



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

GIAC Certified Incident Handler

## Pass GIAC GCIH Exam with 100% Guarantee

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

<https://www.pass4itsure.com/gcih.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**

MyDoom, Zotob, and Blaster are all examples of what type of malware?

- A. Trojans
- B. Kernel-Mode Rootkits
- C. Worms
- D. Browser Helper Objects (BHOs)

Correct Answer: C

---

**QUESTION 2**

Maria works as the Chief Security Officer for PassGuide Inc. She wants to send secret messages to the CEO of the company. To secure these messages, she uses a technique of hiding a secret message within an ordinary message. The technique provides '\\security through obscurity\\'. What technique is Maria using?

- A. Steganography
- B. Public-key cryptography
- C. RSA algorithm
- D. Encryption

Correct Answer: A

---

**QUESTION 3**

Suppose a web application builds the SQL command "select PhoneNumber from contacts where Company = '\\[value]\\';". What would the result likely be if an attacker submitted the value "GIAC\\'; drop table contacts; --" to the database?

- A. Nothing. The '\\contacts;--\\' portion is syntactically incorrect.
- B. The database would attempt to drop the PhoneNumber from the '\\GIAC\\' table.
- C. The '\\contacts\\' table would be deleted from the database.
- D. The database would drop all records containing '\\GIAC\\' from the '\\contacts\\' table.

Correct Answer: B

---

**QUESTION 4**



Which Linux command will list locally defined Windows users, groups, and SID\\s?

- A. enum
- B. smbstatus
- C. rpcclient
- D. smbclient

Correct Answer: C

The rpcclient command list users and groups which are defined on the local host, as well as any domain users/groups the machine knows about. It also lists SIDs defined for local users. The enum command is a tool which runs on Windows to list users and groups. Smbclient is a Linux tool which can be used to list shares and get or put files on a Windows host. The smbstatus command lists current Samba connections.

---

#### QUESTION 5

Which of the following tools will show all TCP and UDP connections on a Windows system?

- A. Net
- B. TCPView
- C. Netcat
- D. Psinfo

Correct Answer: B

TCPView shows all TCP and UDP endpoints on your system. The listing includes the name of the process that owns each endpoint, the state of TCP connections, and the remote addresses. Psinfo, net, and netcat do not have this capability.

[GCIH VCE Dumps](#)

[GCIH Study Guide](#)

[GCIH Braindumps](#)