PT0-002 Q&As

CompTIA PenTest+

Pass CompTIA PT0-002 Exam with 100% Guarantee

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

https://www.pass4itsure.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

A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website\\'s response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?

A. Situational awareness

B. Rescheduling

C. DDoS defense

D. Deconfliction

Correct Answer: D

https://redteam.guide/docs/definitions/ Deconfliction is the process of coordinating activities and communicating information to avoid interference, confusion, or conflict among different parties involved in an operation. The network engineer contacted the penetration tester to check if the GET requests were part of the test, and to avoid any potential misunderstanding or disruption of the test or the website. The other options are not related to the purpose of checking with the penetration tester.

QUESTION 2

A penetration tester was hired to test Wi-Fi equipment. Which of the following tools should be used to gather information about the wireless network?

A. Kismet

B. Burp Suite

C. BeEF

D. WHOIS

Correct Answer: A

Kismet is a well-known tool used in penetration testing for wireless network detection, packet sniffing, and intrusion detection. It is particularly useful for gathering information about Wi-Fi networks as it can detect hidden networks and capture network packets. This capability allows penetration testers to analyze the wireless environment, identify potential vulnerabilities, and assess the security posture of the Wi-Fi equipment being tested. Unlike the other tools listed, Kismet is specifically designed for wireless network analysis, making it the ideal choice for this task.

QUESTION 3

When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

A. Clarify the statement of work.

B. Obtain an asset inventory from the client.

C. Interview all stakeholders.

D. Identify all third parties involved.

Correct Answer: A

Clarifying the statement of work is one of the most important items to develop fully prior to beginning the penetration testing activities, as it defines the scope, objectives, deliverables, and expectations of the engagement. The statement of work is a formal document that outlines the agreement between the penetration tester and the client and serves as a reference for both parties throughout the engagement. It should include details such as the type, duration, and frequency of testing, the target systems and networks, the authorized methods and tools, the reporting format and schedule, and any legal or ethical considerations.

QUESTION 4

A penetration tester wrote the following Bash script to brute force a local service password:

```
#!/bin/bash
for p in $(cat wordlist.txt);do
        echo $p | nc -u 127.0.0.1 20000 | grep "Wrong Password" &  ( echo
"The correct password is $p" && break )
done
```

The script is not working as expected. Which of the following changes should the penetration tester make to get the script to work?

A.
Replace
```
& ( echo "The correct password is $p" && break )
```
With
```
&& echo "The correct password is $p" || break
```

B.
Replace
```
& ( echo "The correct password is $p" && break )
```
With
```
& echo "The correct password is $p" | break
```

C.
Replace
```
& ( echo "The correct password is $p" && break )
```
With
```
&& ( echo "The correct password is $p" && break )
```

