



CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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 gather information about a service running on an open port, which often includes the version number of the application or server. Here's why banner grabbing is the correct Answer

? Banner Grabbing: It involves connecting to a service and reading the welcome banner or response, which typically includes version information. This is a direct method to identify the version number of a web application server.

? SSL Certificate Inspection: While it can provide information about the server, it is not reliable for identifying specific application versions.

? URL Spidering: This is used for discovering URLs and resources within a web application, not for version identification.

? Directory Brute Forcing: This is used to discover hidden directories and files, not for identifying version information.

References from Pentest:

? Luke HTB: Shows how banner grabbing can be used to identify the versions of services running on a server.

? Writeup HTB: Demonstrates the importance of gathering version information through techniques like banner grabbing during enumeration phases.

Conclusion:

Option C, banner grabbing, is the most appropriate technique for confirming the version number of a web application server.

=====

NEW QUESTION 2

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.

References 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.

=====

NEW QUESTION 3

DRAG DROP

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

INSTRUCTIONS

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

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

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

Your Partner of IT Exam *visit - <https://www.exambible.com>*

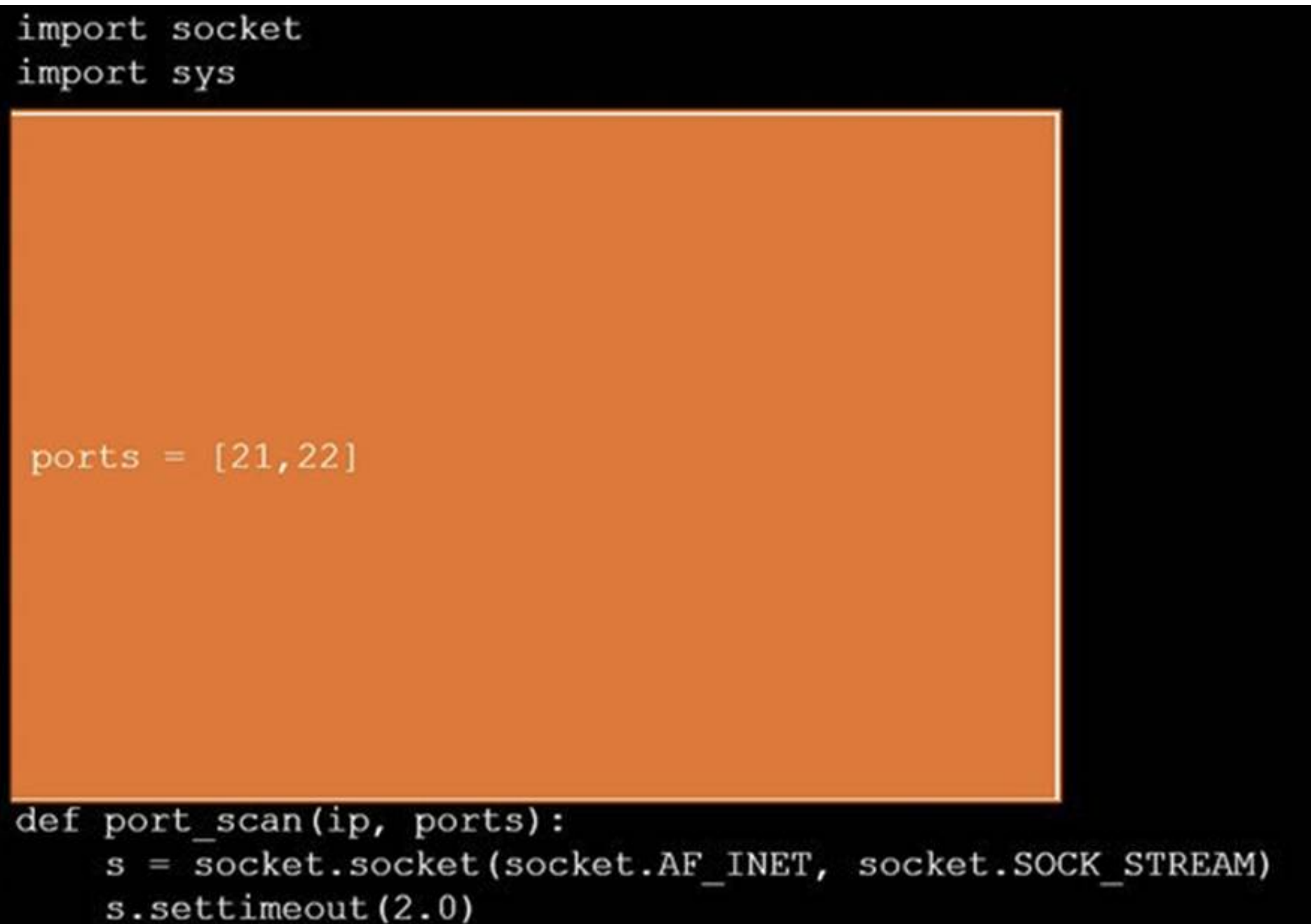
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



