# GCFA 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.certbus.com/gcfa.html**

100% Passing Guarantee
100% Money Back Assurance

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



**QUESTION 1**

You want to change the attribute of a file named ACE.TXT to Hidden. Which command line will enable you to set the attribute?

A. ATTRIB ACE.TXT -H

B. ATTRIB ACE.TXT /HR

C. ATTRIB ACE.TXT +H

D. ATTRIB ACE.TXT /H

Correct Answer: C

**QUESTION 2**

Which of the following tools can be used to perform a whois query?

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

A. Sam Spade

B. SuperScan

C. Traceroute

D. WsPingPro

Correct Answer: ABD

**QUESTION 3**

Which of the following switches of the XCOPY command copies attributes while copying files?

A. /o

B. /p

C. /k

D. /s

Correct Answer: D

**QUESTION 4**

Which of the following file systems provides file-level security?

A. CDFS

B. FAT

C. FAT32

D. NTFS

Correct Answer: D

**QUESTION 5**

Mark works as a security manager for SofTech Inc. He is using a technique for monitoring what the employees are doing with corporate resources. Which of the following techniques is being used by Mark to gather evidence of an ongoing computer crime if a member of the staff is e- mailing company\\'s secrets to an opponent?

A. Electronic surveillance

B. Civil investigation

C. Physical surveillance

D. Criminal investigation

Correct Answer: A

**QUESTION 6**

Which of the following tools in Helix Windows Live is used to reveal the database password of password protected MDB files created using Microsoft Access or with Jet Database Engine?

A. Asterisk logger

B. FAU

C. Galleta

D. Access Pass View

Correct Answer: D

**QUESTION 7**

You work as a Network Administrator for NetTech Inc. The company\\'s network is connected to the Internet. For security, you want to restrict unauthorized access to the network with minimum administrative effort. You want to

implement a hardware-based solution. What will you do to accomplish this?

A. Connect a brouter to the network.

B. Implement firewall on the network.

C. Connect a router to the network.

D. Implement a proxy server on the network.

Correct Answer: B

**QUESTION 8**

Which of the following registry hives stores configuration information specific to a particular user who is currently logged on to the computer?

A. HKEY_USERS

B. HKEY_CURRENT_USER

C. HKEY_LOCAL_MACHINE

D. HKEY_CLASSES_ROOT

Correct Answer: B

**QUESTION 9**

Which of the following commands is used to create or delete partitions on Windows XP?

A. Part

B. DISKPART

C. fdisk

D. Active

Correct Answer: B

**QUESTION 10**

When you start your computer, Windows operating system reports that the hard disk drive has bad sectors. What will be your first step in resolving this issue?

A. Run the FORMAT command from DOS prompt.

B. Replace the data cable of the hard disk drive.

C. Run DEFRAG on the hard drive.

D. Run SCANDISK with the Thorough option.

Correct Answer: D

**QUESTION 11**

Which of the following types of attacks cannot be prevented by technical measures only?

A. Ping flood attack

B. Brute force

C. Smurf DoS

D. Social engineering

Correct Answer: D

**QUESTION 12**

Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?

A. Chain of evidence

B. Chain of custody

C. Incident response policy

D. Evidence access policy

Correct Answer: B

**QUESTION 13**

Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?

A. Technical representative

B. Information security representative

C. Legal representative

D. Lead investigator

Correct Answer: A

**QUESTION 14**

You are the Security Consultant and have been hired to check security for a client\\'s network. Your client has stated that he has many concerns but the most critical is the security of Web applications on their Web server. What should be your highest priority then in checking his network?

A. Vulnerability scanning

B. Setting up IDS

C. Port scanning

D. Setting up a honey pot

Correct Answer: A

**QUESTION 15**

Which of the following switches of the XCOPY command copies file ownerships and NTFS permissions on files while copying the files?

A. /r

B. /p

C. /s

D. /o

Correct Answer: D