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.passapply.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

When conducting reconnaissance against a target, which of the following should be used to avoid directory communicating with the target?

A. Nmap tool

B. Maltego community edition

C. Nessus vulnerability scanner

D. OpenVAS

E. Melasploit

Correct Answer: B

QUESTION 2

A penetration tester is designing a phishing campaign and wants to build list of users (or the target organization. Which of the following techniques would be the MOST appropriate? (Select TWO)

A. Query an Internet WHOIS database.

B. Search posted job listings.

C. Scrape the company website.

D. Harvest users from social networking sites.

E. Socially engineer the corporate call center.

Correct Answer: CD

QUESTION 3

A company hires a penetration tester to determine if there are any vulnerabilities in its new VPN concentrator installation with an external IP of 100.170.60.5.

Which of the following commands will test if the VPN is available?

A. fpipe.exe -1 8080 -r 80 100.170.60.5

B. ike-scan -A -t 1 --sourceip=apoof_ip 100.170.60.5

C. nmap -sS -A -f 100.170.60.5

D. nc 100.170.60.5 8080 /bin/sh

Correct Answer: B

QUESTION 4

A penetration tester identifies the following findings during an external vulnerability scan:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80,443
SSLv3 accepted on the HTTPS connections	443
Mod_rewrite enabled on Apache servers	80,443
Windows Server 2012 host found	21

Which of the following attack strategies should be prioritized from the scan results above?

A. Obsolete software may contain exploitable components

B. Weak password management practices may be employed

C. Cryptographically weak protocols may be intercepted

D. Web server configurations may reveal sensitive information

Correct Answer: D

QUESTION 5

When considering threat actor scoping prior to an engagement, which of the following characteristics makes an APT challenging to emulate?

A. Development of custom zero-day exploits and tools

B. Leveraging the dark net for non-attribution

C. Tenacity and efficacy of social engineering attacks

D. Amount of bandwidth available for DoS attacks

Correct Answer: C