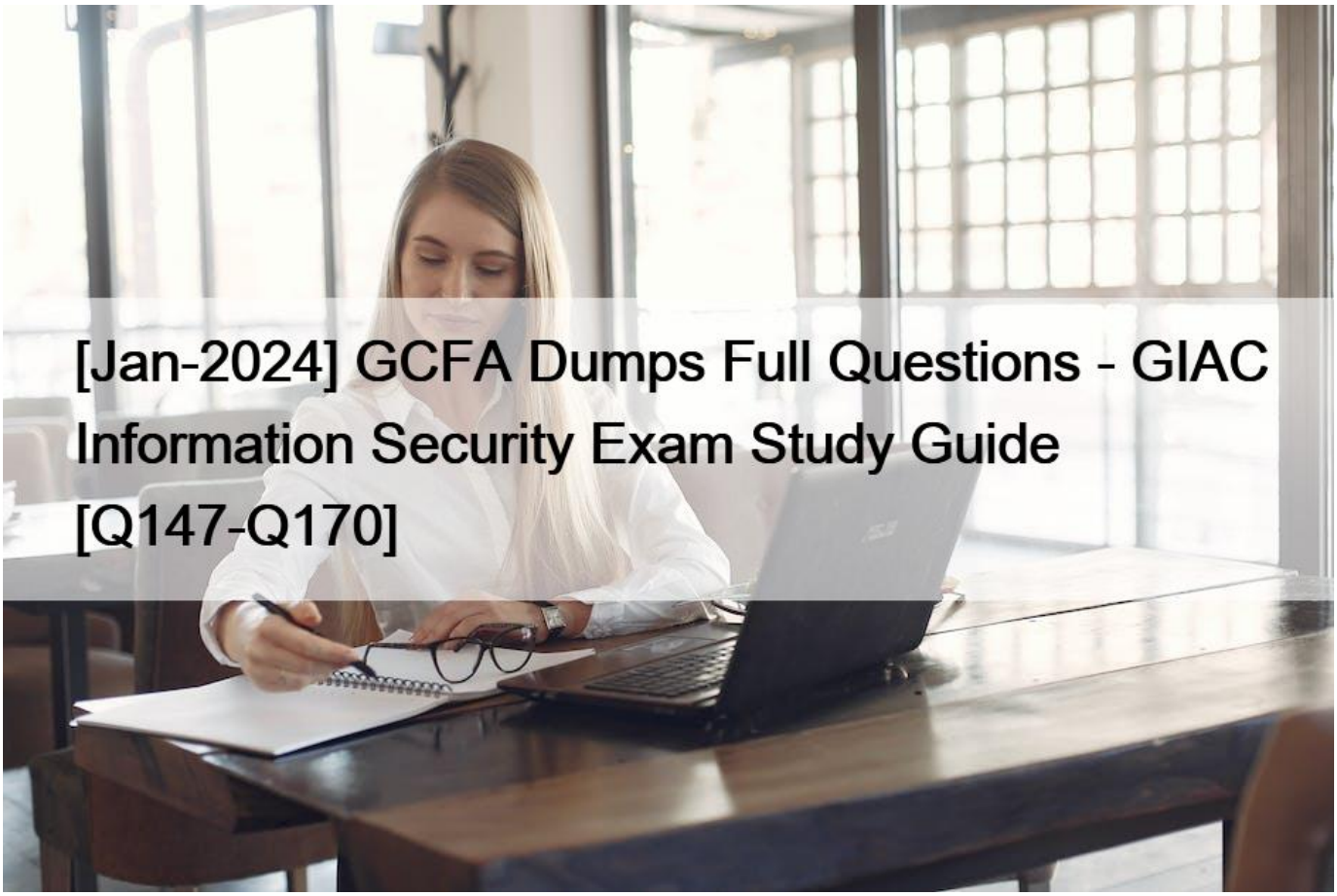
[Jan-2024 GCFA Dumps Full Questions - GIAC Information Security Exam Study Guide [Q147-Q170



[Jan-2024] GCFA Dumps Full Questions - GIAC Information Security Exam Study Guide
Exam Questions and Answers for GCFA Study Guide

NO.147 You want to upgrade a partition in your computer’s hard disk drive from FAT to NTFS. Which of the following DOS commands will you use to accomplish this?
* FORMAT C: /s
* CONVERT C: /fs:ntfs
* SYS C:
* FDISK /mbr

NO.148 Which of the following is used for remote file access by UNIX/Linux systems?
* NetWare Core Protocol (NCP)
* Common Internet File System (CIFS)
* Server Message Block (SMB)
* Network File System (NFS)

NO.149 Mark works as a Network administrator for SecureEnet Inc. His system runs on Mac OS

X. He wants to boot his system from the Network Interface Controller (NIC). Which of the following snag keys will Mark use to perform the required function?
* N
* D
* C
* Z
Section: Volume B

NO.150 You work as a Network Administrator for Blue Well Inc. Your company’s network has a Windows 2000 server with the FAT file system. This server stores sensitive data. You want to encrypt this data to protect it from unauthorized access. You also have to accomplish the following goals:

Data should be encrypted and secure.

▪

Administrative effort should be minimum.

▪

You should have the ability to recover encrypted files in case the file owner leaves the company.

▪

Other permissions on encrypted files should be unaffected.

▪

File-level security is required on the disk where data is stored.

▪

Encryption or decryption of files should not be the responsibility of the file owner.

▪

You take the following steps to accomplish these goals:

Convert the FAT file system to NTFS file system.

▪

Use third-party data encryption software.

▪

What will happen after taking these steps?

