but with paid tools.
B. YES, it can be done with a seeker.
C. NO, it is a very complicated technique.
Answer: B (LEAVE A REPLY)
Geolocation phishing is an advanced social engineering technique used to trick a victim into revealing their precise physical location. This is typically achieved by sending the target a link to a deceptive web page that appears to offer a legitimate service or interesting content. When the user clicks the link, the page requests permission to access the device's location services (GPS). If the user clicks "Allow," the exact coordinates are transmitted back to the attacker.
One of the most prominent tools used in the ethical hacking course for this purpose isSeeker. Seeker is an open-source tool that creates a fake website-often mimicking a "Near Me" service or a weather app-to entice the user into sharing their location. Unlike standard IP-based geolocation, which only provides a general area based on the Internet Service Provider's location, Seeker uses the device's actual GPS data to provide accuracy within meters.
This technique is a powerful example of how attackers can combine technical vulnerabilities with human psychology. In a professional penetration test, geolocation phishing might be used to demonstrate how an executive could be tracked or how a remote worker's location could be compromised. Defending against this threat requires high user awareness: individuals should never grant location permissions to unfamiliar websites or links received via unsolicited emails or messages. It highlights that sensitive data isn't just limited to passwords; it also includes the physical whereabouts of individuals.

NEW QUESTION: 15
Which of the following is an example of social engineering?
A. Use of antivirus software.
B. Periodic updating of the operating system.
C. Ask users to disclose their password over the phone.
Answer: (SHOW ANSWER)

Identifying examples of social engineering is crucial for recognizing the diverse ways attackers attempt to circumvent technical security controls. A classic and highly effective example of social engineering is
"vishing" (voice phishing), where an attacker calls a user and attempts to persuade them to disclose sensitive information, such as their network password, over the phone. This technique relies on the attacker's ability to sound professional, authoritative, or helpful, creating a scenario where the victim feels compelled to comply.
In contrast, options such as the use of antivirus software and periodic updating of the operating system are technical security controls. These are automated or administrative processes designed to protect the system's integrity from malware and exploits. Social engineering, however, bypasses these technical defenses by targeting the user directly. When an attacker asks for a password over the phone, they are not attempting to "break" the password through a brute-force attack; they are simply asking for the "key to the front door" by exploiting the user's trust.
This specific example highlights the concept of "Pretexting." The attacker may claim there is a critical security breach or a technical error on the user's account and that the password is required to "fix" the issue.
Once the user discloses the password, the attacker has gained legitimate access to the system, often leaving no immediate trace of a technical intrusion. For an ethical hacker, documenting these types of vulnerabilities is essential. It demonstrates that even the most advanced firewall or antivirus cannot protect an organization if its employees are willing to give away credentials to an unverified caller. This reinforces the need for
"Security Awareness Training," which teaches individuals that legitimate IT personnel will never ask for a full password over a phone call or through an unencrypted communication channel.

NEW QUESTION: 16
When critical vulnerabilities are detected, what should be done?
A. Document the problem and do nothing.
B. Exploit it and extract as much information as possible.
C. Inform the corresponding area for a prompt solution.
Answer: C (LEAVE A REPLY)
In the professional penetration testing process, the discovery of a "critical" vulnerability-one that could lead to immediate system compromise or data loss-triggers a specific ethical and procedural response. While the ultimate goal of a pentest is to find weaknesses, the primary duty of an ethical hacker is to ensure the safety and security of the client's environment. Therefore, when a critical flaw is identified, the tester must immediately inform the relevant stakeholders or technical teams so that a prompt solution or "hotfix" can be implemented.
This immediate reporting deviates from the standard "end-of-test" report delivery because critical vulnerabilities represent an "active risk". If a tester finds an unpatched, high-impact

vulnerability that is publicly known, there is a high probability that a real attacker could exploit it while the pentest is still ongoing. By notifying the client immediately, the tester helps mitigate the risk of an actual breach occurring during the assessment. This process is often detailed in the "Rules of Engagement" (RoE) agreed upon before the test begins. Once the "corresponding area" (such as the DevOps or Security Operations team) is informed, the tester documents the vulnerability with clear reproduction steps and remediation advice. The tester may then be asked to "re-test" the vulnerability after the fix has been applied to verify its effectiveness. This highlights the collaborative nature of ethical hacking; it is not just about "breaking in" (Option B), but about the strategic management of risk. Professionalism in pentesting is defined by this commitment to communication and the proactive protection of the client's assets, ensuring that vulnerabilities are closed as quickly as possible to minimize the window of opportunity for malicious actors.

NEW QUESTION: 17
What is a WAF?
A. A Web Application Form (WAF) protects printers from multiple attacks.
B. A Web Application Functionality (WAF) protects computers from multiple attacks.
C. A Web Application Firewall (WAF) protects the web application server from multiple attacks.
Answer: C (LEAVE A REPLY)
A Web Application Firewall (WAF) is a specialized information security control designed to protect web applications by filtering, monitoring, and blocking HTTP/HTTPS traffic to and from a web service. Unlike a traditional network firewall that filters traffic based on IP addresses and ports, a WAF operates at the Application Layer (Layer 7 of the OSI model). It inspects the actual content of the web traffic to identify and neutralize sophisticated application-level attacks such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and File Inclusion.
A WAF acts as a "reverse proxy," sitting in front of the web application server and acting as an intermediary.
It uses a set of rules (often based on the OWASP Top 10) to determine which traffic is legitimate and which is malicious. For example, if a user submits a search query containing

suspicious SQL commands, the WAF will recognize the pattern and drop the request before it ever reaches the database, thereby protecting the server from compromise.
In the context of ethical hacking, a WAF is a formidable defense that testers must learn to navigate. During a penetration test, a WAF may block automated scanning tools, forcing the tester to use manual, stealthy techniques to identify vulnerabilities. For organizations, implementing a WAF is a critical "defense-in-depth" strategy. Even if a web application has an underlying code vulnerability, the WAF can provide a "virtual patch" by blocking the exploit attempt at the network edge. This allows developers time to fix the code without leaving the application exposed. Mastering WAF configuration and bypass techniques is essential for security professionals who aim to protect modern, web-centric business environments.

NEW QUESTION: 18
What is Masquerading?
A. Consists of impersonating the identity of a legitimate user of a computer system or its environment.
B. A method for masking network traffic.
C. Web authentication method.
Answer: A (LEAVE A REPLY)
Masquerading is a sophisticated attack vector that consists of an unauthorized user or process impersonating the identity of a legitimate user, system, or service within a computer environment. In the context of cybersecurity, the goal of masquerading is to bypass authentication controls and gain access to restricted resources or information by appearing as a trusted entity. This is often a critical step in the "Gaining Access" phase of a cyberattack, as it allows the attacker to operate under the radar of traditional security logging.
There are several ways masquerading can manifest:
* User Impersonation: An attacker uses stolen credentials (usernames and passwords) to log into a system as a legitimate employee.
* IP Spoofing: An attacker crafts network packets with a forged source IP address to make it appear as though the traffic is coming from a trusted internal machine.
* Email Spoofing: An attacker sends an email that appears to come from a known, trusted source (like an executive or a bank) to trick the recipient into performing an action, such as revealing a password.
Managing and mitigating the threat of masquerading requires robust "Identity and Access Management" (IAM) controls. The most effective defense is Multi-Factor Authentication (MFA). Even if an attacker successfully masquerades as a user by stealing their password, the MFA requirement provides a second layer of verification that is much harder to forge. Additionally, organizations can use "Behavioral Analytics" to detect anomalies; for example, if a user who typically logs in from London suddenly logs in from a different continent, the system can flag it as a potential masquerading attempt. By understanding

that masquerading relies on the manipulation of trust and identity, ethical hackers can help organizations implement "Zero Trust" architectures, where every request is verified regardless of where it appears to originate.

