Vendor: CompTIA

Exam Code:PT0-002

Exam Name: CompTIA PenTest+ Certification Exam

Version: Demo

QUESTION 1

A penetration tester opened a reverse shell on a Linux web server and successfully escalated privileges to root. During the engagement, the tester noticed that another user logged in frequently as root to perform work tasks.

To avoid disrupting this user\\'s work, which of the following is the BEST option for the penetration tester to maintain root-level persistence on this server during the test?

A. Add a web shell to the root of the website.

B. Upgrade the reverse shell to a true TTY terminal.

C. Add a new user with ID 0 to the /etc/passwd file.

D. Change the password of the root user and revert after the test.

Correct Answer: C

The best option for the penetration tester to maintain root-level persistence on this server during the test is to add a new user with ID 0 to the /etc/passwd file. This will allow the penetration tester to use the same user account as the other user, but with root privileges, meaning that it won\\'t disrupt the other user\\'s work. This can be done by adding a new line with the username and the numerical user ID 0 to the /etc/passwd file. For example, if the username for the other user is "johndoe", the line to add would be "johndoe:x:0:0:John Doe:/root:/bin/bash". After the user is added, the penetration tester can use the "su" command to switch to the new user and gain root privileges.

QUESTION 2

Which of the following situations would MOST likely warrant revalidation of a previous security assessment?

A. After detection of a breach

B. After a merger or an acquisition

C. When an organization updates its network firewall configurations

D. When most of the vulnerabilities have been remediated

Correct Answer: D

QUESTION 3

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

A. Wait for the next login and perform a downgrade attack on the server.

B. Capture traffic using Wireshark.

C. Perform a brute-force attack over the server.

D. Use an FTP exploit against the server.

Correct Answer: B

Reference: https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b

---

QUESTION 4

A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svsaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svsaccount /add >> batchjopb3.bat
net user svsaccount
runas /user:svsaccount mimikatz
```

Which of the following should the tester do AFTER delivering the final report?

A. Delete the scheduled batch job.

B. Close the reverse shell connection.

C. Downgrade the svsaccount permissions.

D. Remove the tester-created credentials.

Correct Answer: D

QUESTION 5

A client would like to have a penetration test performed that leverages a continuously updated TTPs framework and covers a wide variety of enterprise systems and networks. Which of the following methodologies should be used to BEST meet the client\\'s expectations?

A. OWASP Top 10

B. MITRE ATTandCK framework

C. NIST Cybersecurity Framework

D. The Diamond Model of Intrusion Analysis

Correct Answer: B

QUESTION 6

A consultant is reviewing the following output after reports of intermittent connectivity issues:

(192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]

(192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]

(192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]

(192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]

(192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]

(192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]

(224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]

(239.255.255.250)

at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet] Which of the following is MOST likely to be reported by the consultant?

A.

A device on the network has an IP address in the wrong subnet.

B.

A multicast session was initiated using the wrong multicast group.

C.

An ARP flooding attack is using the broadcast address to perform DDoS.

D.

A device on the network has poisoned the ARP cache.

Correct Answer: D

The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address. With this on the same network, intermittent connectivity will be inevitable as along as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.

QUESTION 7

Which of the following concepts defines the specific set of steps and approaches that are conducted during a penetration test?

A. Scope details

B. Findings

C. Methodology

D. Statement of work

Correct Answer: C

QUESTION 8

A penetration tester needs to upload the results of a port scan to a centralized security tool. Which of the following commands would allow the tester to save the results in an interchangeable format?

A. nmap -iL results 192.168.0.10-100

B. nmap 192.168.0.10-100-O > results

C. nmap -A 192.168.0.10-100-oX results

D. nmap 192.168.0.10-100 | grep "results"

Correct Answer: C

QUESTION 9

A tester who is performing a penetration test discovers an older firewall that is known to have serious vulnerabilities to remote attacks but is not part of the original list of IP addresses for the engagement. Which of the following is the BEST option for the tester to take?

A. Segment the firewall from the cloud.

B. Scan the firewall for vulnerabilities.

C. Notify the client about the firewall.

D. Apply patches to the firewall.

Correct Answer: C

QUESTION 10

During the reconnaissance phase, a penetration tester obtains the following output:

Reply from 192.168.1.23: bytes=32 time