Free Questions for PT0-002 by actualtestdumps

Shared by Rosa on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are a penetration tester running port scans on a server.

INSTRUCTIONS

Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Image not found or type unknown

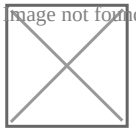
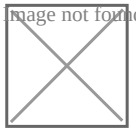


Image not found or type unknown



Options:

A) See explanation below

Answer:

A

Explanation:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions

https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host

Question 2

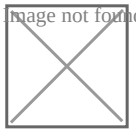
Question Type: MultipleChoice

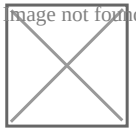
A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.

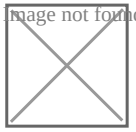
INSTRUCTIONS

Select the appropriate answer(s), given the output from each section.

Output 1







Options:

A) See all the solutions below in Explanation

Answer:

A

Question 3

Question Type: **MultipleChoice**

A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.

INSTRUCTIONS

Select the appropriate answer(s), given the output from each section.

Output 1

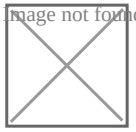


Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Options:

A) See all the solutions below in Explanation

Answer:

A

Question 4

Question Type: MultipleChoice

Using the output, identify potential attack vectors that should be further investigated.

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Options:

A) Explanation:
1: Null session enumeration
Weak SMB file permissions
Fragmentation attack
2: nmap
-sV
-p 1-1023
192.168.2.2
3: #!/usr/bin/python
export $PORTS = 21,22
for $PORT in $PORTS:
try:
s.connect((ip, port))
print("%s:%s -- OPEN" % (ip, port))
except socket.timeout
print("%:%s -- TIMEOUT" % (ip, port))
except socket.error as e:
print("%:%s -- CLOSED" % (ip, port))
finally
s.close()
port_scan(sys.argv[1], ports)

Answer:

A

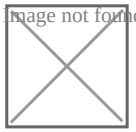
Question 5

Question Type: MultipleChoice

A penetration tester performs the following command:

Which of the following snippets of output will the tester MOST likely receive?

Image not found or type unknown



Options:

A) Option A

B) Option B

C) Option C

D) Option D

Answer:

A

Question 6

Question Type: MultipleChoice

A penetration tester obtained the following results after scanning a web server using the dirb utility:

...

GENERATED WORDS: 4612

...

DOWNLOADED: 4612 -- FOUND: 4

Which of the following elements is MOST likely to contain useful information for the penetration tester?

Options:

A) index.html

B) about

C) info

D) home.html

Answer:

B

Question 7

Question Type: MultipleChoice

You are a penetration tester running port scans on a server.

INSTRUCTIONS

Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Image not found or type unknown

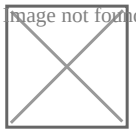
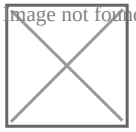


Image not found or type unknown



Options:

A) See explanation below

Answer:

A

Explanation:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions

https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host

Question 8

Question Type: MultipleChoice

The results of an Nmap scan are as follows:

Nmap scan report for (10.2.1.22)

Host is up (0.0102s latency).

Not shown: 998 filtered ports

Port State Service

80/tcp open http

|_http-title: 80F 22% RH 1009.1MB (text/html)

|_http-slowloris-check:

| VULNERABLE:

| Slowloris DoS Attack

| <..>

Device type: bridge|general purpose

Running (JUST GUESSING) : QEMU (95%)

OS CPE: cpe:/a:qemu:qemu

No exact OS matches found for host (test conditions non-ideal).

Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds

Which of the following device types will MOST likely have a similar response? (Choose two.)

Options:

A) Network device

B) Public-facing web server

C) Active Directory domain controller

D) IoT/embedded device

E) Exposed RDP

F) Print queue

Answer:

B, D

Explanation:

https://www.netscout.com/what-is-ddos/slowloris-attacks

From the http-title in the output, this looks like an IoT device with RH implying Relative Humidity, that offers a web-based interface for visualizing the results.

Question 9

Question Type: MultipleChoice

A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

Options:

A) Forensically acquire the backdoor Trojan and perform attribution

B) Utilize the backdoor in support of the engagement

C) Continue the engagement and include the backdoor finding in the final report

D) Inform the customer immediately about the backdoor

Answer:

D

Question 10

Question Type: MultipleChoice

A penetration tester conducted an assessment on a web server. The logs from this session show the following:

Which of the following attacks is being attempted?

Options:

A) Clickjacking

B) Session hijacking

C) Parameter pollution

D) Cookie hijacking

E) Cross-site scripting

Answer:

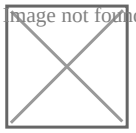
C

Question 11

Question Type: **MultipleChoice**

A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

Image not found or type unknown



Which of the following is the MOST likely reason for the lack of output?

Options:

A) The HTTP port is not open on the firewall.

B) The tester did not run sudo before the command.

C) The web server is using HTTPS instead of HTTP.

D) This URI returned a server error.

Answer:

A