NEW QUESTION: 19
Is it important to perform penetration testing for companies?
A. Yes, in order to sell the information.
B. Yes, in order to protect information and systems.
C. No, because hackers do not exist.
Answer: B (LEAVE A REPLY)
Penetration testing is critically important for companies because it helpsprotect information, systems, and business operations, making option B the correct answer. Penetration testing simulates real-world attacks in a controlled and authorized manner to identify vulnerabilities before malicious actors exploit them.
Organizations face constant threats from cybercriminals, hacktivists, insider threats, and automated attacks.
Regular penetration testing allows companies to assess their security posture, validate the effectiveness of existing controls, and identify weaknesses in networks, applications, and processes. Ethical hackers provide actionable recommendations that help reduce risk and improve resilience.
Option A is incorrect because selling discovered information is unethical and illegal. Option C is incorrect because cyber threats are real and continue to grow in complexity and frequency.
From an ethical hacking perspective, penetration testing supports compliance with security standards, protects customer data, and prevents financial and reputational damage. It also helps organizations prioritize remediation efforts based on real risk rather than assumptions.
Penetration testing is not a one-time activity but part of a continuous security strategy. By regularly testing defenses, companies can adapt to evolving threats and maintain a strong security posture.

NEW QUESTION: 20
What is a Stored Cross-Site Scripting Attack (Stored XSS)?
A. The malicious code is permanently stored on the server.
B. The source code of the page, this can be html or javascript.
C. In this type of attack, the malicious code is sent to the web server via an HTTP request. The server then processes the request and returns a response that includes the malicious code.
Answer: (SHOW ANSWER)
Persistent Cross-Site Scripting (XSS), also known as Stored XSS, is one of the most dangerous forms of web application vulnerabilities. It occurs when a web application

receives data from a user and stores it permanently in its backend database or filesystem without proper sanitization or encoding. Common vectors for persistent XSS include comment sections, user profiles, message boards, and "Contact Us" forms. Unlike Reflected XSS, where the payload is included in a specific URL and only affects the user who clicks that link, a persistent XSS payload is served automatically to every user who visits the affected page.
When an attacker successfully injects a malicious script (typically JavaScript), the server "remembers" this script. Every time a legitimate user requests the page where the data is displayed, the server includes the malicious code in the HTML response. The user's browser, trusting the source, executes the script. This can lead to devastating consequences, such as session hijacking through the theft of session cookies, account takeover, or the redirection of users to malicious websites. From an ethical hacking perspective, identifying persistent XSS involves testing all input fields that result in data being displayed later. Mitigation strategies focus on the principle of "filter input, escape output." Input should be validated against a strict whitelist of allowed characters, and any data rendered in the browser must be context-aware encoded (e.g., converting < to <) to prevent the browser from interpreting the data as executable code. Because the payload is stored on the server, this vulnerability represents a significant risk to the entire user base of an organization, making it a high-priority finding in any security assessment.

NEW QUESTION: 21
What is active recognition?
A. We only see the target without performing actions.
B. Gathers information by interacting with the target.
C. Recognizes the target but does nothing.
Answer: B (LEAVE A REPLY)
Active recognition, also known as "Active Reconnaissance," is a critical phase of penetration testing where the tester gathers detailed information by directly interacting with the target system or network. Unlike
"Passive Reconnaissance," which involves collecting publicly available information from search engines (like Google Dorking) or social media without the target's knowledge, active recognition involves sending data packets to the target's infrastructure to elicit a response.
Common activities during the active recognition phase include port scanning, service version detection, and vulnerability scanning. For example, using a tool like Nmap to scan a server's open ports is a form of active recognition. The scanner sends "probes" to the server, and based on the server's reply (or lack thereof), the tester can determine which services are running (e.g., a web server on port 80 or a database on port 3306).
This phase is essential because it provides the technical "blueprint" of the target that the tester will use to plan an exploit.

However, active recognition carries a significant risk: it is much more likely to be detected by security systems like Intrusion Detection Systems (IDS) or firewalls. Because the tester is directly "knocking on the doors" of the target, their IP address and activity may be logged. In a professional pentest, the degree of
"stealth" used during active recognition is a key consideration. Testers may slow down their scans or use techniques to blend in with normal network traffic to avoid detection. For the organization, being able to detect active reconnaissance is a vital part of threat management, as it often serves as the "early warning sign" that a more sophisticated attack is being prepared. Mastering this phase allows a pentester to efficiently map the attack surface while understanding the operational limits of the target's defensive controls.

NEW QUESTION: 22
What is a public IP address?
A. An IP address that everyone uses.
B. An IP address assigned by an Internet Service Provider (ISP) that is accessible over the internet.
C. An IP address assigned by a modem to devices within a local network.
Answer: B (LEAVE A REPLY)
A public IP address is aninternet-routable address assigned by an Internet Service Provider (ISP), making option B the correct answer. Public IPs uniquely identify a device or network on the global internet and allow communication with external systems.
Option A is incorrect because public IPs are unique, not shared by everyone. Option C is incorrect because IP addresses assigned by a modem or router to internal devices are private IP addresses, typically managed using Network Address Translation (NAT).
From an ethical hacking perspective, public IP addresses are significant because they representexternally exposed attack surfaces. Services accessible via public IPs may be scanned, targeted, or attacked if not properly secured.
Understanding the difference between public and private IP addressing helps ethical hackers assess network exposure, firewall configurations, and access control policies. Defenders can reduce risk by limiting services exposed on public IPs and enforcing strong security controls.
Public IP management is a core information security concept, influencing perimeter security, network design, and threat modeling in modern environments.

NEW QUESTION: 23
What is a vulnerability scan?
A. It is the process of identifying, quantifying and prioritizing vulnerabilities in computer systems.
B. It is the process of mapping the network and nodes in a building for better distribution.
C. It is the process of identifying and exploiting gaps no matter what.
Answer: (SHOW ANSWER)

Vulnerability scanning is a fundamental, automated cybersecurity practice designed to systematically identify and evaluate security weaknesses within an organization's IT infrastructure. Unlike penetration testing, which actively attempts to exploit flaws to gauge the depth of a potential breach, vulnerability scanning is generally a non-intrusive "reconnaissance-level" check. It uses specialized software tools-vulnerability scanners-to probe network devices, servers, and applications to compare discovered services against databases of known security flaws (Common Vulnerabilities and Exposures, or CVEs).
The process typically unfolds in several stages:
* System Discovery: Identifying all physical and virtual assets on the network, such as routers, physical hosts, and cloud endpoints.
* Vulnerability Detection: Probing open ports and services using techniques like "banner grabbing" or
"fingerprinting" to identify software versions and configurations.
* Prioritization and Reporting: Assigning severity scores (often using the CVSS framework) to identified flaws based on factors like ease of exploitation and potential impact.
Vulnerability scans are essential for maintaining a strong security posture because they can be run continuously and automatically at a lower cost than manual testing. They help organizations stay ahead of
"zero-day" and emerging threats by flagging missing patches, weak passwords, and insecure default configurations. While highly effective at identifying broad classes of vulnerabilities-such as SQL injection or outdated encryption-scanners can produce "false positives," requiring security teams to validate findings before proceeding with remediation. Ultimately, vulnerability scanning serves as the critical first step in a broader vulnerability management lifecycle.

