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

QUESTION 1

A penetration tester ran an Nmap scan against a target and received the following output:

```
Starting Nmap 7.60 (https://nmap.org) at 2019-04-22 13:58 EDT
Nmap scan report for 192.168.121.1
Host is up (1.0s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open msrpc
139/tcp   open netbios-ssn
445/tcp   open microsoft-ds
3089/tcp  open ms-term-serv
```

Which of the following commands would be best for the penetration tester to execute NEXT to discover any weaknesses or vulnerabilities?

A. onesixtyone ? 192.168.121.1

B. enum4linux ? 192.168.121.1

C. snmpwalk ? public 192.168.121.1

D. medusa ? 192.168.121.1 ? users.txt ? passwords.txt ? ssh

Correct Answer: C

QUESTION 2

Which of the following is the MOST comprehensive type of penetration test on a network?

A. Black box

B. White box

C. Gray box

D. Red team

E. Architecture review

Correct Answer: A

Reference: https://purplesec.us/types-penetration-testing/

QUESTION 3

An engineer, who is conducting a penetration test for a web application, discovers the user login process sends from field data using the HTTP GET method. To mitigate the risk of exposing sensitive information, the form should be sent using an:

A. HTTP POST method.

B. HTTP OPTIONS method.

C. HTTP PUT method.

D. HTTP TRACE method.

Correct Answer: A

QUESTION 4

A penetration tester is using the Onesixtyone tool on Kali Linux to try to exploit the SNMP protocol on a target that has SNMP enabled Which of the following types of attacks is the penetration tester performing?

A. Buffer overflow attack

B. Man-in-the-middle attack

C. Dictionary-based attack

D. Name resolution attack

Correct Answer: C

QUESTION 5

A penetration tester needs to provide the code used to exploit a DNS server in the final report. In which of the following parts of the report should the penetration tester place the code?

A. Executive summary

B. Remediation

C. Conclusion

D. Technical summary

Correct Answer: A

Reference: https://phoenixnap.com/blog/penetration-testing