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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following actions would BEST explain why a testing team would need to reach out to a customer\\'s emergency contact during an assessment?

A. To confirm assessment dates

B. To escalate the detection of a prior compromise

C. To submit the weekly status report

D. To announce that testing will begin

Correct Answer: B

QUESTION 2

A penetration tester is conducting a test after hours and notices a critical system was taken down. Which of the following contacts should be notified first?

A. Secondary

B. Emergency

C. Technical

D. Primary

Correct Answer: B

QUESTION 3

Penetration tester is developing exploits to attack multiple versions of a common software package. The versions have different menus and)ut.. they have a common log-in screen that the exploit must use. The penetration tester develops code to perform the log-in that can be each of the exploits targeted to a specific version. Which of the following terms is used to describe this common log-in code example?

A. Conditional

B. Library

C. Dictionary

D. Sub application

Correct Answer: B

The term that is used to describe the common log-in code example is library, which is a collection of reusable code or functions that can be imported or called by other programs or scripts. A library can help simplify or modularize the code development process by providing common or frequently used functionality that can be shared across different programs or scripts. In this case, the penetration tester develops a library of code to perform the log-in that can be imported or called by each of the exploits targeted to a specific version of the software package. The other options are not valid terms that describe the common log-in code example. Conditional is a programming construct that executes a block of code based on a logical condition or expression, such as if-else statements. Dictionary is a data structure that stores key-value pairs, where each key is associated with a value, such as a Python dictionary. Sub application is not a standard programming term, but it may refer to an application that runs within another application, such as a web application.

QUESTION 4

Given the following user-supplied data:

www.comptia.com/info.php?id=1 AND 1=1

Which of the following attack techniques is the penetration tester likely implementing?

A. Boolean-based SQL injection

B. Time-based SQL injection

C. Stored cross-site scripting

D. Reflected cross-site scripting

Correct Answer: A

The user-supplied data www.comptia.com/info.php?id=1 AND 1=1 is indicative of a Boolean-based SQL injection attack. In this attack, the attacker manipulates a SQL query by inserting additional SQL logic that will always evaluate to true (in this case, AND 1=1) to gain unauthorized access to database information. This type of attack exploits improper input validation in web applications to manipulate database queries. The other attack techniques listed (Time-based SQL injection, Stored cross-site scripting, Reflected cross- site scripting) involve different methodologies and are not demonstrated by the given user- supplied data.

QUESTION 5

A penetration tester has gained access to part of an internal network and wants to exploit on a different network segment. Using Scapy, the tester runs the following command:

```
sendp(Ether()/dotlq(vlan=100)/dotq(vlan=50)/IP(dst="172.16.50.10")/ICMP())
```

Which of the following represents what the penetration tester is attempting to accomplish?

A. DNS cache poisoning

B. MAC spoofing

C. ARP poisoning

D. Double-tagging attack

Correct Answer: D

https://scapy.readthedocs.io/en/latest/usage.html

QUESTION 6

A penetration tester runs the following command:

nmap -p- -A 10.0.1.10

Given the execution of this command, which of the following quantities of ports will Nmap scan?

A. 1,000

B. 1,024

C. 10,000

D. 65,535

Correct Answer: D

The nmap command with the -p- flag scans all ports from 1 to 65535 on the target host. The -A flag enables OS detection, version detection, script scanning, and traceroute. Therefore, the command will scan 65,535 ports on the host

10.0.1.10 and perform additional analysis on the open ports.

QUESTION 7

A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

A. Alternate data streams

B. PowerShell modules

C. MP4 steganography

D. PsExec

Correct Answer: A

Alternate data streams (ADS) are a feature of the NTFS file system that allows storing additional data in a file without affecting its size, name, or functionality. ADS can be used to hide or embed data or executable code in a file, such as a specially crafted binary for later execution. ADS can be created or accessed using various tools or commands, such as the command prompt, PowerShell, or Sysinternals12. For example, the following command can create an ADS named secret.exe in a file named test.txt and run it using wmic.exe process call create function: type secret.exe > test.txt:secret.exe and wmic process call create "cmd.exe /c test.txt:secret.exe"

QUESTION 8

A penetration tester successfully performed an exploit on a host and was able to hop from VLAN 100 to VLAN 200. VLAN 200 contains servers that perform financial transactions, and the penetration tester now wants the local interface of the attacker machine to have a static ARP entry in the local cache. The attacker machine has the following:

IP Address: 192.168.1.63

Physical Address: 60-36-dd-a6-c5-33

Which of the following commands would the penetration tester MOST likely use in order to establish a static ARP entry successfully?