NEW QUESTION: 24
What is the best practice to protect against malware?
A. Sharing login information on suspicious websites.
B. Clicking on suspicious links to verify their authenticity.
C. Installing and keeping antivirus software up to date.
Answer: (SHOW ANSWER)
One of the most effective best practices to protect against malware isinstalling and regularly updating antivirus software, making option C the correct answer. Antivirus and endpoint protection solutions are designed to detect, block, and remove malicious software such as viruses, worms, trojans, ransomware, and spyware.
Modern malware evolves rapidly, using obfuscation and zero-day techniques to bypass outdated defenses.
Keeping antivirus software up to date ensures that the latest malware signatures, heuristics, and behavioral detection mechanisms are in place. Ethical hackers emphasize this practice because many successful attacks exploit systems with outdated or disabled security software.

Option A is incorrect because sharing login credentials on suspicious websites significantly increases the risk of malware infection and credential theft. Option B is incorrect because clicking on suspicious links is a common infection vector used in phishing and malware distribution campaigns.
From an ethical hacking perspective, malware prevention is part ofdefense-in-depth. Antivirus software should be combined with patch management, least-privilege access, secure browsing habits, and user awareness training. Ethical hackers often demonstrate how quickly unprotected systems can be compromised to highlight the importance of these controls.
Strong malware protection reduces attack surfaces, prevents data loss, and supports incident response efforts.
Maintaining updated antivirus software is a foundational information security control in modern environments.

NEW QUESTION: 25
What is a reverse shell?
A. It refers to a process in which the victim's machine connects to the attacker's machine to receive commands.
B. It refers to when the terminal is run with root.
C. A common Linux command console.
Answer: A (LEAVE A REPLY)
A reverse shell is a fundamental technique used during the "Gaining Access" and "Maintaining Access" phases of a penetration test. In a standard (bind) shell, the attacker connects to a specific port on the victim's machine to gain command-line access. However, most modern firewalls block incoming connections to unauthorized ports. To bypass this, a reverse shell reverses the connection logic: the victim's machine is tricked into initiating anoutgoingconnection to the attacker's machine, which is "listening" for the call.
This technique is highly effective because firewalls are typically much more permissive with "egress" (outgoing) traffic than with "ingress" (incoming) traffic. For example, an attacker might host a listener on port
443 (HTTPS). Since most organizations allow internal machines to browse the web over port 443, the firewall perceives the reverse shell connection as standard web traffic and allows it to pass. Once the connection is established, the attacker has a terminal interface on the victim's machine, allowing them to execute commands remotely.
In professional pentesting, establishing a reverse shell is often the primary goal of an exploit. It provides the
"foothold" needed for lateral movement and privilege escalation. Common tools used to create reverse shells include Netcat (nc), Bash, and Python scripts. To defend against this, organizations must implement "Egress Filtering," which restricts outgoing traffic to only known, necessary destinations. Security professionals also monitor for "long-lived" connections to unusual IP addresses, as these can be a tell-tale sign of an active reverse

shell. Understanding how these connections manipulate network policy is crucial for any ethical hacker seeking to demonstrate how internal systems can be compromised despite robust perimeter defenses.

NEW QUESTION: 26
What is a black hat hacker?
A. They use their computer skills to steal confidential information, to infect computer systems, to restrict access to a system.
B. They use their computer skills to protect confidential information to restrict access to a system.
C. They check the wiring of installations, provide support to users and are aware of servers in small companies.
Answer: A (LEAVE A REPLY)
A "Black Hat" hacker is the primary threat actor in the cybersecurity landscape, representing the criminal element of the hacking community. These individuals use their advanced computer skills and technical knowledge with malicious intent to breach security defenses. Their goals typically involve stealing confidential information, infecting computer systems with malware, or restricting access to a system (as seen in DDoS or ransomware attacks) for personal gain, financial profit, or ideological reasons.
Black Hat hackers operate without authorization and often hide their tracks through anonymization tools like VPNs, Tor, and proxy chains. Their methodology involves finding and exploiting vulnerabilities-often
"Zero-Day" flaws that the vendor is not yet aware of-to gain a foothold in a target network. Once inside, they may engage in corporate espionage, sell stolen data on the dark web, or hold an organization's operations hostage.
For a security professional, managing the threat of Black Hat hackers is a continuous cycle of "Threat Hunting" and "Risk Mitigation." Ethical hackers must study the tactics, techniques, and procedures (TTPs) used by Black Hats to build more resilient defenses. While Black Hats are the "adversaries," they also drive the evolution of security technology; as they find new ways to break into systems, the industry must develop new encryption, authentication, and monitoring tools to stop them. Understanding the mindset of a Black Hat-how they prioritize targets and which vulnerabilities they find most attractive-is a key component of the CEH curriculum. It allows defenders to think like their opponents, ensuring that security controls are placed where they are most needed to protect an organization's most valuable confidential assets.

NEW QUESTION: 27
Is it important to perform pentesting to companies?
A. YES, in order to protect the information.
B. NO, since hackers do not exist.
C. YES, in order to sell the information.

Answer: A (LEAVE A REPLY)
Penetration testing, or "pentesting," is a vital component of a robust information security strategy for any modern organization. It serves as a proactive security measure designed to evaluate the effectiveness of a company's defenses by simulating a real-world cyber-attack. The primary objective is to identify vulnerabilities before malicious actors can find and exploit them, thereby protecting sensitive corporate and customer information.
Regular pentesting provides several critical benefits:
* Risk Identification: It uncovers hidden flaws in software, misconfigured hardware, and weak security protocols that automated scanners might miss.
* Compliance and Regulation: Many industries (such as healthcare and finance) are legally required by frameworks like HIPAA or PCI DSS to conduct regular security assessments to ensure data privacy.
* Testing Defense Capabilities: It allows the organization's "Blue Team" (defenders) to practice their incident response and detection capabilities against a controlled "Red Team" (attackers) threat.
* Cost Avoidance: Discovering a vulnerability through a pentest is significantly cheaper than dealing with the aftermath of a genuine data breach, which involves legal fees, loss of customer trust, and potential regulatory fines.
In a digital landscape where threats are constantly evolving, pentesting provides a "snapshot" of an organization's security posture at a specific point in time. By adopting the mindset of an attacker, companies can gain actionable insights into how to harden their perimeters and internal networks. This continuous cycle of testing and remediation is essential for maintaining the confidentiality, integrity, and availability of data in an increasingly hostile online environment.

NEW QUESTION: 28
Can an FTP protocol be breached?
A. NO, it is very safe.
B. YES, with the appropriate techniques.
C. YES, asking the administrator for the user and password.
Answer: B (LEAVE A REPLY)
The File Transfer Protocol (FTP) is one of the oldest and most widely used protocols for moving files across a network. However, from a security standpoint, standard FTP is inherently vulnerable because it was designed without security in mind. It transmits all data, including sensitive login credentials (usernames and passwords), in "cleartext". This means that anyone with the ability to "sniff" or intercept the network traffic- using tools like Wireshark-can easily read the credentials as they pass through the network.
A breach of the FTP protocol is highly possible using appropriate techniques such as man-in-the-middle (MITM) attacks, brute-forcing, or exploiting specific vulnerabilities in the FTP server software itself. Because FTP does not use encryption, it provides a massive attack vector for hackers to steal data or gain a foothold in an organization's internal systems.

While asking an administrator (Option C) is a form of social engineering, the technical breach refers to the exploitation of the protocol's inherent weaknesses.
To mitigate this attack vector, ethical hacking strategies strongly advocate for the replacement of standard FTP with secure alternatives like SFTP (SSH File Transfer Protocol) or FTPS (FTP over SSL/TLS). These protocols encrypt both the credentials and the data being transferred, rendering intercepted information unreadable. In a professional penetration test, checking for open FTP ports and attempting to sniff traffic or use default credentials are standard procedures to demonstrate the risk of using legacy, unencrypted protocols in a modern network environment.

