Free Questions for PT0-002 by ebraindumps

Shared by Noble on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company has hired a penetration tester to deploy and set up a rogue access point on the network.

Which of the following is the BEST tool to use to accomplish this goal?

Options:

A- Wireshark

B- Aircrack-ng

C- Kismet

D- Wifite

Answer:

B

Question 2

Question Type: MultipleChoice

Which of the following tools would be MOST useful in collecting vendor and other security-relevant information for IoT devices to support passive reconnaissance?

Options:

A- Shodan

B- Nmap

C- WebScarab-NG

D- Nessus

Answer:

B

Question 3

Question Type: **MultipleChoice**

A penetration tester is attempting to discover live hosts on a subnet quickly.

Which of the following commands will perform a ping scan?

Options:

A- nmap -sn 10.12.1.0/24

B- nmap -sV -A 10.12.1.0/24

C- nmap -Pn 10.12.1.0/24

D- nmap -sT -p- 10.12.1.0/24

Answer:

A

Question 4

Question Type: MultipleChoice

A penetration tester found the following valid URL while doing a manual assessment of a web application: http://www.example.com/product.php?id=123987.

Which of the following automated tools would be best to use NEXT to try to identify a vulnerability in this URL?

Options:

A- SQLmap

B- Nessus

C- Nikto

D- DirBuster

Answer:

B

Question 5

Question Type: **MultipleChoice**

A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables.

Which of the following should be included as a recommendation in the remediation report?

Options:

A- Stronger algorithmic requirements

B- Access controls on the server

C- Encryption on the user passwords

D- A patch management program

Answer:

C

Question 6

Question Type: MultipleChoice

A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server.

Which of the following can be done with the pcap to gain access to the server?

Options:

A- Perform vertical privilege escalation.

B- Replay the captured traffic to the server to recreate the session.

C- Use John the Ripper to crack the password.

D- Utilize a pass-the-hash attack.

Answer:

D

Question 7

Question Type: MultipleChoice

A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary dat

a. The penetration testers have been given an internal network starting position.

Which of the following actions, if performed, would be ethical within the scope of the assessment?

Options:

A- Exploiting a configuration weakness in the SQL database

B- Intercepting outbound TLS traffic

C- Gaining access to hosts by injecting malware into the enterprise-wide update server

D- Leveraging a vulnerability on the internal CA to issue fraudulent client certificates

E- Establishing and maintaining persistence on the domain controller

Answer:

B

Question 8

Question Type: MultipleChoice

A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.

Which of the following is the BEST action for the penetration tester to take?

Options:

A- Utilize the tunnel as a means of pivoting to other internal devices.

B- Disregard the IP range, as it is out of scope.

C- Stop the assessment and inform the emergency contact.

D- Scan the IP range for additional systems to exploit.

Answer:

D

Question 9

Question Type: MultipleChoice

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.

Which of the following Nmap scan syntaxes would BEST accomplish this objective?

Options:

A- nmap -sT -vvv -O 192.168.1.2/24 -PO

B- nmap -sV 192.168.1.2/24 -PO

C- nmap -sA -v -O 192.168.1.2/24

D- nmap -sS -O 192.168.1.2/24 -T1

Answer:

D

To Get Premium Files for PT0-002 Visit

https://www.p2pexams.com/products/pt0-002

For More Free Questions Visit

https://www.p2pexams.com/comptia/pdf/pt0-002