Free Questions for PT0-002 by dumpssheet

Shared by Atkins on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A penetration tester received a .pcap file to look for credentials to use in an engagement.

Which of the following tools should the tester utilize to open and read the .pcap file?

Options:

A- Nmap

B- Wireshark

C- Metasploit

D- Netcat

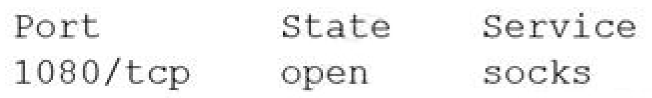
Answer:

B

Question 2

Question Type: **MultipleChoice**

A penetration tester conducts an Nmap scan against a target and receives the following results:



```
Port          State     Service
1080/tcp      open      socks
```

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

Options:

A- Nessus

B- ProxyChains

C- OWASPZAP

D- Empire

Answer:

B

Question 3

Question Type: **MultipleChoice**

A penetration tester has been hired to perform a physical penetration test to gain access to a secure room within a client's building. Exterior reconnaissance identifies two entrances, a WiFi guest network, and multiple security cameras connected to the Internet.

Which of the following tools or techniques would BEST support additional reconnaissance?

Options:

A- Wardriving

B- Shodan

C- Recon-ng

D- Aircrack-ng

Answer:

C

Question 4

Question Type: **MultipleChoice**

A new client hired a penetration-testing company for a month-long contract for various security assessments against the client's new service. The client is expecting to make the new service publicly available shortly after the assessment is complete and is planning to fix any findings, except for critical issues, after the service is made public. The client wants a simple report structure and does not want to receive daily findings.

Which of the following is most important for the penetration tester to define FIRST?

Options:

A- Establish the format required by the client.

B- Establish the threshold of risk to escalate to the client immediately.

C- Establish the method of potential false positives.

D- Establish the preferred day of the week for reporting.

Answer:

A

Question 5

Question Type: MultipleChoice

A consulting company is completing the ROE during scoping.

Which of the following should be included in the ROE?

Options:

A- Cost ofthe assessment

B- Report distribution

C- Testing restrictions

D- Liability

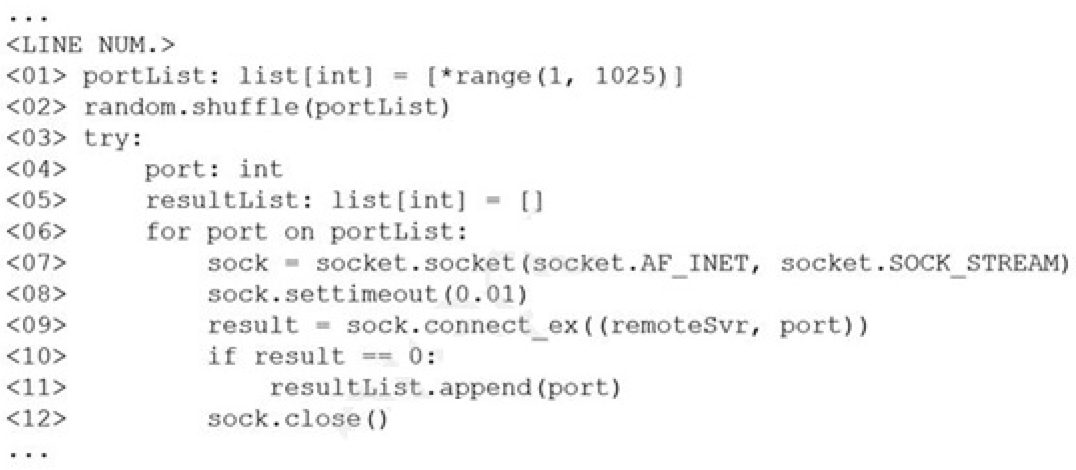
Answer:

B

Question 6

Question Type: **MultipleChoice**

The following line-numbered Python code snippet is being used in reconnaissance:



```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a "probable port scan" alert in the organization's IDS?

Options:

A- Line 01

B- Line 02

C- Line 07

D- Line 08

Answer:

D

Question 7

Question Type: **MultipleChoice**

A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test.

Which of the following describes the scope of the assessment?

Options:

A- Partially known environment testing

B- Known environment testing

C- Unknown environment testing

D- Physical environment testing

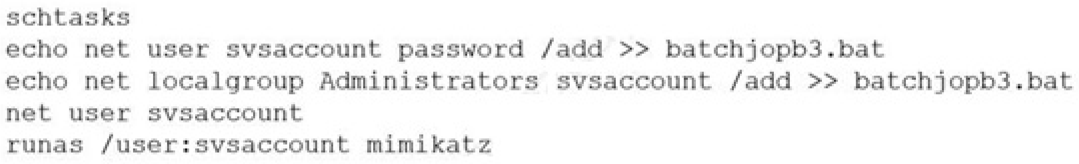
Answer:

C

Question 8

Question Type: MultipleChoice

A penetration tester ran the following commands on a Windows server:



```
schtasks
echo net user svsaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svsaccount /add >> batchjopb3.bat
net user svsaccount
runas /user:svsaccount mimikatz
```

Which of the following should the tester do AFTER delivering the final report?

Options:

A- Delete the scheduled batch job.

B- Close the reverse shell connection.

C- Downgrade the svsaccount permissions.

D- Remove the tester-created credentials.

Answer:

D

Question 9

Question Type: **MultipleChoice**

A company's Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi's router.

Which of the following is MOST vulnerable to a brute-force attack?

Options:

A- WPS

B- WPA2-EAP

C- WPA-TKIP

D- WPA2-PSK

Answer:

A

Question 10

Question Type: MultipleChoice

A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability.

Which of the following is the BEST way to ensure this is a true positive?

Options:

A- Run another scanner to compare.

B- Perform a manual test on the server.

C- Check the results on the scanner.

D- Look for the vulnerability online.

Answer:

B

Question 11

Question Type: MultipleChoice

A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.

In which of the following places should the penetration tester look FIRST for the employees' numbers?

Options:

A- Web archive

B- GitHub

C- File metadata

D- Underground forums

Answer:

A