NEW QUESTION: 29
What is a White Hat hacker?
A. A cybersecurity professional who uses their skills to legally identify and fix vulnerabilities in systems, networks, or applications to improve security.
B. A person who creates exploits solely to expose vulnerable systems without authorization.
C. A hacker who exploits vulnerabilities to steal or sell sensitive information for personal profit.
Answer: A (LEAVE A REPLY)
A White Hat hacker is atrusted cybersecurity professionalwho uses hacking skills ethically and legally to improve system security, making option A the correct answer. White Hat hackers operate with explicit authorization from system owners and follow strict legal and professional guidelines.
White Hats perform tasks such as vulnerability assessments, penetration testing, code reviews, and security audits. Their objective is not to cause harm but to identify weaknesses before malicious attackers exploit them. Their work directly contributes to risk reduction, regulatory compliance, and improved organizational resilience.
Option B is incorrect because creating and exploiting vulnerabilities without authorization is unethical and illegal. Option C describes a Black Hat hacker, whose actions are driven by financial gain and disregard for damage caused.
Understanding hacker classifications is essential in ethical hacking education. White Hats represent the defensive and professional side of hacking, often working as security consultants, internal security teams, or researchers.
White Hat hacking promotes responsible disclosure, secure development practices, and continuous improvement of security controls. Their role is fundamental to modern cybersecurity defense strategies.

NEW QUESTION: 30
Is it illegal to practice with vulnhub machines?
A. NO, since these machines do not have existing vulnerabilities, it is only useful to see them.

B. YES, you are hacking into a system without authorization.
C. NO, since these machines are in a local environment and do not have contact with any organization.
Answer: C (LEAVE A REPLY)
In the field of ethical hacking, the distinction between legal skill-building and criminal activity is defined primarily by authorization and consent. Legislation such as the Computer Misuse Act (CMA) 1990 makes it a criminal offense to access computer material without explicit permission from the owner. However, practicing with "VulnHub" machines is entirely legal and considered an industry best practice for developing technical proficiency. VulnHub provides intentionally vulnerable virtual machine (VM) images that researchers download and run within their own isolated, local environments. Because the individual practicing is the owner and administrator of the physical host machine and the virtualized target, they have absolute "authorization" to conduct testing. These machines are specifically designed to be disconnected from external networks or organizations, ensuring that the hacking activity remains confined to a "safe lab" environment.
Practicing in such a sandbox allows an ethical hacker to refine their exploitation techniques-such as reconnaissance, scanning, and gaining access-without risk of harming third-party systems or violating privacy laws. It provides a controlled setting where the "intent" is educational rather than malicious.
Conversely, testing these same techniques against any external website or network without a formal contract and written scope would be a serious crime punishable by imprisonment. Therefore, using locally hosted vulnerable labs like VulnHub is not only legal but essential for any professional aspiring to earn certifications like the OSCP while staying within the confines of ethical and legal boundaries.

NEW QUESTION: 31
On which website can you check if your email account has been compromised?
A. https://facebook.com
B. https://haveibeenpwned.com
C. https://rincondelvago.com
Answer: B (LEAVE A REPLY)
The correct platform used to check whether an email address has been involved in known data breaches is
https://haveibeenpwned.com
, making option B the correct answer. This service aggregates data from publicly disclosed breaches and allows users to verify if their credentials have been exposed.
Understanding data breaches is a key part of current security trends, as credential leaks remain one of the most common causes of account compromise. Ethical hackers, security professionals, and even everyday users use such services to assess exposure and take corrective action, such as changing passwords or enabling multi-factor authentication.

Option A, Facebook, is a social media platform and does not provide breach-checking services. Option C is unrelated and does not serve any cybersecurity or breach-monitoring function.
From an ethical hacking standpoint, breach-awareness tools help reinforce proactive defense strategies. They raise awareness of credential reuse risks and demonstrate how leaked data can be weaponized in phishing, credential stuffing, and social engineering attacks.
Monitoring breach exposure is not hacking; it is a defensive security measure. Ethical hackers use this knowledge to educate organizations on password hygiene, the importance of unique credentials, and the implementation of identity protection controls. Staying informed about breaches is essential in modern cybersecurity environments.

NEW QUESTION: 32
Is it possible to clone a web page?
A. No
B. Yes
Answer: (SHOW ANSWER)
Yes, it is possible to clone a web page, making option B the correct answer. Web page cloning involves copying the structure, appearance, and content of a legitimate website, often for malicious purposes such as phishing or credential harvesting.
Attackers use cloning to trick users into believing they are interacting with a trusted site. Ethical hackers study this technique to demonstrate the risks of social engineering and help organizations implement defenses such as user education, domain monitoring, and email security controls.
Cloning does not typically require exploiting vulnerabilities; instead, it abuses publicly available content and human trust. This makes it a powerful and common attack vector. Understanding web page cloning helps organizations recognize phishing threats and protect users from impersonation attacks. Ethical hackers use controlled demonstrations to raise awareness and improve detection capabilities.

NEW QUESTION: 33
What is the main purpose of a "SQL injection" attack?

A. Accessing an organization's network.
B. Intercepting web traffic.
C. Exploiting a database by manipulating SQL commands.
Answer: (SHOW ANSWER)
SQL Injection (SQLi) is one of the most prevalent and damaging information security threats targeting web applications. Its main purpose is to exploit a database by manipulating Structured Query Language (SQL) commands through user-supplied input. This occurs when an application fails to properly filter or "sanitize" data entered into forms, URL parameters, or cookies, allowing an attacker to "inject" their own SQL code into the query that the application sends to the back-end database.
When successful, a SQL injection attack can have catastrophic consequences for an organization's data integrity and confidentiality. An attacker can bypass authentication to log in as an administrator without a password, view sensitive user data, modify or delete database records, and in some cases, gain administrative control over the entire database server. A classic example is the ' OR 1=1 -- injection, which forces a query to return "true" regardless of the credentials provided, effectively opening the door to the system.
Managing the threat of SQLi is a top priority for web security. The most effective defense is the use of
"Parameterized Queries" (also known as prepared statements), which ensure that the database treats user input as data rather than executable code. Additionally, implementing "Input Validation" and the "Principle of Least Privilege" for database accounts helps mitigate the potential damage. From an ethical hacking standpoint, identifying SQLi vulnerabilities is a core component of vulnerability scanning and manual testing. Because databases often hold an organization's most valuable assets-including customer identities and financial records-protecting them from injection attacks is a non-negotiable aspect of modern information security management.

NEW QUESTION: 34
Do Google dorks show hacked computers?
A. YES, Google dorks hacks pages for us in order to access data.
B. NO, Google dorks works to search for specific topics.
C. YES, Google dorks works as a backdoor to all web pages.
Answer: (SHOW ANSWER)
Google Dorking, also known as Google Hacking, is a passive reconnaissance technique that involves using advanced search operators to filter through the vast index of the Google search engine. It is important to clarify that Google Dorks do not "hack" computers or websites themselves; rather, they utilize the search engine's indexing power to find information that has already been made public-often inadvertently. By using specific strings like filetype:log, intitle:"index of", or inurl:admin, a researcher can locate sensitive directories, exposed log files, or configuration pages that were never intended to be indexed by search bots.

