PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

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

https://www.pass2lead.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

A. Storage access

B. Limited network access

C. Misconfigured DHCP server

D. Incorrect credentials

E. Network access controls

Correct Answer: AB

QUESTION 2

A penetration tester observes that the content security policy header is missing during a web application penetration test. Which of the following techniques would the penetration tester MOST likely perform?

A. Command injection attack

B. Clickjacking attack

C. Directory traversal attack

D. Remote file inclusion attack

Correct Answer: B

References: https://geekflare.com/http-header-implementation/

QUESTION 3

A web server is running PHP, and a penetration tester is using LFI to execute commands by passing parameters through the URL. This is possible because server logs were poisoned to execute the PHP system ( ) function. Which of the following would retrieve the contents of the passwd file?

A. \\'\\'andCMD_cat /etc/passwd--andid-34\\'\\'

B. \\'\\'andCMD=cat / etc/passwd%andid= 34\\'\\'

C. \\'\\'andCMD=cat ../../../../etc/passwd7id=34\\'

D. \\'\\'andsystem(CMD) \\'\\'cat /etc/passedandid=34\\'\\'

Correct Answer: A

QUESTION 4

A malicious user wants to perform an MITM attack on a computer. The computer network configuration is given below:

IP: 192.168.1.20 NETMASK: 255.255.255.0 DEFAULT GATEWAY: 192.168.1.254 DHCP: 192.168.1.253 DNS: 192.168.10.10, 192.168.20.10

Which of the following commands should the malicious user execute to perform the MITM attack?

A. arpspoof -c both -r -t 192.168.1.1 192.168.1.20

B. arpspoof -t 192.168.1.20 192.168.1.254

C. arpspoof -c both -t 192.168.1.20 192.168.1.253

D. arpspoof -r -t 192 .168.1.253 192.168.1.20

Correct Answer: B

Reference: https://www.hackers-arise.com/single-post/2017/07/25/Man-the-Middle-MiTM- Attack-with-ARPspoofing

QUESTION 5

A penetration tester is attempting to scan a legacy web application using the scanner\\'s default scan settings. The scans continually result in the application becoming unresponsive. Which of the following can help to alleviate this issue?

A. Packet shaping

B. Flow control

C. Bandwidth limits

D. Query throttling

Correct Answer: A