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



```
import socket
import sys

ports = [21, 22]

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

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

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

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

    finally
        s.close()
```

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

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

NEW QUESTION 4

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
- B. Configure Evilginx to bypass two-factor authentication using a phishlet that simulates the mail portal for the company.
- C. Configure Gophish to use an external domain
- D. Clone the email portal web page from the company and get the two-factor authentication code using a brute-force attack method.
- E. Configure an external domain using a typosquatting technique

- F. Configure SET to bypass two-factor authentication using a phishlet that mimics the mail portal for the company.
- G. Configure Gophish to use an external domain
- H. 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:

? Typosquatting:

? Steps:

Pentest References:

? 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.

=====

NEW QUESTION 5

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

? Option B: nc -tulpn 1234 192.168.1.2

? Option C: responder.py -I eth0 -wP

? Option D: crackmapexec smb 192.168.1.0/24

References 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.

=====

NEW QUESTION 6

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:

? User Enumeration:

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

? uk.co.certification.simulator.questionpool.PList@10ddf175 smbclient -L //192.168.50.2 -U anonymous

? Advantages:

? References from Pentesting Literature: References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 7

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:

? Usage in Threat Modeling:

? Process:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 8

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:

Metadata services in cloud environments provide information about the configuration and instance details, including sensitive data used during the initialization of virtual machines. Attackers can access this information to exploit and gain unauthorized access.

? Understanding Metadata Services:

? Common Information Exposed:

? Security Risks:

? Best Practices:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 9

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.

References 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.

=====

NEW QUESTION 10

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

- A. Network configuration errors in Kubernetes services
- B. Weaknesses and misconfigurations in the Kubernetes cluster
- C. Application deployment issues in Kubernetes
- D. Security vulnerabilities specific to Docker containers

Answer: B

Explanation:

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

? Kube-hunter: It scans Kubernetes clusters to identify security issues, such as

misconfigurations, insecure settings, and potential attack vectors.

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

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

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

References from Pentest:

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

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

Conclusion:

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

=====

NEW QUESTION 10

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.

References from Pentest:

? Anubis HTB: Demonstrates the process of cleaning up and ensuring that all implants are removed after an assessment.

? Forge HTB: Highlights the importance of thoroughly cleaning up and terminating any payloads or implants to leave the environment secure post-assessment.

=====

NEW QUESTION 11

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

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

Answer: C

Explanation:

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

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

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

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

? Server-Side Template Injection: This involves injecting code into server-side templates, not JavaScript that executes in the user??s browser.

References from Pentest:

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

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

=====

NEW QUESTION 13

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):

? Other Attacks:

Pentest References:

? 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

=====

NEW QUESTION 16

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

? Option B: Hydra

? Option C: BloodHound

? Option D: CrackMapExec

References from Pentest:

? Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.

? Horizontall HTB: Shows how CrackMapExec can be used for various post- exploitation activities, including using NTLM hashes to authenticate and execute commands.