From a threat management perspective, Google Dorking is a double-edged sword. Ethical hackers use it during the information-gathering phase of a penetration test to see what an organization is leaking to the public web. This might include SQL error messages, which can reveal database structures, or publicly accessible backup files containing sensitive credentials. However, the tool itself is not a "backdoor" or an exploit; it is a sophisticated way of querying a database of cached website content.
If a computer or server appears in a Google Dork result, it typically means the administrator failed to configure the robots.txt file or server permissions correctly, allowing Google's crawlers to document the internal structure. Managing this threat involves regular "dorking" of one's own domain to ensure that no sensitive paths or files are visible to the public. Understanding that Google Dorks are simply advanced search queries helps security professionals realize that the "leak" occurs at the server configuration level, not within the search engine itself. Consequently, remediation focuses on tightening access controls and ensuring that internal-only resources are not reachable or indexable by external search engines.

NEW QUESTION: 35
What is malware?
A. Refers to any software specifically designed to protect, safeguard and store data on a device, network or system.
B. Refers to any software specifically designed to damage, infect, steal data or otherwise cause a nuisance to a device, network or system without the owner's consent.
C. It is an Antivirus for servers especially.
Answer: (SHOW ANSWER)
Malware, short for "malicious software," is a broad category of software specifically engineered to perform unauthorized and often harmful actions on a computer system, network, or device. Its primary characteristic is that it operateswithout the owner's consent. Malware is the primary tool used by cybercriminals to achieve various objectives, ranging from financial gain to corporate espionage and simple disruption.
Malware encompasses several distinct types, each with its own method of infection and goal:
* Viruses and Worms: Designed to spread from one file or computer to another, often damaging data or consuming network bandwidth along the way.
* Trojan Horses: Programs that disguise themselves as legitimate software to trick users into installing them, only to reveal a malicious "payload" once active.
* Ransomware: Encrypts the victim's data and demands payment for the decryption key.
* Spyware and Stealers: Secretly monitor user activity or steal sensitive information like passwords and credit card numbers.
* Rootkits: Specialized malware designed to provide high-level "root" access while remaining hidden from the operating system and antivirus software.

Ethical hackers study malware to understand how to defend against it. This involves analyzing "Attack Vectors" (how malware enters a system), "Persistence Mechanisms" (how it stays there), and "Command and Control" (how it communicates with the attacker). Protecting against malware requires a multi-layered defense strategy, including updated antivirus software, strictAcceptable Use Policies (AUP), and regular vulnerability scanning to close the gaps that malware exploits to infect systems.

NEW QUESTION: 36
What is a "flag" in the context of cybersecurity competitions like Capture the Flag (CTF)?
A. A file inside the machine with a key word or letters to check that it was successfully breached.
B. A common flag with a pirate skull in meaning of hackers.
C. A list of commands used as a guide to hack the machine.
Answer: A (LEAVE A REPLY)
In the context of ethical hacking, "Capture the Flag" (CTF) is a specialized competition or training exercise designed to sharpen the technical skills of cybersecurity professionals. A "flag" is a specific piece of data- often a unique alphanumeric string or a specific file-hidden within a target system, server, or application.
The primary purpose of the flag is to serve as objective proof that an ethical hacker or penetration tester has successfully navigated the security layers of a machine and achieved a specific level of access, such as user- level or administrative (root) access.
From a technical standpoint, flags are strategically placed in directories that are typically restricted, such as
/root or /home/user in Linux environments, or within sensitive database tables. Finding the flag confirms that the attacker has exploited a specific vulnerability, such as a misconfiguration, a weak password, or a software flaw. This methodology is integral to the "Post-Exploitation" phase of a penetration test, where the goal is to demonstrate the impact of a breach.
In professional certification environments like the CEH (Certified Ethical Hacker) or platforms like TryHackMe and Hack The Box, these flags are submitted to a scoring engine to validate the completion of a task. Unlike the popularized imagery of "pirate flags" or simple command lists, a real-world digital flag is a cryptographic validator of a successful exploit. It ensures that the practitioner did not just stumble upon a system but actually manipulated its internal logic to extract sensitive information. Understanding the nature of flags helps researchers focus on the ultimate goal: identifying where sensitive data resides and how it can be protected against unauthorized extraction by malicious actors.

NEW QUESTION: 37
What is Nessus used for?
A. To watch videos on a blocked network.
B. To scan a network or system for vulnerabilities.

C. For automated hacking.
Answer: B (LEAVE A REPLY)
Nessus is a globally recognized, industry-standardvulnerability scannerused by security professionals to identify security flaws in a network, operating system, or application. Developed by Tenable, it is a comprehensive tool that automates the process of finding weaknesses such as unpatched software, weak passwords, misconfigurations, and "zero-day" vulnerabilities.
Nessus operates by probing a target system and comparing the results against an extensive, constantly updated database of thousands of known vulnerabilities (plugins). The scanning process typically involves:
* Host Discovery: Identifying which devices are active on the network.
* Port Scanning: Checking for open services and identifying their versions.
* Vulnerability Assessment: Running specific checks to see if those services are susceptible to known exploits.
* Compliance Auditing: Ensuring that systems meet specific security standards like PCI DSS or HIPAA.
Unlike "automated hacking" tools that focus on exploitation, Nessus is adiagnostic tool. It provides detailed reports that categorize vulnerabilities by severity (Critical, High, Medium, Low) and offers specific remediation advice on how to fix the issues. In a professional penetration test, Nessus is used during the
"Vulnerability Analysis" phase to provide a broad map of the target's weaknesses. This allows the tester to prioritize which flaws to attempt to exploit manually. Regular use of Nessus is a cornerstone of any proactive vulnerability management program.

NEW QUESTION: 38
Can the FTP protocol be breached?
A. Yes, by asking the administrator for credentials.
B. Yes, using appropriate attack techniques.
C. No, FTP is very secure.
Answer: B (LEAVE A REPLY)
Yes, the FTP protocol can be breached, making option B the correct answer. FTP transmits usernames, passwords, and datain clear text, which makes it highly vulnerable to interception and attack.
Attackers can exploit FTP through techniques such as credential sniffing, brute-force attacks, anonymous access abuse, and man-in-the-middle attacks. Ethical hackers frequently demonstrate FTP weaknesses during penetration testing to highlight the risks of using outdated protocols.
Option A is incorrect because asking for credentials is not an attack technique. Option C is incorrect because FTP is considered insecure by modern security standards.
From a defensive standpoint, FTP should be replaced with secure alternatives such asSFTP or FTPS, which encrypt authentication and data transfers. Ethical hackers use

FTP breach demonstrations to encourage protocol modernization and better access controls.
Understanding insecure protocols is essential for managing information security threats. Eliminating weak services like FTP significantly reduces an organization's attack surface and exposure to credential compromise.

NEW QUESTION: 39
What is Phishing?
A. It is a type of cyber-attack in which attackers try to trick people to obtain confidential information, such as usernames.
B. It is the method to brute force passwords in web pages.
C. It is a technique used to capture network traffic in order to obtain passwords in plain text.
Answer: (SHOW ANSWER)
Phishing is a widespread form of social engineering where an attacker sends deceptive communications that appear to come from a reputable source, such as a bank, a popular web service, or even an internal IT department. The primary goal is to trick the recipient into revealing sensitive personal or corporate information, such as usernames, passwords, credit card numbers, or proprietary data.
A typical phishing attack often involves an email or text message that creates a sense of urgency-for example, claiming there has been "unauthorized activity" on an account and providing a link to "verify your identity". This link leads to a fraudulent website that looks identical to the legitimate one. When the victim enters their credentials, they are directly handed over to the attacker.
Phishing has evolved into several specialized categories:
* Spear Phishing: Targeted attacks aimed at a specific individual or organization, often using personalized information to increase the appearance of legitimacy.
* Whaling: A form of spear phishing directed at high-level executives (CEOs, CFOs) to steal high-value information or authorize large wire transfers.
* Vishing and Smishing: Phishing conducted via voice calls (Vishing) or SMS text messages (Smishing).
From an ethical hacking perspective, phishing simulations are a critical part of a security assessment because they test the "human firewall." Even the most advanced technical defenses can be bypassed if an employee is manipulated into providing their login token or clicking a malicious attachment. Protecting against phishing requires a combination of technical controls (email filters, MFA) and constant user awareness training.

