# 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.geekcert.com/gpen.html**

100% Passing Guarantee
100% Money Back Assurance

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

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

**QUESTION 1**

Which of the following tasks can be performed by using netcat utility? Each correct answer represents a complete solution. Choose all that apply.

A. Firewall testing

B. Creating a Backdoor

C. Port scanning and service identification

D. Checking file integrity

Correct Answer: ABC

**QUESTION 2**

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint. Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

A. nmap -O -p

B. nmap -sS

C. nmap -sU -p

D. nmap –sT

Correct Answer: A

**QUESTION 3**

What happens when you scan a broadcast IP address of a network?

Each correct answer represents a complete solution. Choose all that apply.

A. It will show an error in the scanning process.

B. Scanning of the broadcast IP address cannot be performed.

C. It may show smurf DoS attack in the network IDS of the victim.

D. It leads to scanning of all the IP addresses on that subnet at the same time.

Correct Answer: CD

**QUESTION 4**

Which of the following statements about Fport is true?

A. It works as a process viewer.

B. It works as a datapipe on Windows.

C. It works as a datapipe on Linux.

D. It is a source port forwarder/redirector.

Correct Answer: A

**QUESTION 5**

You want to find out what ports a system is listening on. What Is the correct command on a Linux system?

A. netstat nap

B. f port/p

C. tasklist/v

D. Isof -nao

Correct Answer: A

Reference: http://cbl.abuseat.org/advanced.html