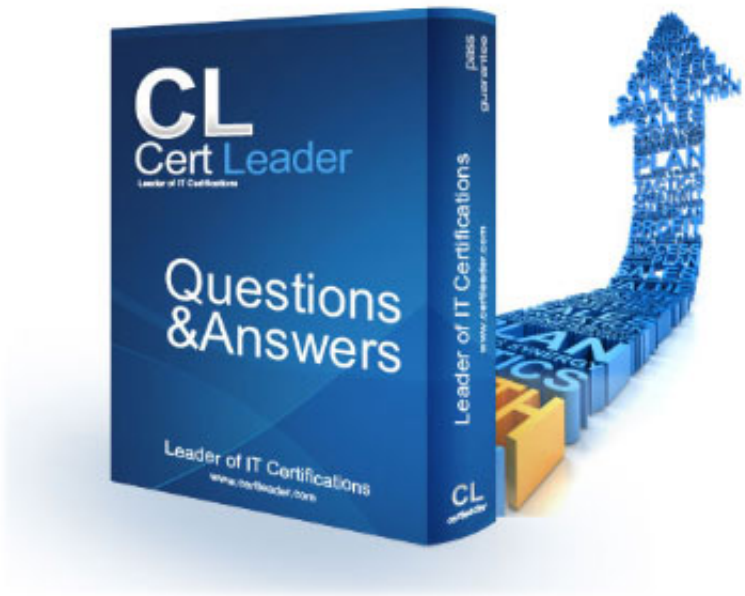
# GCFA - GIAC Certified Forensics Analyst

## https://www.certleader.com/GCFA-dumps.html



1. Which of the following statements about the compression feature of the NTFS file system are true?

Each correct answer represents a complete solution. Choose two.

A. Users can work with NTFS-compressed files without decompressing them.

B. It supports compression only on volumes.

C. Compressed files on an NTFS volume can be read and written by any Windows-based application after they are decompressed.

D. It supports compression on volumes, folders, and files.

**Answer:** A,D

2. Which of the following is used for remote file access by UNIX/Linux systems?

A. NetWare Core Protocol (NCP)

B. Common Internet File System (CIFS)

C. Server Message Block (SMB)

D. Network File System (NFS)

**Answer:** D

3. Which of the following uses hard disk drive space to provide extra memory for a computer?

A. Virtual memory

B. File system

C. Cluster

D. RAM

**Answer:** A

4. Which of the following laws or acts, formed in Australia, enforces prohibition against cyber stalking?

A. Stalking by Electronic Communications Act (2001)

B. Malicious Communications Act (1998)

C. Anti-Cyber-Stalking law (1999)

D. Stalking Amendment Act (1999)

**Answer:** D

5. You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack. Which of the following logs will you review to accomplish the task?

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

A. System logs

B. Event logs

C. Web server logs

D. Program logs

**Answer:** A,B,D

6. Which of the following statements are true about routers?

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

A. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.

B. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.

C. Routers do not limit physical broadcast traffic.

D. Routers act as protocol translators and bind dissimilar networks.

**Answer:** A,B,D

7. 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

**Answer:** B

8. Which of the following Windows Registry key contains the password file of the user?

A. HKEY_USER

B. HKEY_CURRENT_CONFIG

C. HKEY_DYN_DATA

D. HKEY_LOCAL_MACHINE

**Answer:** D

9. Which of the following file systems is used by both CD and DVD?

A. Network File System (NFS)

B. New Technology File System (NTFS)

C. Compact Disk File System (CDFS)

D. Universal Disk Format (UDF)

**Answer:** D

10. Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

A. 18 U.S.C. 1030

B. 18 U.S.C. 1362

C. 18 U.S.C. 2701

D. 18 U.S.C. 2510

E. 18 U.S.C. 1029

**Answer:** B

11. You want to retrieve information whether your system is in promiscuous mode or not. Which of the following commands will you use?

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

A. grep Promisc /var/log/messages

B. ip link

C. ifconfig | grep PROMISC

D. show promisc

**Answer:** A,B,C

12. Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate and examine drive image of a compromised system, which is suspected to be used in cyber crime. Adam uses Forensic Sorter to sort the contents of hard drive in different categories. Which of the following type of image formats is NOT supported by Forensic Sorter?

A. PFR image file

B. iso image file

C. RAW image file

D. EnCase image file

**Answer:** B

13. You work as a Network Administrator for Net World International. You want to configure a Windows 2000 computer to dual boot with Windows 98. The hard disk drive of the computer will be configured as a single partition drive. Which of the following file systems will you use to accomplish this?

A. NTFS

B. HPFS

C. FAT16

D. FAT32

**Answer:** D

14. Adam works as a Security Administrator for Umbrella Technology Inc. He reported a breach in security to his senior members, stating that "security defenses has been breached and exploited for 2 weeks by hackers." The hackers had accessed and downloaded 50,000 addresses containing customer credit cards and passwords. Umbrella Technology was looking to law enforcement officials to protect their intellectual

property. The intruder entered through an employee's home machine, which was connected to Umbrella Technology's corporate VPN network. The application called BEAST Trojan was used in the attack to open a "back door" allowing the hackers undetected access. The security breach was discovered when customers complained about the usage of their credit cards without their knowledge. The hackers were traced back to Shanghai, China through e-mail address evidence. The credit card information was sent to that same e-mail address. The passwords allowed the hackers to access Umbrella Technology's network from a remote location, posing as employees.

Which of the following actions can Adam perform to prevent such attacks from occurring in future?

A. Apply different security policy to make passwords of employees more complex.

B. Replace the VPN access with dial-up modem access to the company's network.

C. Disable VPN access to all employees of the company from home machines

D. Allow VPN access but replace the standard authentication with biometric authentication.

**Answer:** C

15. Which of the following tools is an asterisk password revealer tool?

A. Aircrack

B. SnadBoy

C. Cain and Abel

D. Pwdump3

**Answer:** B

16. John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. Which of the following commands will John use to display information about all mounted file systems?

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

A. du

B. ls

C. df

D. df -m

**Answer:** C,D

17. You work as a Computer Hacking Forensic Investigator for SecureNet Inc. You want to investigate Cross-Site Scripting attack on your company's Website. Which of the following methods of investigation can you use to accomplish the task?

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

A. Review the source of any HTML-formatted e-mail messages for embedded scripts or links in the URL to the company's site.

B. Use a Web proxy to view the Web server transactions in real time and investigate any communication with outside servers.

C. Use Wireshark to capture traffic going to the server and then searching for the requests going to the input page, which may give log of the malicious traffic and the IP address of the source.

D. Look at the Web servers logs and normal traffic logging.

**Answer:** A,B,D

18. Which of the following describes software technologies that improve portability, manageability, and compatibility of applications by encapsulating them from the underlying operating system on which they are executed?

A. Group Policy

B. System registry

C. System control

D. Application virtualization

**Answer:** D

19. Which of the following provides high availability of data?

A. RAID

B. Anti-virus software

C. EFS

D. Backup

**Answer:** A

20. Convention on Cybercrime, created by the Council of Europe, is the treaty seeking to address

Computer crime and Internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Which of the following chapters of Convention of Cybercrime contains the provisions for mutual assistances and extradition rules related to cybercrimes?

A. Chapter II

B. Chapter IV

C. Chapter III

D. Chapter I

**Answer:** C

# Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

## 100% Pass Your GCFA Exam with Our Prep Materials Via below:

https://www.certleader.com/GCFA-dumps.html