Conclusion:

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

=====

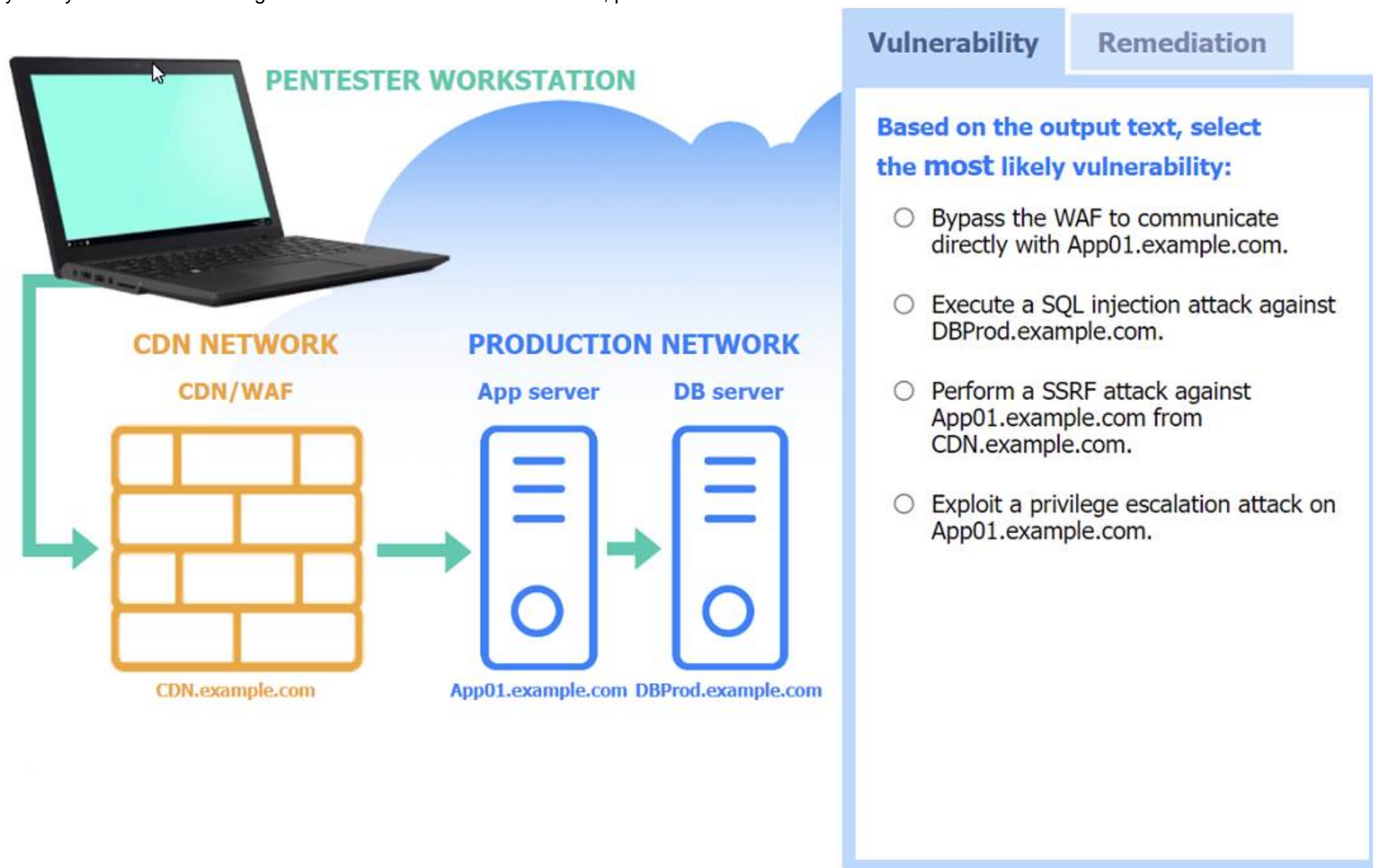
NEW QUESTION 18

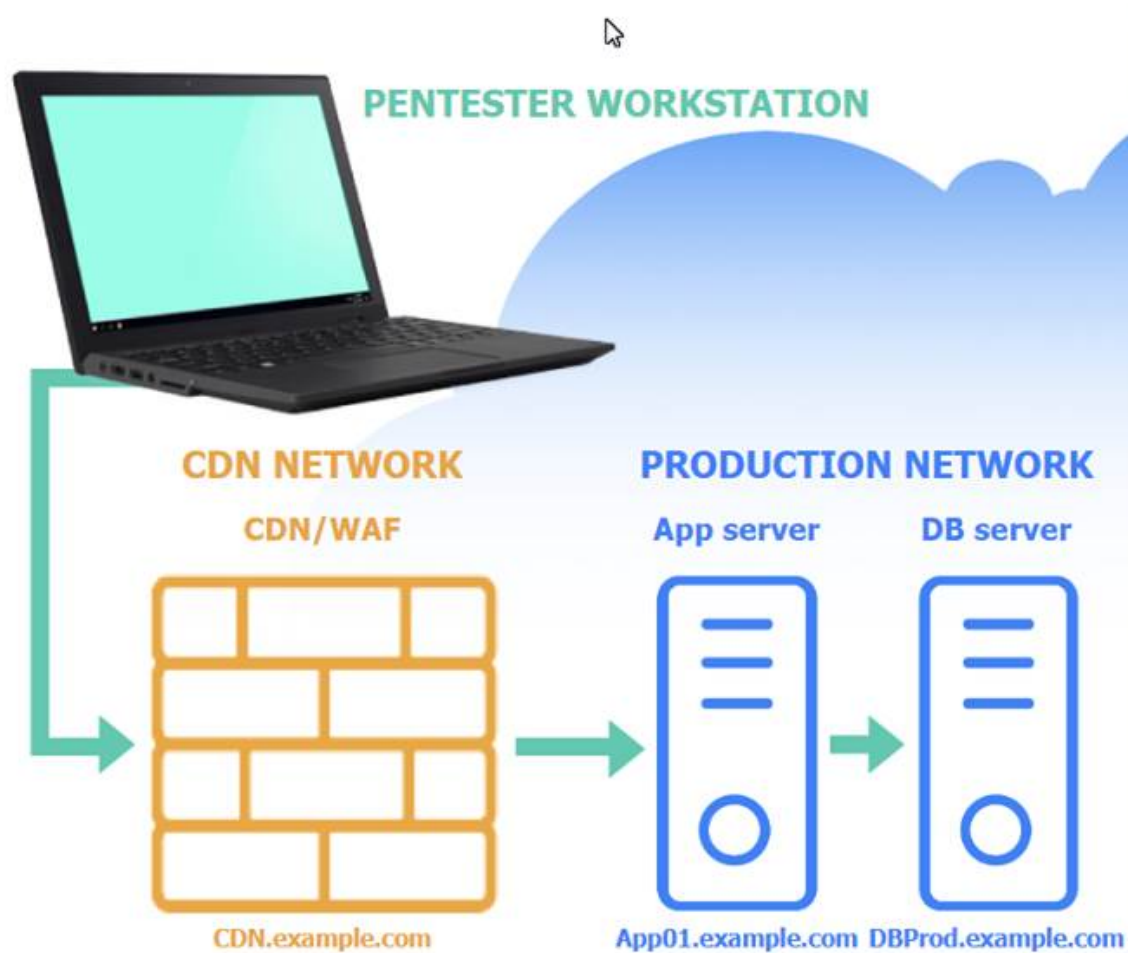
SIMULATION

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

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.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.

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	

DB server



Nmap scan report for 103.1.45.50

Host is up (0.046s latency).

PORT	STATE	SERVICE	VERSION
80/tcp	filtered	http	
443/tcp	filtered	ssl/http	
3306/tcp	filtered	mysql	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Vulnerability

Remediation

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

- ☐ Bypass the WAF to communicate directly with App01.example.com.
- ☐ Execute a SQL injection attack against DBProd.example.com.
- ☒ Perform a SSRF attack against App01.example.com from CDN.example.com.
- ☐ 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.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.

