PT0-002 Q&As

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Which of the following members of a client organization are most likely authorized to provide a signed authorization letter prior to the start date of a penetration test?

A. The IT department

B. The executive management team and legal personnel

C. Organizational security personnel

D. The human resources team

Correct Answer: B

QUESTION 2

As part of an active reconnaissance, a penetration tester intercepts and analyzes network traffic, including API requests and responses. Which of the following can be gained by capturing and examining the API traffic?

A. Assessing the performance of the network\\'s API communication

B. Identifying the token/authentication detail

C. Enumerating all users of the application

D. Extracting confidential user data from the intercepted API responses

Correct Answer: B

By intercepting and analyzing the API traffic, a penetration tester can gain valuable information about the authentication mechanism and the tokens used by the API. Tokens are typically used to identify and authorize users or applications that access the API. A penetration tester can use this information to perform attacks such as token hijacking, token tampering, or token replay. The other options are not directly related to the API traffic, but rather to the application logic or the network performance.

QUESTION 3

A penetration tester analyzed a web-application log file and discovered an input that was sent to the company\\'s web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

A. SQL injection

B. HTML injection

C. Remote command injection

D. DLL injection

Correct Answer: A

WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection34. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data1. Based on this information, one possible answer to your question is A. SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

QUESTION 4

A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

A. As backup in case the original documents are lost

B. To guide them through the building entrances

C. To validate the billing information with the client

D. As proof in case they are discovered

Correct Answer: D

The penetration testers should carry copies of the engagement documents with them as proof in case they are discovered by security guards, employees, or law enforcement officials. The engagement documents should include the scope, objectives, authorization, and contact information of the penetration testing team and the client. This will help avoid any legal or ethical issues that may arise from trespassing, breaking and entering, or unauthorized access. The other options are not valid reasons for carrying the engagement documents with them.

Reference: https://hub.packtpub.com/penetration-testing-rules-of-engagement/

QUESTION 5

A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions?

A. Aircrack-ng

B. Wireshark

C. Wifite

D. Kismet

Correct Answer: A

Aircrack-ng is a suite of tools that allows the penetration tester to test the effectiveness of the wireless IDS solutions by performing various attacks on wireless networks, such as cracking WEP and WPA keys, capturing and injecting packets, deauthenticating clients, or creating fake access points. Aircrack-ng can also generate different types of traffic and signatures that can trigger the wireless IDS alerts or responses, such as ARP requests, EAPOL frames, or beacon frames.

Reference: https://purplesec.us/perform-wireless-penetration-test/

QUESTION 6

A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company\\'s network. Which of the following accounts should the tester use to return the MOST results?

A. Root user

B. Local administrator

C. Service

D. Network administrator

Correct Answer: C

QUESTION 7

A penetration tester is assessing a wireless network. Although monitoring the correct channel and SSID, the tester is unable to capture a handshake between the clients and the AP. Which of the following attacks is the MOST effective to allow the penetration tester to capture a handshake?

A. Key reinstallation

B. Deauthentication

C. Evil twin

D. Replay

Correct Answer: B

Deauth will make the client connect again

QUESTION 8

A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:

Pre-engagement interaction (scoping and ROE) Intelligence gathering (reconnaissance) Threat modeling Vulnerability analysis Exploitation and post exploitation Reporting

Which of the following methodologies does the client use?

A. OWASP Web Security Testing Guide

B. PTES technical guidelines

C. NIST SP 800-115

D. OSSTMM

Correct Answer: B

Reference: https://kirkpatrickprice.com/blog/stages-of-penetration-testing-according-to- ptes/

QUESTION 9

A penetration tester will be performing a vulnerability scan as part of the penetration test on a client\\'s website. The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?

A. -8 -T0

B. --script "http*vuln*"

C. -sn

D. -O -A

Correct Answer: B

Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command Nmap -p 445 -n - T4 --open 172.21.0.0/16 would scan for SMB port 445 over a /16 network with

the following options:

-p 445 specifies the port number to scan.

-n disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.

-T4 sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.

-Open only shows hosts that have open ports, which can reduce the output and focus on relevant results. The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time

sensitive.

QUESTION 10

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 11

A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

A. nmap –f –sV –p80 192.168.1.20

B. nmap –sS –sL –p80 192.168.1.20

C. nmap –A –T4 –p80 192.168.1.20

D. nmap –O –v –p80 192.168.1.20

Correct Answer: C

This command will scan the host 192.168.1.20 on port 80 using the following options:

-A: This option enables OS detection, version detection, script scanning, and traceroute. This will help to determine if the host is running an approved version of Linux and a patched version of Apache, as well as other information about the

host and the network path.

