Free Questions for PT0-002 by vceexamstest

Shared by Boyle on 29-01-2024

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 192.168.1.112. Given the following output:

```
[ATTEMPT] target 192.168.1.112 - login "root" - pass "abcde"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "edcfg"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "qazsw"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "tyuio"
```

Which of the following is the penetration tester conducting?

Options:

A- Port scan

B- Brute force

C- Credential stuffing

D- DoS attack

Answer:

B

Explanation:

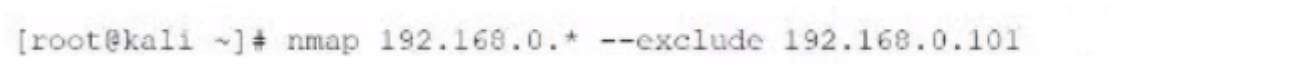
The output shows multiple login attempts with different passwords for the same username "root" on the IP address 192.168.1.112. This is indicative of a brute force attack, where an attacker systematically tries various password combinations to gain unauthorized access.Reference:The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 4: Conducting Passive Reconnaissance; The Official CompTIA PenTest+ Student Guide (Exam PT0-002), Lesson 4: Conducting Active Reconnaissance.

Question 2

Question Type: MultipleChoice

Given the following Nmap scan command:

[root@kali ~]# nmap 192.168.0 .* -- exclude 192.168.0.101



Which of the following is the total number of servers that Nmap will attempt to scan?

Options:

A- 1

B- 101

C- 255

D- 256

Answer:

C

Explanation:

The Nmap scan command given will scan all the hosts in the 192.168.0.0/24 subnet, except for the one with the IP address 192.168.0.101. The subnet has 256 possible hosts, but one of them is excluded, so the total number of servers that Nmap will attempt to scan is 255.Reference:

Nmap Commands - 17 Basic Commands for Linux Network, Section: Scan Multiple Hosts, Subsection: Excluding Hosts from Search

Nmap Cheat Sheet 2023: All the Commands and More, Section: Target Specification, Subsection: -exclude

Question 3

Question Type: MultipleChoice

During a vulnerability scanning phase, a penetration tester wants to execute an Nmap scan using custom NSE scripts stored in the following folder:

/home/user/scripts

/home/user/scripts

Which of the following commands should the penetration tester use to perform this scan?

Options:

A- nmap resume 'not intrusive'

B- nmap script default safe

C- nmap script /home/user/scripts

D- nmap -load /home/user/scripts

Answer:

C

Explanation:

The Nmap command in the question aims to use custom NSE scripts stored in a specific folder. The correct syntax for this option is to use the script argument followed by the path to the folder. The other commands are either invalid, use the wrong argument, or do not specify the folder path.Reference:Best PenTest+ certification study resources and training materials,CompTIA PenTest+ PT0-002 Cert Guide,101 Labs --- CompTIA PenTest+: Hands-on Labs for the PT0-002 Exam

Question 4

Question Type: MultipleChoice

Which of the following should be included in scope documentation?

Options:

A- Service accounts

B- Tester experience

C- Disclaimer

D- Number of tests

Answer:

C

Explanation:

A disclaimer is a statement that limits the liability of the penetration tester and the client in case of any unintended consequences or damages caused by the testing activities. It should be included in the scope documentation to clarify the roles and responsibilities of both parties and to avoid any legal disputes or misunderstandings.Service accounts, tester experience, and number of tests are not essential elements of the scope documentation, although they may be relevant for other aspects of the penetration testing process.Reference:The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 1: Planning and Scoping Penetration Tests1; The Official CompTIA PenTest+ Student Guide (Exam PT0-002), Lesson 1: Planning and Scoping Penetration Tests2; What is the Scope of a Penetration Test?3

Question 5

Question Type: MultipleChoice

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

Options:

A- Operating cost

B- Required scope of work

C- Non-disclosure agreement

D- Client's budget

Answer:

B

Explanation:

When calculating the price of a penetration test service for a client, the most important aspect to consider is therequired scope of work1. 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 test2.

Question 6

Question Type: MultipleChoice

A penetration tester managed to exploit a vulnerability using the following payload:

IF (1=1) WAIT FOR DELAY '0:0:15'

Which of the following actions would best mitigate this type ol attack?

