# GCFA$^{\text{Q\&As}}$

GIAC Certified Forensics Analyst

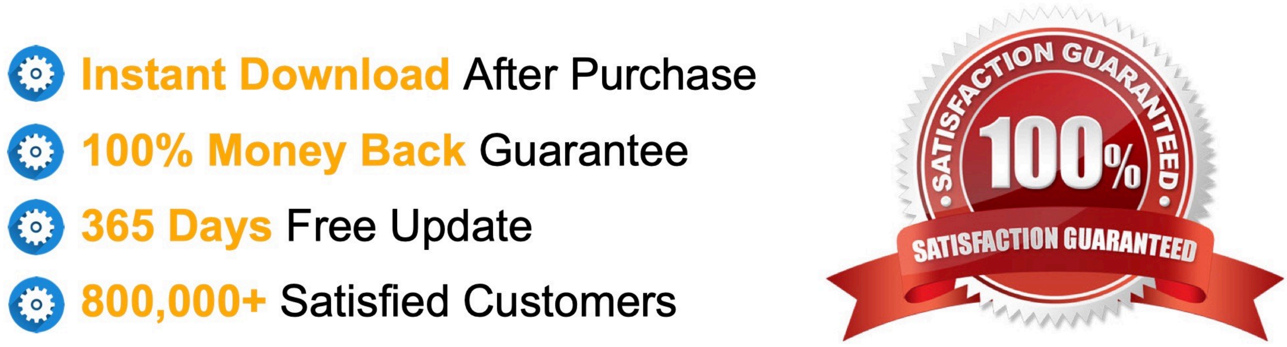
## Pass GIAC GCFA Exam with 100% Guarantee

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

**https://www.geekcert.com/gcfa.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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

**QUESTION 1**

TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?

A. Solaris

B. Red Hat

C. Knoppix

D. Windows

Correct Answer: D

**QUESTION 2**

An executive in your company reports odd behavior on her PDA. After investigation you discover that a trusted device is actually copying data off the PDA. The executive tells you that the behavior started shortly after accepting an e-business card from an unknown person. What type of attack is this?

A. Session Hijacking

B. Bluesnarfing

C. PDA Hijacking

D. Privilege Escalation

Correct Answer: B

**QUESTION 3**

Based on the case study, to implement more security, which of the following additional technologies should you implement for laptop computers?

(Click the Exhibit button on the toolbar to see the case study.)

Each correct answer represents a complete solution. Choose two.

A. PAP authentication

B. Encrypting File System (EFS)

C. Digital certificates

D. Two-factor authentication

E. Encrypted Data Transmissions

Correct Answer: BC

**QUESTION 4**

John works as a contract Ethical Hacker. He has recently got a project to do security checking for www.we-are-secure.com. He wants to find out the operating system of the we-are-secure server in the information gathering step. Which of the following commands will he use to accomplish the task?

Each correct answer represents a complete solution. Choose two.

A. nc 208.100.2.25 23

B. nmap -v -O www.we-are-secure.com

C. nc -v -n 208.100.2.25 80

D. nmap -v -O 208.100.2.25

Correct Answer: BD

**QUESTION 5**

Nathan works as a professional Ethical Hacker. He wants to see all open TCP/IP and UDP ports of his computer. Nathan uses the netstat command for this purpose but he is still unable to map open ports to the running process with PID, process name, and path. Which of the following commands will Nathan use to accomplish the task?

A. ping

B. Psloggedon

C. Pslist

D. fport

Correct Answer: D