-T4: This option sets the timing template to aggressive, which speeds up the scan by increasing the number of parallel probes, reducing the timeouts, and assuming faster responses.

-p80: This option specifies the port to scan, which is 80 in this case. Port 80 is commonly used for HTTP services, such as Apache web server.

Reference: https://nmap.org/book/man-version-detection.html

QUESTION 12

A penetration tester is conducting a penetration test and discovers a vulnerability on a web server that is owned by the client. Exploiting the vulnerability allows the tester to open a reverse shell. Enumerating the server for privilege escalation, the tester discovers the following:

```
netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 10.1.1.24:48850 24.176.9.43:59036 ESTABLISHED
tcp 0 0 0.0.0.0:22 :0.0.0.0* LISTEN
tcp 0 0 10.1.1.24:50112 136.12.56.217:58003 ESTABLISHED
tcp 0 0 10.1.1.24:80 115.93.193.245:40243 ESTABLISHED
tcp 0 0 10.1.1.24:80 210.117.12.2:40252 ESTABLISHED
tcp6 0 0 :::22 :::* LISTEN
udp 0 0 10.1.1.24:161 0.0.0.0:*
```

Which of the following should the penetration tester do NEXT?

A. Close the reverse shell the tester is using.

B. Note this finding for inclusion in the final report.

C. Investigate the high numbered port connections.

D. Contact the client immediately.

Correct Answer: C

The image shows the output of the netstat -antu command, which displays active internet connections for the TCP and UDP protocols. The output shows that there are four established TCP connections and two listening UDP connections on the host. The established TCP connections have high numbered ports as their local addresses, such as 49152, 49153, 49154, and 49155. These ports are in the range of ephemeral ports, which are dynamically assigned by the operating system for temporary use by applications or processes. The foreign addresses of these connections are also high numbered ports, such as 4433, 4434, 4435, and 4436. These ports are not well-known or registered ports for any common service or protocol. The combination of high numbered ports for both local and foreign addresses suggests that these connections are suspicious and may indicate a backdoor or a covert channel on the host. Therefore, the penetration tester should investigate these connections next to determine their nature and purpose. The other options are not appropriate actions for the penetration tester at this stage.

QUESTION 13

A penetration tester discovered a code repository and noticed passwords were hashed before they were stored in the database with the following code? salt = `123\\' hash = hashlib.pbkdf2_hmac(`sha256\\', plaintext, salt, 10000) The tester recommended the code be updated to the following salt = os.urandom(32) hash = hashlib.pbkdf2_hmac(`sha256\\', plaintext, salt, 10000).

Which of the following steps should the penetration tester recommend?

A. Changing passwords that were created before this code update

B. Keeping hashes created by both methods for compatibility

C. Rehashing all old passwords with the new code

D. Replacing the SHA-256 algorithm to something more secure

Correct Answer: A

The penetration tester recommended the code be updated to use a random salt instead of a fixed salt for hashing passwords. A salt is a random value that is added to the plaintext password before hashing it, to prevent attacks such as rainbow tables or dictionary attacks that rely on precomputed hashes of common or weak passwords. A random salt ensures that each password hash is unique and unpredictable, even if two users have the same password. However, changing the salt does not affect the existing hashes that were created with the old salt, which may still be vulnerable to attacks. Therefore, the penetration tester should recommend changing passwords that were created before this code update, so that they can be hashed with the new salt and be more secure. The other options are not valid steps that the penetration tester should recommend. Keeping hashes created by both methods for compatibility would defeat the purpose of updating the code, as it would leave some hashes vulnerable to attacks. Rehashing all old passwords with the new code would not work, as it would require knowing the plaintext passwords, which are not stored in the database. Replacing the SHA-256 algorithm to something more secure is not necessary, as SHA-256 is a secure and widely used hashing algorithm that has no known vulnerabilities or collisions.

QUESTION 14

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

nmap -n -vv -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?

A. -su

B. -pn

C. -sn

D. -ss

Correct Answer: B

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 15

A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?

A. Netcraft

B. CentralOps

C. Responder

D. FOCA

Correct Answer: D

https://kalilinuxtutorials.com/foca-metadata-hidden-documents/ FOCA (Fingerprinting Organizations with Collected Archives) is a tool that is used to find hidden information in documents available on the web. It can be used to extract metadata from documents such as PDF, Microsoft Office, OpenOffice, and others. The metadata can include information such as the author, creation date, and software used to create the document. FOCA can also extract information from the document\\'s properties such as the title, keywords, and comments. This tool can also identify specific keywords and patterns in the document and can be useful in identifying sensitive information that may have been inadvertently left in the document.