NEW QUESTION: 40
What is a CVE?
A. Common Non-Vulnerable Entries that list secure systems.
B. A hacker magazine available for purchase.

C. Common Vulnerabilities and Exposures (CVE) is a publicly available list of known computer security vulnerabilities.

Answer: (SHOW ANSWER)

CVE stands forCommon Vulnerabilities and Exposures, making option C the correct answer. CVE is a standardized system used to identify, name, and catalog publicly disclosed cybersecurity vulnerabilities.

Each CVE entry is assigned a unique identifier, allowing security professionals worldwide to reference the same vulnerability consistently. Ethical hackers, system administrators, and security vendors rely on CVEs to track vulnerabilities, assess risk, and prioritize patching efforts.

Option A is incorrect because CVEs catalog vulnerabilities, not secure systems. Option B is incorrect because CVE is not a publication or magazine.

From an ethical hacking perspective, CVEs play a crucial role in vulnerability management and penetration testing. Ethical hackers reference CVEs to understand exploitability, identify affected systems, and demonstrate risk using documented evidence.

Understanding CVEs supports effective communication between security teams, vendors, and management.

They are foundational to modern vulnerability scanning, patch management, and threat intelligence programs.

NEW QUESTION: 41

What is a security breach?

A. A cybersecurity incident that results in unauthorized access to personal or corporate data.

B. The hacking of the entire internet.

C. An internet shutdown or breakup.

Answer: A (LEAVE A REPLY)

A security breach is acybersecurity incident in which unauthorized individuals gain access to sensitive personal or organizational data, making option A the correct answer. Security breaches can involve data theft, data exposure, system compromise, or loss of confidentiality, integrity, or availability.

Breaches may occur due to malware infections, phishing attacks, weak credentials, unpatched vulnerabilities, insider threats, or misconfigured systems. Ethical hackers analyze breach scenarios to understand how attackers bypass defenses and what impact the breach can have on business operations.

Option B is incorrect because hacking the entire internet is unrealistic and not a valid definition. Option C is incorrect because internet outages are infrastructure issues, not necessarily security breaches.

From a defensive standpoint, understanding security breaches helps organizations improve detection, response, and recovery capabilities. Ethical hackers help simulate breach scenarios to identify gaps in monitoring and incident response plans.

Preventing breaches requires layered security controls, user awareness, continuous monitoring, and regular testing. Ethical hacking plays a critical role in reducing breach likelihood and impact.

NEW QUESTION: 42
What is risk assessment?
A. It is the process to buy antivirus.
B. Is the process of comparing the results of the risk analysis with the risk assessment criteria to determine whether the risk or its magnitude is acceptable or tolerable.
C. It is the process of comparing the results of the analysis with other companies.
Answer: B (LEAVE A REPLY)
Risk assessment is a systematic and critical component of information security management. It is the process of identifying, analyzing, and evaluating risks to determine their significance and to prioritize how they should be addressed. According to formal security standards, it involves comparing the findings of arisk analysis-which identifies threats and vulnerabilities-against establishedrisk assessment criteria. These criteria represent the organization's "risk appetite," or the level of risk they are willing to accept in exchange for pursuing their business objectives.
The risk assessment process typically involves three major steps:
* Identification: Finding out what could happen and why (e.g., identifying that a database is vulnerable to SQL injection).
* Analysis: Determining the likelihood of a threat occurring and the potential impact it would have on the organization's confidentiality, integrity, or availability.
* Evaluation: Deciding whether the resulting risk level isacceptable or tolerable.
If a risk is deemed intolerable, the organization must decide on a treatment strategy:Mitigation(reducing the risk via controls like firewalls),Transfer(buying insurance),Avoidance(stopping the risky activity), orAcceptance(acknowledging the risk if the cost of fixing it is too high). For an ethical hacker, a risk assessment provides the context for their work; it helps them understand which assets are most critical to the business and ensures that their findings are prioritized based on actual business impact rather than just technical severity.

NEW QUESTION: 43
What is malware?
A. Refers to any software specifically designed to protect, safeguard and store data on a device, network or system.
B. Refers to any software specifically designed to damage, infect, steal data or otherwise cause a nuisance to a device, network or computer system, without the owner's consent.
C. It is an Antivirus for servers especially.
Answer: B (LEAVE A REPLY)

Malware, short for "malicious software," is a broad category of intrusive software developed by cybercriminals to compromise the confidentiality, integrity, or availability of a victim's data. It encompasses a wide variety of threats, including viruses, worms, Trojans, ransomware, and spyware. The defining characteristic of malware is that it is installed and executed on a system without the explicit consent or knowledge of the owner, with the primary intent of causing harm, stealing sensitive information, or gaining unauthorized access.
Managing malware as a security threat involves understanding its infection vectors and payload behaviors.
Viruses attach themselves to legitimate files and spread through user interaction, while worms are self- replicating and spread across networks automatically by exploiting vulnerabilities. Trojans disguise themselves as useful programs to trick users into executing them, often opening "backdoors" for further exploitation. Ransomware, one of the most profitable forms of malware today, encrypts a user's files and demands payment for the decryption key.
Ethical hackers study malware to develop better detection signatures and behavioral analysis techniques. By analyzing how malware obfuscates its code or communicates with a Command and Control (C2) server, security professionals can implement better endpoint protection and network monitoring. Protecting against malware requires a multi-layered defense strategy, including up-to-date antivirus software, regular system patching, and user awareness training to prevent the execution of suspicious attachments or links.
Understanding the diverse nature of malware is essential for any cybersecurity expert, as it remains the primary tool used by attackers to gain a foothold within targeted organizations.

NEW QUESTION: 44
What is Netcat?
A. It is a hacking tool designed only for Windows systems.
B. It is a versatile, open-source networking tool used for reading and writing data over network connections.
C. It is a hacking tool designed only for Linux systems.
Answer: (SHOW ANSWER)
Netcat, often referred to as the"Swiss Army knife of networking,"is a versatile, open-source tool used for reading from and writing to network connections using TCP or UDP. This makes option B the correct answer.
Netcat is widely used in ethical hacking, penetration testing, and system administration due to its flexibility and simplicity.
Netcat can perform a wide range of networking tasks, includingport scanning, banner grabbing, file transfers, reverse shells, bind shells, and debugging network services. It is commonly used during thereconnaissance, exploitation, and post-exploitation phasesof ethical hacking. Because of its ability to create raw network connections, it can simulate both client and server behavior.

Option A and option C are incorrect because Netcat iscross-platformand works on Linux, Windows, macOS, and other Unix-like systems. It is not limited to a single operating system, nor is it exclusively a hacking tool; it is also used legitimately by network administrators for troubleshooting and testing.
From a defensive security perspective, understanding Netcat is important because attackers frequently abuse it to establish unauthorized communication channels or backdoors. Ethical hackers use Netcat responsibly to demonstrate how weak configurations or exposed services can be exploited.
By identifying improper Netcat usage during assessments, organizations can improve monitoring, restrict unnecessary outbound connections, and strengthen endpoint security controls.

