PT0-001$^{\text{Q\&As}}$

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

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

https://www.pass4itsure.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

A consultant is identifying versions of Windows operating systems on a network Which of the following Nmap commands should the consultant run?

A. nmap -T4 -v -sU -iL /tmp/list.txt -Pn --script smb-system-info

B. nmap -T4 -v -iL /tmp/list .txt -Pn --script smb-os-disccvery

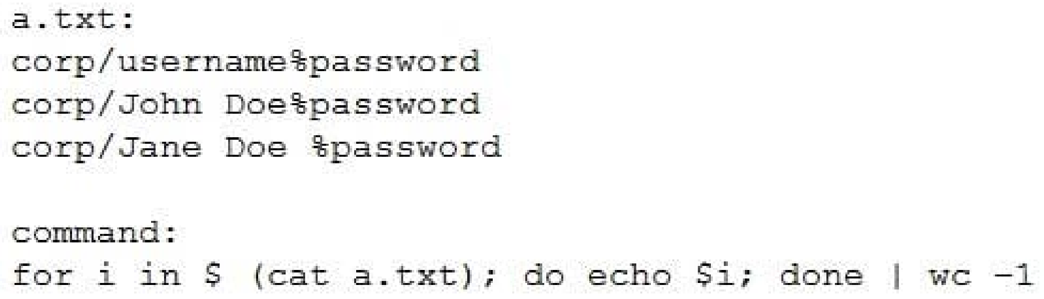
C. nmap -T4 -v -6 -iL /tmp/liat.txt -Pn --script smb-os-discovery -p 135-139

D. nmap -T4 -v --script smb-system-info 192.163.1.0/24

Correct Answer: B

QUESTION 2

A penetration tester runs the following on a machine:



```
a.txt:
corp/username%password
corp/John Doe%password
corp/Jane Doe %password

command:
for i in $ (cat a.txt); do echo $i; done | wc -1
```

Which of the following will be returned?

B. 3

C. 5

D. 6

Correct Answer: B

QUESTION 3

While engaging clients for a penetration test from highly regulated industries, which of the following is usually the MOST important to the clients from a business perspective?

A. Letter of engagement and attestation of findings

B. NDA and MSA

C. SOW and final report

D. Risk summary and executive summary

Correct Answer: B

QUESTION 4

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 5

A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the BEST step for the penetration tester to take?

A. Obtain staff information by calling the company and using social engineering techniques.

B. Visit the client and use impersonation to obtain information from staff.

C. Send spoofed emails to staff to see if staff will respond with sensitive information.

D. Search the Internet for information on staff such as social networking sites.

Correct Answer: D

Reference: https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it