D.
Replace
```
& ( echo "The correct password is $p" && break )
```
With
```
|| ( echo "The correct password is $p" && break )
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 5

Which of the following is the most important aspect to consider when calculating the price of a penetration test service for a client?

A. Operating cost

B. Required scope of work

C. Non-disclosure agreement

D. Client\\'s budget

Correct Answer: B

When calculating the price of a penetration test service for a client, the most important aspect to consider is the required scope of work 1. The scope of work defines the objectives of the penetration test and the systems that will be tested. It is

important to understand the scope of work to determine the resources required to complete the test and the time it will take to complete the test 2.

References: 2: CompTIA. (2021). CompTIA PenTest+ Certification Exam Objectives.

Retrieved from

https://www.comptia.org/content/dam/comptia/documents/certifications/Exam%20Objective s/CompTIA-PenTest%2B%20Exam%20Objectives%20PT0-002.pdf 1: O\\'Brien, D. (2021). The Official CompTIA PenTest+ Study Guide (Exam PT0002). John Wiley and Sons.

QUESTION 6

A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\C$\temp /persistent no
copy c:\temp\hack.exe S:\temp\hack.exe
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)

A. Redirecting output from a file to a remote system

B. Building a scheduled task for execution

C. Mapping a share to a remote system

D. Executing a file on the remote system

E. Creating a new process on all domain systems

F. Setting up a reverse shell from a remote system

G. Adding an additional IP address on the compromised system

Correct Answer: CD

WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

QUESTION 7

A security firm is discussing the results of a penetration test with the client. Based on the findings, the client wants to focus the remaining time on a critical network segment. Which of the following BEST describes the action taking place?

A. Maximizing the likelihood of finding vulnerabilities

B. Reprioritizing the goals/objectives

C. Eliminating the potential for false positives

D. Reducing the risk to the client environment

Correct Answer: B

Goal Reprioritization Have the goals of the assessment changed? Has any new information been found that might affect the goal or desired end state? I would also agree with A, because by goal reprioritization you are more likely to find vulnerabilities in this specific segment of critical network, but it is a side effect of goal reprioritization.

QUESTION 8

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

A. VRFY and EXPN

B. VRFY and TURN

C. EXPN and TURN

D. RCPT TO and VRFY

Correct Answer: A

The VRFY and EXPN commands can be used to enumerate user accounts on an SMTP server, as they are used to verify the existence of users or mailing lists. VRFY (verify) asks the server to confirm that a given user name or address is valid. EXPN (expand) asks the server to expand a mailing list into its individual members. These commands can be used by a penetration tester to identify valid user names or e-mail addresses on the target SMTP server. Reference: https://hackerone.com/reports/193314

QUESTION 9

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

A. HTTPS communication

B. Public and private keys

C. Password encryption

D. Sessions and cookies

Correct Answer: D

QUESTION 10

During the scoping phase of an assessment, a client requested that any remote code exploits discovered during testing would be reported immediately so the vulnerability could be fixed as soon as possible. The penetration tester did not agree with this request, and after testing began, the tester discovered a vulnerability and gained internal access to the system. Additionally, this scenario led to a loss of confidential credit card data and a hole in the system. At the end of the test, the penetration tester willfully failed to report this information and left the vulnerability in place. A few months later, the client was breached and credit card data was stolen. After being notified about the breach, which of the following steps should the company take NEXT?

A. Deny that the vulnerability existed

B. Investigate the penetration tester.

C. Accept that the client was right.

D. Fire the penetration tester.

Correct Answer: B

The penetration tester violated the client\\'s request and the code of ethics by not reporting the vulnerability immediately and leaving it in place. This could have contributed to the breach and the data loss. The company should investigate the penetration tester\\'s actions and motives, and hold them accountable for any negligence or malpractice.

QUESTION 11

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. The output shows an ARP table that contains

entries for IP addresses and their corresponding MAC addresses on a local network interface (en0). ARP stands for Address Resolution Protocol and is used to map IP addresses to MAC addresses on a network.

However, one entry in the table is suspicious:

? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet] This entry has the same MAC address as another entry:

? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet] This indicates that a device on the network has poisoned the ARP cache by sending false ARP replies that associate its MAC address with multiple IP addresses, including

192.168.1.136 and 192.168.1.1 (which is likely the gateway address). This allows the device to intercept or redirect traffic intended for those IP addresses.

QUESTION 12

A penetration-testing team needs to test the security of electronic records in a company\\'s office. Per the terms of engagement, the penetration test is to be conducted after hours and should not include circumventing the alarm or performing destructive entry. During outside reconnaissance, the team sees an open door from an adjoining building. Which of the following would be allowed under the terms of the engagement?

A. Prying the lock open on the records room

B. Climbing in an open window of the adjoining building

C. Presenting a false employee ID to the night guard

D. Obstructing the motion sensors in the hallway of the records room

Correct Answer: B

The terms of engagement state that the penetration test should not include circumventing the alarm or performing destructive entry, which rules out options A and D. Option C is also not allowed, as it involves social engineering, which is not part of the scope. Option B is the only one that does not violate the terms of engagement, as it uses an open door from an adjoining building to gain access to the records room. This can help the penetration tester to test the physical security of the electronic records without breaking any rules.

QUESTION 13

A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

A. The web server is using a WAF.

B. The web server is behind a load balancer.

C. The web server is redirecting the requests.

D. The local antivirus on the web server Is rejecting the connection.

Correct Answer: A

A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks. If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

QUESTION 14

A penetration tester observes an application enforcing strict access controls. Which of the following would allow the tester to bypass these controls and successfully access the organization\\'s sensitive files?

A. Remote file inclusion

B. Cross-site scripting

C. SQL injection

D. Insecure direct object references

Correct Answer: D

Insecure Direct Object References (IDOR) vulnerabilities occur when an application provides direct access to objects based on user-supplied input. This can allow an attacker to bypass authorization and access resources in the system directly, for example database records or files1. In this case, the penetration tester could potentially bypass the strict access controls and access the organization\\'s sensitive files. References: IDOR Vulnerability Overview

QUESTION 15

A company developed a new web application to allow its customers to submit loan applications. A penetration tester is reviewing the application and discovers that the application was developed in ASP and used MSSQL for its back-end

database. Using the application\\'s search form, the penetration tester inputs the following code in the search input field:

IMG SRC=vbscript:msgbox ("Vulnerable_to_Attack") ; >originalAttribute="SRC"originalPath="vbscript;msgbox ("Vulnerable_to_Attack ") ;>"

When the tester checks the submit button on the search form, the web browser returns a pop-up windows that displays "Vulnerable_to_Attack."

Which of the following vulnerabilities did the tester discover in the web application?

A. SQL injection

B. Command injection

C. Cross-site request forgery

D. Cross-site scripting

Correct Answer: D