Most likely vulnerability: Perform a SSRF attack against App01.example.com from CDN.example.com.

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

Two best remediation options:

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

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

? Restrict direct communications to App01.example.com to only approved components: This limits the exposure of the application server by ensuring that only specified, trusted entities can communicate with it.

? Require an additional authentication header value between CDN.example.com

and App01.example.com: Adding an authentication layer between the CDN and the app server helps ensure that requests are legitimate and originate from trusted sources, mitigating SSRF and other indirect attack vectors.

Nmap Scan Observations:

? CDN/WAF shows open ports for HTTP and HTTPS but filtered for MySQL, indicating it acts as a filtering layer.

? App Server has open ports for HTTP, HTTPS, and filtered for MySQL.

? DB Server has all ports filtered, typical for a database server that should not be directly accessible.

These findings align with the SSRF vulnerability and the appropriate remediation steps to enhance the security of internal communications.

NEW QUESTION 22

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.

References from Pentest:

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

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

Conclusion:

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

=====

NEW QUESTION 24

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:

? Purpose:

? Process:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 28

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:

? Purpose:

? Why Enumerate Permissions:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 32

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:

? Advantages:

? Comparison with Other Techniques:

Pentest References:

? 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.

=====

NEW QUESTION 37

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:

? Monitoring Mode:

? Aircrack-ng Suite: `airmon-ng start wlan0`

This command starts the interface wlan0 in monitoring mode.

? Steps to Capture WPA2 Handshakes: `airodump-ng wlan0mon`

Pentest References:

? Wireless Security Assessments: Understanding the importance of monitoring mode for capturing data during wireless penetration tests.

? Aircrack-ng Tools: Utilizing the suite effectively for tasks like capturing WPA2 handshakes, deauthenticating clients, and cracking passwords.

By enabling monitoring mode with Aircrack-ng, the tester can capture the necessary WPA2 handshakes to further analyze and attempt to crack the Wi-Fi network's password.

=====

NEW QUESTION 39

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.

References from Pentest:

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

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

=====

NEW QUESTION 40

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 provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings.

? Components of an Assessment Report:

? Importance of Attack Narrative:

? References from Pentesting Literature: Step-by-Step Explanation

References:

? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups

=====

NEW QUESTION 41

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. icacds.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):
? icacls.exe:
? nltest.exe:
? rundll.exe:
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.
=====

NEW QUESTION 46

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:

? Comparison with Other Options:
=====

NEW QUESTION 50

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):
? Advantages of DAST:
? Examples of DAST Tools:
Pentest References:
? 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.
=====

NEW QUESTION 51

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:
? Spear Phishing:
? Comparison with Other Risks:
Email addresses are a starting point for phishing attacks, making unauthorized access to the network the most relevant risk.
=====

NEW QUESTION 55

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.

References 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.

=====

NEW QUESTION 60

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:

? Alternative Review Options:

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.

=====

NEW QUESTION 65

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:

? EPSS:

? Analysis:

Pentest References:

? Vulnerability Prioritization: Using CVSS and EPSS scores to prioritize vulnerabilities based on severity and likelihood of exploitation.

? Risk Assessment: Understanding the balance between impact (CVSS) and exploit likelihood (EPSS) to identify the most critical targets for remediation or attack.

By focusing on Target 1, which has a balanced combination of severity and exploitability, the penetration tester can address the most likely target for attacks based on the given scores.

=====

NEW QUESTION 68

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:

? Manual Banner Grabbing:

Step-by-Step Explanationtelnet target_ip 80

? uk.co.certification.simulator.questionpool.PList@5af47689 nc target_ip 80

? Automated Banner Grabbing: nmap -sV target_ip
? Benefits:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=====

NEW QUESTION 69

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:

? Commands Breakdown:

? Issue:

? Solution:

Pentest References:

? 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.

=====

NEW QUESTION 72

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

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

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

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

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

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

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

NEW QUESTION 74

.....

Relate Links

100% Pass Your PT0-003 Exam with ExamBible Prep Materials

<https://www.exambible.com/PT0-003-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>