PT0-002$^{Q\&As}$

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

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

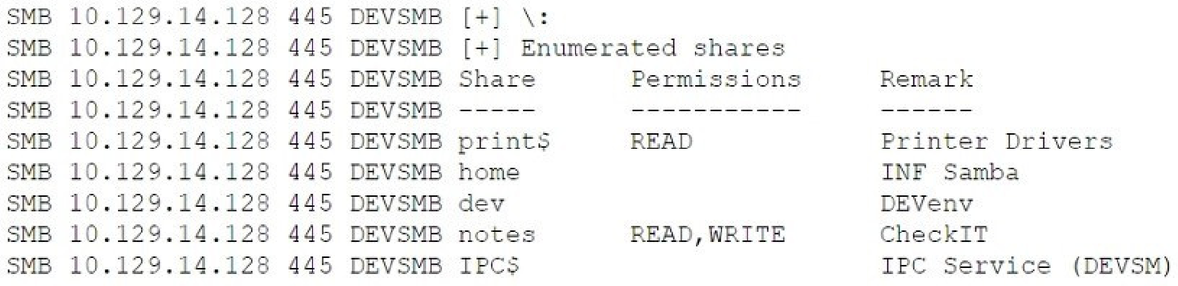
https://www.geekcert.com/pt0-002.html

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 is enumerating shares and receives the following output:



```
SMB 10.129.14.128 445 DEVSMB [+] \:
SMB 10.129.14.128 445 DEVSMB [+] Enumerated shares
SMB 10.129.14.128 445 DEVSMB Share      Permissions     Remark
SMB 10.129.14.128 445 DEVSMB -----      -----------     ------
SMB 10.129.14.128 445 DEVSMB print$     READ            Printer Drivers
SMB 10.129.14.128 445 DEVSMB home                       INF Samba
SMB 10.129.14.128 445 DEVSMB dev                        DEVenv
SMB 10.129.14.128 445 DEVSMB notes      READ,WRITE      CheckIT
SMB 10.129.14.128 445 DEVSMB IPC$                       IPC Service (DEVSM)
```

Which of the following should the penetration tester enumerate next?

A. dev

B. print$

C. home

D. notes

Correct Answer: A

QUESTION 2

A software company has hired a security consultant to assess the security of the company\\'s software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

A. Weak authentication schemes

B. Credentials stored in strings

C. Buffer overflows

D. Non-optimized resource management

Correct Answer: C

fuzzing introduces unexpected inputs into a system and watches to see if the system has any negative reactions to the inputs that indicate security, performance, or quality gaps or issues

QUESTION 3

During a vulnerability scan a penetration tester enters the following Nmap command against all of the non-Windows clients:

```
nmap -sX -T4 -p 21-25, 67, 80, 139, 8080 192.168.11.191
```

The penetration tester reviews the packet capture in Wireshark and notices that the target responds with an RST packet flag set for all of the targeted ports. Which of the following does this information most likely indicate?

A. All of the ports in the target range are closed.

B. Nmap needs more time to scan the ports in the target range.

C. The ports in the target range cannot be scanned because they are common UDP ports.

D. All of the ports in the target range are open

Correct Answer: A

The Nmap command uses the Xmas scan technique, which sends packets with the FIN, PSH, and URG flags set. This is an attempt to bypass firewall rules and elicit a response from open ports. However, if the target responds with an RST packet, it means that the port is closed. Open ports will either ignore the Xmas scan packets or send back an ACK packet. Therefore, the information most likely indicates that all of the ports in the target range are closed. References: [Nmap Scan Types], [Nmap Port Scanning Techniques], [CompTIA PenTest+ Study Guide: Exam PT0-002, Chapter 4: Conducting Passive Reconnaissance, page 127]

QUESTION 4

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?

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.

Correct Answer: D

QUESTION 5

A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client\\'s requirements?

A. "cisco-ios" "admin+1234"

B. "cisco-ios" "no-password"

C. "cisco-ios" "default-passwords"

D. "cisco-ios" "last-modified"

Correct Answer: B