Options:

A- Encrypting passwords

B- Parameterizing queries

C- Encoding output

D- Sanitizing HTML

Answer:

B

Explanation:

The payload used by the penetration tester is a type of blind SQL injection attack that delays the response of the database by 15 seconds if the condition is true. This can be used to extract information from the database by asking a series of true or false questions. To prevent this type of attack, the best practice is to use parameterized queries, which separate the user input from the SQL statement and prevent the injection of malicious code. Encrypting passwords, encoding output, and sanitizing HTML are also good security measures, but they do not directly address the SQL injection vulnerability.Reference:

The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 5: Attacks and Exploits, Section 5.2: Perform Network Attacks, Subsection: SQL Injection, p. 235-237

Blind SQL Injection | OWASP Foundation, Description and Examples sections

Time-Based Blind SQL Injection Attacks, Introduction and Microsoft SQL Server sections

Question 7

Question Type: MultipleChoice

A penetration tester executes the following Nmap command and obtains the following output:

```
nmap -A -p- remotehost

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4p1 Debian
25/tcp   open  smtp    Postfix smtpd
80/tcp   open  http    Apache/2.4.25 (Debian)
3306/tcp open  mysql   MariaDB (unauthorized)
```

Which of the following commands would best help the penetration tester discover an exploitable service?

A)

```
nmap -v -p 25 --script smtp-enum-users remotehost
```

B)

```
nmap -v --script=mysql-info.nse remotehost
```

C)

```
nmap --script=smb-brute.nse remotehost
```

D)

```
nmap -p 3306 --script "http*vuln*" remotehost
```

Options:

A- nmap -v -p 25 -- soript smtp-enum-users remotehost

B- nmap -v -- script=mysql-info.nse remotehost

C- nmap --ocript=omb-brute.noe remotehoat

D- nmap -p 3306 -- script 'http*vuln*' remotehost

Answer:

B

Explanation:

The Nmap command in the question scans all ports on the remote host and identifies the services and versions running on them. The output shows that port 3306 is open and running MariaDB, which is a fork of MySQL. Therefore, the best command to discover an exploitable service would be to use the mysql-info.nse script, which gathers information about the MySQL server, such as the version, user accounts, databases, and configuration variables. The other commands are either misspelled, irrelevant, or too broad for the task.Reference:Best PenTest+ certification study resources and training materials,CompTIA PenTest+ PT0-002 Cert Guide,101 Labs --- CompTIA PenTest+: Hands-on Labs for the PT0-002 Exam

Question 8

Question Type: MultipleChoice

Which of the following tools would be the best to use to intercept an HTTP response at an API, change its content, and forward it back to the origin mobile device?

Options:

A- Drozer

B- Burp Suite

C- Android SDK Tools

D- MobSF

Answer:

B

Explanation:

Burp Suite is a web application security testing tool that can intercept, modify, and forward HTTP requests and responses. It can be used to manipulate the data sent between an API and a mobile device, such as changing the content of the response before it reaches the device. Drozer is a framework for Android security assessment, but it does not intercept HTTP traffic. Android SDK Tools are a set of tools for developing Android applications, but they do not have the functionality to intercept and modify HTTP responses.MobSF is a mobile security framework that can perform static and dynamic analysis of Android and iOS applications, but it does not have the capability to intercept and change HTTP responses at an API level.Reference:The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 8: Application Testing1; The Official CompTIA PenTest+ Student Guide (Exam PT0-002), Lesson 8: Application Testing2; Burp Suite Documentation3

Question 9

Question Type: MultipleChoice

A security analyst is conducting an unknown environment test from 192.168 3.3. The analyst wants to limit observation of the penetration tester's activities and lower the probability of detection by intrusion protection and detection systems. Which of the following Nmap commands should the analyst use to achieve This objective?

Options:

A- Nmap --F 192.168.5.5

B- Map --datalength 2.192.168.5.5

C- Nmap --D 10.5.2.2.168.5.5

D- Map --scanflags SYNFIN 192.168.5.5

Answer:

D

Explanation:

To limit observation of the penetration tester's activities and lower the probability of detection by intrusion protection and detection systems, the security analyst should use theNmap -D 10.5.2.2 192.168.3.3command1. The -D option is used to conceal the identity of the attacker by using decoy IP addresses.This option can be used to confuse the IDS/IPS and lower the probability of detection1.

Question 10

Question Type: MultipleChoice

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?

Options:

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.

Answer:

C

Explanation:

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.