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

* File-level security will be available on the disk where data is stored.
* Data will be encrypted and secure.
* Encryption or decryption of files will no longer be the responsibility of the file owner.
* Other permissions on encrypted files will remain unaffected.
* Administrative effort will be minimum.

NO.151 You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to query an image root device and RAM disk size. Which of the following Unix commands can you use to accomplish the task?
* rdev
* mount
* setfdprm
* rdump

Section: Volume B

NO.152 John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He wants to test the effect of a virus on the We-are-secure server. He injects the virus on the server and, as a result, the server becomes infected with the virus even though an established antivirus program is installed on the server. Which of the following do you think are the reasons why the antivirus installed on the server did not detect the virus injected by John?

Each correct answer represents a complete solution. Choose all that apply.
* The mutation engine of the virus is generating a new encrypted code.
* The virus, used by John, is not in the database of the antivirus program installed on the server.
* John has created a new virus.
* John has changed the signature of the virus.

NO.153 Which of the following is used to store configuration settings and options on Microsoft Windows operating systems?
* Windows Config file
* Group policy editor
* Windows setting
* Windows Registry

NO.154 The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement?

Each correct answer represents a complete solution. Choose all that apply.
* Information dissemination policy
* Additional personnel security controls
* Incident response plan
* Electronic monitoring statement

NO.155 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.
* du
* ls
* df
* df -m

NO.156 Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?
* Chain of evidence
* Chain of custody
* Incident response policy
* Evidence access policy

Section: Volume B

NO.157 Which of the following diagnostic codes sent by POST to the internal port h80 refers to the system board error?
* 200 to 299
* 100 to 199
* 400 to 499
* 300 to 399

NO.158 John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He traceroutes the We-are-secure server and gets the following result:

```
traceroute to IP_address (IP_address): 1-30 hops, 38 byte packets
1 SF-rt5-fe9-0.geo.net (166.90.6.1) 0.48 ms 0.440 ms 0.378 ms
2 SF-core1-h1.geo.net (166.90.1.17) 0.618 ms 0.571 ms 0.521 ms
3 SF-rt2-f0.geo.net (166.90.5.7) 1.19 ms 1.94 ms 1.13 ms
4 * * *
5 * * *
```

Considering the above traceroute result, which of the following statements can be true?

Each correct answer represents a complete solution. Choose all that apply.
* While tracerouting, John’s network connection has become slow.
* Some router along the path is down.
* The We-are-secure server is using a packet filtering firewall.
* The IP address of the We-are-secure server is not valid.

Section: Volume B

NO.159 John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He wants to test the effect of a virus on the We-are-secure server. He injects the virus on the server and, as a result, the server becomes infected with the virus even though an established antivirus program is installed on the server. Which of the following do you think are the reasons why the antivirus installed on the server did not detect the virus injected by John?

Each correct answer represents a complete solution. Choose all that apply.
* The mutation engine of the virus is generating a new encrypted code.
* The virus, used by John, is not in the database of the antivirus program installed on the server.
* John has created a new virus.
* John has changed the signature of the virus.

Section: Volume B

NO.160 Mark is the Administrator of a Linux computer. He wants to check the status of failed Telnet-based login attempts on the Linux computer. Which of the following shell commands will he use to accomplish the task?
* GREP
* CP
* FSCK

* CAT

NO.161 You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to allow direct access to the filesystems data structure. Which of the following Unix commands can you use to accomplish the task?
* du
* debugfs
* df
* dosfsck

NO.162 Which of the following IP addresses are private addresses?

Each correct answer represents a complete solution. Choose all that apply.
* 19.3.22.17
* 192.168.15.2
* 192.166.54.32
* 10.0.0.3

NO.163 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?
* Run the FORMAT command from DOS prompt.
* Replace the data cable of the hard disk drive.
* Run DEFRAG on the hard drive.
* Run SCANDISK with the Thorough option.

NO.164 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.
* Users can work with NTFS-compressed files without decompressing them.
* It supports compression only on volumes.
* Compressed files on an NTFS volume can be read and written by any Windows-based application after they are decompressed.
* It supports compression on volumes, folders, and files.

NO.165 Which of the following is included in a memory dump file?
* Security ID
* List of loaded drivers
* The kernel-mode call stack for the thread that stopped the process from execution
* Stop message and its parameters

NO.166 Which of the following file systems provides file-level security?
* CDFS
* FAT
* FAT32
* NTFS

NO.167 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.
* nc 208.100.2.25 23

* nmap -v -O www.we-are-secure.com
* nc -v -n 208.100.2.25 80
* nmap -v -O 208.100.2.25

Explanation/Reference:

NO.168 Adrian, the Network Administrator for Peach Tree Inc., wants to install a new computer on the company’s network. He asks his assistant to make a boot disk with minimum files. The boot disk will be used to boot the computer, which does not have an operating system installed, yet. Which of the following files will he include on the disk?

* IO.SYS, MSDOS.SYS, COMMAND.COM, and AUTOEXEC.BAT.
* IO.SYS, MSDOS.SYS, and COMMAND.COM.
* IO.SYS, MSDOS.SYS, COMMAND.COM, and CONFIG.SYS.
* IO.SYS, MSDOS.SYS, COMMAND.COM, and FDISK.

NO.169 Which of the following file systems provides integrated security?

* CDFS
* EFS
* HPFS
* FAT32

NO.170 Adam, a malicious hacker, hides a hacking tool from a system administrator of his company by using Alternate Data Streams (ADS) feature. Which of the following statements is true in context with the above scenario?

* Alternate Data Streams is a feature of Linux operating system.
* Adam is using FAT file system.
* Adam is using NTFS file system.
* Adam’s system runs on Microsoft Windows 98 operating system.