GPEN Q&As

GIAC Certified Penetration Tester

Pass GIAC GPEN Exam with 100% Guarantee

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

https://www.leads4pass.com/gpen.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which protocol would need to be available on a target in order for Nmap to identify services like IMAPS and POP3S?

A. HTTPS

B. SSL

C. LDAP

D. TLS

Correct Answer: A

Reference: http://nmap.org/book/vscan.html

QUESTION 2

You want to run the nmap command that includes the host specification of 202.176.56-57.*. How many hosts will you scan?

A. 256

B. 512

C. 1024

D. 64

Correct Answer: B

QUESTION 3

Fill in the blank with the appropriate word.

____is a port scanner that can also be used for the OS detection.

A. Nmap

Correct Answer: A

QUESTION 4

Why is OSSTMM beneficial to the pen tester?

A. It provides a legal and contractual framework for testing

B. It provides in-depth knowledge on tools

C. It provides report templates

D. It includes an automated testing engine similar to Metasploit

Correct Answer: C

Reference: http://www.pen-tests.com/open-source-security-testing-methodology-manual-osstmm.html

QUESTION 5

Which of the following is a tool for SSH and SSL MITM attacks?

A. Ettercap

B. Cain

C. Dsniff

D. AirJack

Correct Answer: C