NEW QUESTION: 45
What is a reverse shell?
A. It refers to when the terminal is run with root privileges.
B. A common Linux command-line console.
C. It refers to a process in which the victim's machine initiates a connection back to the attacker's machine to receive commands.
Answer: (SHOW ANSWER)
A reverse shell is a technique used in ethical hacking and penetration testing where the target (victim) system initiates a connection back to the attacker's system, allowing the attacker to execute commands remotely. This makes option C the correct answer.
Unlike a bind shell, where the victim opens a listening port, a reverse shell is particularly effective in environments protected by firewalls or Network Address Translation (NAT). Since outbound connections are often allowed, the victim system connects outward to the attacker, bypassing many network restrictions.
Ethical hackers commonly use reverse shells during the exploitation and post-exploitation phases of penetration testing to maintain access to compromised systems.
Option A is incorrect because running a terminal as root does not define a reverse shell.
Option B is incorrect because a reverse shell is not a standard command-line interface but rather a remote command execution channel.
From an ethical hacking perspective, reverse shells help demonstrate the real-world impact of vulnerabilities such as command injection, remote code execution, or misconfigured services. Once established, a reverse shell may allow privilege escalation, lateral movement, or data exfiltration-highlighting serious security risks.
Understanding reverse shells is essential for both attackers and defenders. Defenders can mitigate reverse shell attacks by implementing strict egress filtering, intrusion detection systems, endpoint protection, and proper system hardening. Ethical testing of reverse shells enables organizations to identify weaknesses and improve overall security posture.

NEW QUESTION: 46

Can ransomware attacks happen to anyone or only to large companies?
A. We can all be infected by ransomware.
B. Only large companies with very important data.
C. Only computers with Windows 7 and XP.
Answer: A (LEAVE A REPLY)
Ransomware is a pervasive and devastating form of malware that encrypts a victim's files, rendering them inaccessible until a ransom, typically in cryptocurrency, is paid to the attacker. A critical misconception in modern cybersecurity is that ransomware only targets high-value, large-scale organizations. In reality, anyonewith an internet-connected device is a potential target. While high-profile attacks on hospitals or infrastructure make the headlines, individuals, small businesses, and non-profits are frequently infected daily. Attackers utilize varied methods to spread ransomware, many of which are non-discriminatory. These include:
* Phishing: Sending mass emails with malicious attachments or links that, once clicked, execute the ransomware payload.
* Exploiting Vulnerabilities: Automated bots scan the internet for unpatched software or exposed services (like RDP) to gain entry regardless of the target's identity.
* Malvertising: Injecting malicious code into legitimate online advertising networks.
The shift toward "Ransomware-as-a-Service" (RaaS) has lowered the barrier to entry for criminals, allowing even low-skilled attackers to launch wide-reaching campaigns. For an individual, the loss of personal photos or tax documents can be just as traumatic as a data breach is for a company. Because ransomware can strike any operating system or device type, ethical hacking principles emphasize that every user must maintain a proactive defense. This includes regular data backups, keeping software updated to close security holes, and exercising extreme caution with email communication.

NEW QUESTION: 47
Do hackers only use Linux?
A. Yes, since Linux is the only platform that works correctly for these tasks.
B. Linux and Windows only.
C. No, hackers use all operating systems.
Answer: C (LEAVE A REPLY)

While Linux distributions like Kali Linux and Parrot OS are highly favored by the security community due to their open-source nature and pre-installed toolkits, it is a misconception that hackers exclusively use Linux.
Malicious actors and ethical hackers alike utilizeall operating systems, including Windows, macOS, and mobile platforms (Android/iOS), depending on their specific objectives.
The choice of operating system is often driven by the "Target Environment." For example:
* Windows: Many hackers use Windows because it is the most prevalent OS in corporate environments.
To develop effective exploits for Windows-based active directories or software, it is often necessary to work within a Windows environment using tools like PowerShell and the .NET framework.
* macOS: This platform is popular among researchers and developers due to its Unix-based core combined with a high-end commercial interface, allowing for a seamless transition between development and security tasks.
* Linux: Linux remains the "OS of choice" for heavy networking tasks, server-side exploits, and automated scripts because of its transparency and the power of its terminal.
Furthermore, hackers often use specialized hardware or mobile devices to conduct "War Driving" (scanning for Wi-Fi) or "Skimming" attacks. In a modern penetration test, a professional might use a Linux machine for reconnaissance, a Windows machine for testing Active Directory vulnerabilities, and a mobile device for testing application security.
An effective hacker must be cross-platform proficient, understanding the unique vulnerabilities and command-line interfaces of every major operating system to successfully navigate a target's network.

NEW QUESTION: 48
Are brute force attacks extremely fast and effective?
A. NO, this type of attack take a long time and there is a probability that it will not work.
B. YES, since the dictionaries on the Internet are very complete.
C. YES, no matter what specifications your computer has.
Answer: A (LEAVE A REPLY)
A brute force attack is a trial-and-error method used to decode encrypted data such as passwords or Data Encryption Standard (DES) keys through exhaustive effort rather than intellectual strategies. The fundamental premise is that the attacker (or their software) attempts every possible combination of characters until the correct one is found. While it is technically "effective" in that it will eventually work given infinite time and resources, in practical application, it is often neither fast nor guaranteed to succeed.
The primary limitation of brute force attacks is time. As password complexity increases (the addition of uppercase letters, numbers, and special symbols), the number of possible combinations grows exponentially.

For a high-entropy password, a standard brute force attack might take years or even centuries to complete, making it practically useless for an immediate breach. Furthermore, modern security systems implement
"lockout" policies-such as freezing an account after three failed attempts-which effectively shuts down automated brute force attempts.
Ethical hackers distinguish between "pure" brute force and "dictionary attacks". A dictionary attack uses a pre- compiled list of common words and previously leaked passwords, which is significantly faster than trying every character combination but only works if the victim uses a common or weak password. To mitigate brute force risks, organizations use "salting" (adding random data to passwords before hashing) and multi-factor authentication (MFA). Therefore, while brute force remains a valid threat vector that must be tested, it is generally considered a "last resort" for an attacker due to its high time cost and high probability of detection or failure.

NEW QUESTION: 49
Which of the following is a Linux distribution dedicated to security auditing and penetration testing?
A. Hannah Montana Linux.
B. Windows XP.
C. Parrot OS.
Answer: C (LEAVE A REPLY)
While Kali Linux is arguably the most recognized operating system in the cybersecurity industry, Parrot OS (Parrot Security OS) is a prominent and highly capable alternative preferred by many security professionals and ethical hackers. Developed by the Frozenbox Network, Parrot OS is based on Debian, much like Kali, but it emphasizes a different philosophy regarding system resources and privacy. Parrot OS is designed to be lightweight and highly portable, often performing better on older hardware or in virtualized environments with limited resources. It comes pre-installed with a vast repository of security tools categorized for information gathering, vulnerability analysis, exploitation, and post-exploitation.
One of the defining features of Parrot OS is its focus on developer-friendly environments and anonymity. It includes "AnonSurf," a pre-configured script that routes all system traffic through the Tor network, providing a layer of privacy for researchers conducting sensitive investigations. Additionally, Parrot OS is often praised for its "Home" edition, which serves as a secure daily-driver operating system for general use, and its
"Security" edition, which is fully loaded for penetration testing. In contrast to Kali's "root by default" history (which has since changed), Parrot OS was built from the ground up with a standard user model to improve security. For an ethical hacker, choosing between Kali and Parrot often comes down to personal preference for the desktop environment (Kali uses XFCE/GNOME/KDE, while Parrot traditionally favors MATE) and specific workflow requirements. Both systems provide the necessary toolsets-such as Nmap, Wireshark,

Burp Suite, and Metasploit-to conduct comprehensive security audits across various network architectures.
Understanding the landscape of security-focused distributions is vital for a professional to select the best tool for a specific operational context.