A. tcpdump -i eth01 arp and arp[6:2] == 2

B. arp -s 192.168.1.63 60-36-DD-A6-C5-33

C. ipconfig /all findstr /v 00-00-00 | findstr Physical

D. route add 192.168.1.63 mask 255.255.255.255.0 192.168.1.1

Correct Answer: B

The arp command is used to manipulate or display the Address Resolution Protocol (ARP) cache, which is a table that maps IP addresses to physical addresses (MAC addresses) on a network. The -s option is used to add a static ARP entry to the cache, which means that it will not expire or be overwritten by dynamic ARP entries. The syntax for adding a static ARP entry is arp -s . Therefore, the command arp -s 192.168.1.63 60-36-DD-A6-C5-33 would add a static ARP entry for the IP address 192.168.1.63 and the physical address 60-36-DD-A6-C5-33 to the local cache of the attacker machine. This would allow the attacker machine to communicate with the target machine without relying on ARP requests or replies. The other commands are not valid or useful for establishing a static ARP entry.

QUESTION 9

A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

A. Nmap

B. Nikto

C. Cain and Abel

D. Ethercap

Correct Answer: B

https://hackertarget.com/nikto-website-scanner/

QUESTION 10

Which of the following types of assessments MOST likely focuses on vulnerabilities with the objective to access specific data?

A. An unknown-environment assessment

B. A known-environment assessment

C. A red-team assessment

D. A compliance-based assessment

Correct Answer: C

A red-team assessment is a type of penetration testing that simulates a real- world attack scenario with the goal of accessing specific data or systems. A red-team assessment is different from an unknown-environment assessment, which does not have a predefined objective and focuses on discovering as much information as possible about the target. A known-environment assessment is a type of penetration testing that involves cooperation and communication with the target organization, and may not focus on specific data or systems. A compliance-based assessment is a type of penetration testing that aims to meet certain regulatory or industry standards, and may not focus on specific data or systems.

QUESTION 11

A private investigation firm is requesting a penetration test to determine the likelihood that attackers can gain access to mobile devices and then exfiltrate data from those devices. Which of the following is a social-engineering method that, if successful, would MOST likely enable both objectives?

A. Send an SMS with a spoofed service number including a link to download a malicious application.

B. Exploit a vulnerability in the MDM and create a new account and device profile.

C. Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading.

D. Infest a website that is often used by employees with malware targeted toward x86 architectures.

Correct Answer: A

Since it doesn\\'t indicate company owned devices, sending a text to download an application is best. And it says social-engineering so a spoofed text falls under that area.

QUESTION 12

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 13

A client has requested that the penetration test scan include the following UDP services:

SNMP, NetBIOS, and DNS.

Which of the following Nmap commands will perform the scan?

A. nmap –vv sUV –p 53, 123-159 10.10.1.20/24 –oA udpscan

B. nmap –vv sUV –p 53,123,161-162 10.10.1.20/24 –oA udpscan

C. nmap –vv sUV –p 53,137-139,161-162 10.10.1.20/24 –oA udpscan

D. nmap –vv sUV –p 53, 122-123, 160-161 10.10.1.20/24 –oA udpscan

Correct Answer: C

QUESTION 14

During an assessment, a penetration tester was able to access the organization\\'s wireless network from outside of the building using a laptop running Aircrack-ng. Which of the following should be recommended to the client to remediate this issue?

A. Changing to Wi-Fi equipment that supports strong encryption

B. Using directional antennae

C. Using WEP encryption

D. Disabling Wi-Fi

Correct Answer: A

If a penetration tester was able to access the organization\\'s wireless network from outside of the building using Aircrack-ng, then it means that the wireless network was not secured with strong encryption or authentication methods. Aircrackng is a tool that can crack weak wireless encryption schemes such as WEP or WPA-PSK using various techniques such as packet capture, injection, replay, and brute force. To remediate this issue, the client should change to Wi-Fi equipment that supports strong encryption such as WPA2 or WPA3, which are more resistant to cracking attacks. Using directional antennae may reduce the signal range of the wireless network, but it would not prevent an attacker who is within range from cracking the encryption. Using WEP encryption is not a good recommendation, as WEP is known to be insecure and vulnerable to Aircrack-ng attacks. Disabling Wi-Fi may eliminate the risk of wireless attacks, but it would also eliminate the benefits of wireless connectivity for the organization.

QUESTION 15

During a test of a custom-built web application, a penetration tester identifies several vulnerabilities. Which of the following would be the most interested in the steps to reproduce these vulnerabilities?

A. Operations staff

B. Developers

C. Third-party stakeholders

D. C-suite executives

Correct Answer: B

The developers would be the most interested in the steps to reproduce the web application vulnerabilities, because they are responsible for fixing the code and implementing security best practices. The steps to reproduce the vulnerabilities would help them understand the root cause of the problem, test the patches, and prevent similar issues in the future. The other options are less interested in the technical details of the vulnerabilities, as they have different roles and responsibilities. The operations staff are more concerned with the availability and performance of the web application, the third-party stakeholders are more interested in the business impact and risk assessment of the vulnerabilities, and the C-suite executives are more focused on the strategic and financial implications of the vulnerabilities123.