



# GCFA<sup>Q&As</sup>

GIAC Certified Forensics Analyst

## Pass GIAC GCFA Exam with 100% Guarantee

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

<https://www.pass4itsure.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



**QUESTION 1**

Which of the following directories contains administrative commands on a UNIX computer?

- A. /usr/local
- B. /sbin
- C. /bin
- D. /export

Correct Answer: B

---

**QUESTION 2**

Adam works as a Security Analyst for Umbrella Inc. He suspects that a virus exists in the network of the company. He scanned the client system with latest signature-based anti-virus, but no productive results have been obtained. Adam suspects that a polymorphic virus exists in the network. Which of the following statements are true about the polymorphic virus?

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

- A. When the user runs the infected file in the disk, it loads virus into the RAM.
- B. The mutation engine of polymorphic virus generates a new encrypted code, this changes the signature of the virus.
- C. It has the ability to mutate and can change its known viral signature and hide from signature based antivirus programs.
- D. The new virus resides in the main memory of the computer and does not infect other files of the operating system.

Correct Answer: ABC

---

**QUESTION 3**

Which of the following involves changing data prior to or during input to a computer in an effort to commit fraud?

- A. Data diddling
- B. Spoofing
- C. Eavesdropping
- D. Wiretapping

Correct Answer: A

---

**QUESTION 4**

Adam works as a professional Penetration tester. A project has been assigned to him to employ penetration testing on the network of Umbrella Inc. He is running the test from home and had downloaded every security scanner from the Internet. Despite knowing the IP range of all of the systems, and the exact network configuration, Adam is unable to get any useful results.

Which of the following is the most like cause of this problem?

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

- A. Security scanners are only as smart as their database and cannot find unpublished vulnerabilities.
- B. Security scanners cannot perform vulnerability linkage.
- C. Security scanners are smart as their database and can find unpublished vulnerabilities.
- D. Security scanners are not designed to do testing through a firewall.

Correct Answer: ABD

---

**QUESTION 5**

Which of the following precautionary steps are taken by the supervisors or employers to avoid sexual harassment in workplace?

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

- A. Establish a complaint mechanism.
- B. Communicate to an employee who is indulging in such behavior.
- C. Contact the police and take legal action.
- D. Immediately take action on the complaint.

Correct Answer: ABD

[Latest GCFA Dumps](#)

[GCFA PDF Dumps](#)

[GCFA Practice Test](#)