NEW QUESTION: 50
What is a flag inside intentionally vulnerable machines?
A. A list of commands used as a guide to hack the machine.
B. A file inside the machine containing a keyword or string that proves the system was successfully compromised.
C. A symbolic pirate flag representing hackers.
Answer: B (LEAVE A REPLY)
In penetration testing labs and intentionally vulnerable machines, a flag is afile or string placed inside the system to verify successful exploitation, making option B the correct answer. Flags are commonly used in Capture The Flag (CTF) challenges, training platforms, and vulnerable virtual machines.
Flags typically contain a unique keyword, hash, or identifier that can only be accessed after exploiting a vulnerability or achieving a specific level of access, such as user or root privileges. Ethical hackers use flags to confirm progress and validate that attack objectives have been met.
Option A is incorrect because flags do not provide instructions or guidance. Option C is incorrect because flags are not symbolic images or representations.
From an ethical hacking education perspective, flags serve asmeasurable proof of exploitation success. They help learners track achievements and ensure that vulnerabilities were exploited correctly rather than guessed or bypassed incorrectly.
Understanding flags reinforces structured penetration testing methodologies, clear objectives, and verification steps. In professional environments, flags conceptually translate to proof-of-concept evidence provided in penetration testing reports to demonstrate risk and impact.

NEW QUESTION: 51
Which of the following was a famous hacktivist group?
A. Anonymous
B. Fan7a5ma
C. Hackers
Answer: A (LEAVE A REPLY)
Anonymous is one of the most well-known and influential hacktivist groups in the history of cybersecurity, making option A the correct answer. Hacktivism refers to the use of hacking techniques to promote political, social, or ideological causes. Understanding hacktivist movements is important when studying current security trends, as these groups have significantly influenced cyber threat landscapes.

Anonymous is characterized as a decentralized collective, meaning it has no formal leadership or membership structure. Its activities have included distributed denial-of-service (DDoS) attacks, website defacements, data leaks, and online campaigns targeting governments, corporations, and organizations perceived to be unethical or oppressive. These actions have brought global attention to issues such as censorship, privacy, corruption, and human rights.
Option B, "Fan7a5ma," is not a widely recognized or historically significant hacktivist group, and option C,
"Hackers," is a generic term that describes individuals with technical skills rather than an organized hacktivist collective. Therefore, both are incorrect.
From an ethical hacking and defensive security perspective, studying groups like Anonymous helps organizations understand non-financially motivated threats. Hacktivist attacks often aim for public exposure, reputational damage, or service disruption rather than direct monetary gain. This requires different defensive strategies, including improved incident response, public communication planning, and monitoring of geopolitical and social developments that may trigger cyber campaigns.
Understanding hacktivist behavior is essential for modern cybersecurity professionals to anticipate emerging threats and strengthen organizational resilience.

NEW QUESTION: 52
What is the Lhost in metasploit?
A. Local host.
B. Host line.
C. Local hosting.
Answer: A (LEAVE A REPLY)
In the Metasploit Framework, LHOST stands forLocal Host. This is a critical configuration variable that specifies the IP address of the attacker's (tester's) machine. When an ethical hacker deploys an exploit- particularly one that utilizes areverse shell-the LHOST tells the victim's machine exactly where to send the connection back to.
Setting the LHOST correctly is vital for the success of an exploitation attempt. In most network environments, especially those involving NAT (Network Address Translation) or VPNs, the tester must ensure they use the IP address that is reachable by the target system. For instance, if the tester is on a local network, they would use their internal IP; however, if they are testing over a wider network or the internet, they must ensure the LHOST points to a public IP or a listener configured to handle the traffic.
Along with LPORT (Local Port), LHOST defines the listener on the attacker's machine. When the exploit executes on the target (RHOST), the payload initiates a connection back to the address defined in LHOST. If this variable is misconfigured, the exploit might successfully run on the victim's end, but the tester will never receive the shell, resulting in a failed attempt. For an ethical hacker, double-checking the LHOST and LPORT settings is a

standard "best practice" before launching any module to ensure a stable and reliable connection is established.

NEW QUESTION: 53
Can Nmap be used for vulnerability scanning?
A. YES, nmap has this capability as well.
B. NO, other software is used for that purpose.
C. NO, nmap can only perform port scanning.
Answer: A (LEAVE A REPLY)
Nmap (Network Mapper) is primarily known as a powerful tool for network discovery and port scanning, but it also possesses robust vulnerability scanning capabilities through theNmap Scripting Engine (NSE). The NSE allows users to write and share simple scripts to automate a wide variety of networking tasks. One of the core categories of scripts available in the NSE is vuln, which is specifically designed to detect known security vulnerabilities on the targets being scanned.
When an ethical hacker runs a scan with the flag --script vuln, Nmap will not only identify open ports but will also cross-reference the discovered services against its internal database of vulnerabilities. For example, if Nmap detects an old version of an SMB service, it can run specific scripts to check if that service is vulnerable to well-known exploits like EternalBlue (MS17-010).
While dedicated vulnerability scanners like Nessus or OpenVAS offer more comprehensive databases and reporting features, Nmap's vulnerability scanning is highly valued for being fast, lightweight, and scriptable.
It is an excellent tool for "quick-look" assessments during the reconnaissance phase. By using NSE, testers can also perform tasks beyond simple vulnerability detection, such as:
* Brute-forcing: Attempting to guess passwords for services like SSH or FTP.
* Malware Detection: Identifying if a server has been infected by certain types of worms or backdoors.
* Configuration Auditing: Checking for insecure default settings.
Integrating Nmap's vulnerability scanning into a penetration testing workflow allows for a more seamless transition from discovery to exploitation, making it one of the most versatile tools in a security professional's toolkit.

NEW QUESTION: 54
Security Vulnerabilities: Understanding Backdoors
A. A person who creates exploits with the sole purpose of exposing existing vulnerable systems.
B. It is a type of hacker who exploits vulnerabilities in search of information that can compromise a company and sell this information in order to make a profit regardless of the damage it may cause to the organization.

C. Refers to a computer security professional or expert who uses their skills and knowledge to identify and fix vulnerabilities in systems, networks or applications for the purpose of improving security and protecting against potential cyber threats.

Answer: C (LEAVE A REPLY)

The term "Whitehack," more commonly known as a "White Hat Hacker," describes individuals who utilize their technical expertise for ethical and legal purposes. These professionals are the cornerstone of the ethical hacking community. They operate under a strict code of ethics and, most importantly, always obtain explicit, written permission before conducting any security assessments or penetration tests. Their primary objective is to strengthen an organization's security posture by proactively discovering vulnerabilities before malicious actors (Black Hats) can exploit them.

White Hat hackers perform various tasks, including penetration testing, vulnerability assessments, security auditing, and developing security protocols. When they identify a flaw, they do not exploit it for personal gain or damage; instead, they document the finding in a comprehensive report and provide actionable remediation advice to the organization's IT and security teams. This collaborative approach helps organizations understand their weaknesses and allocate resources effectively to mitigate risks. Many White Hat hackers are certified professionals, holding credentials such as Certified Ethical Hacker (CEH) or Offensive Security Certified Professional (OSCP). They often work as security consultants, in-house security analysts, or as part of specialized "Red Teams" that simulate real-world attacks to test defensive capabilities. By mimicking the tactics, techniques, and procedures (TTPs) of real adversaries within a controlled and authorized framework, White Hats provide invaluable insights that automated tools alone cannot achieve. Their work is essential in the modern digital landscape, where the constant evolution of threats requires a defensive strategy that is equally dynamic and informed by a deep understanding of the "hacker mindset." Ultimately, the distinction between a White Hat and other types of hackers is defined by intent, authorization, and the commitment to improving the safety of the digital ecosystem.