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.pass2lead.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

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

Correct Answer: A

QUESTION 2

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

Correct Answer: CD

QUESTION 3

Trinity wants to send an email to her friend. She uses the MD5 generator to calculate cryptographic hash of her email to ensure the security and integrity of the email. MD5 generator, which Trinity is using operates in two steps:

Creates check file

Verifies the check file

Which of the following MD5 generators is Trinity using?

A. MD5 Checksum Verifier

B. Mat-MD5

C. Chaos MD5

D. Secure Hash Signature Generator

Correct Answer: A

QUESTION 4

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 5

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. He wants to forward all the kernel messages to the remote host having IP address 192.168.0.1. Which of the following changes will he perform in the syslog.conf file to accomplish the task?

A. kern.* @192.168.0.1

B. !*.* @192.168.0.1

C. *.* @192.168.0.1

D. !kern.* @192.168.0.1

Correct Answer: A

QUESTION 6

The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook\\'s preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?

A. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"

D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Correct Answer: C

QUESTION 7

Which of the following statements is NOT true about FAT16 file system? Each correct answer represents a complete solution. Choose all that apply.

A. FAT16 file system supports Linux operating system.

B. FAT16 file system supports file-level compression.

C. FAT16 file system works well with large disks because the cluster size increases as the disk partition size increases.

D. FAT16 does not support file-level security.

Correct Answer: BC

QUESTION 8

Which of the following is a nonvolatile form of memory that can be reprogrammed by using a special programming device, and need not to be removed from the PC to be reprogrammed?

A. PROM

B. EPROM

C. EEPROM

D. SRAM

E. DRAM

Correct Answer: C

QUESTION 9

You work as a Network Administrator for Perfect Solutions Inc. You install Windows 98 on a computer. By default, which of the following folders does Windows 98 setup use to keep the registry tools?

A. $SYSTEMROOT$REGISTRY

B. $SYSTEMROOT$WINDOWS

C. $SYSTEMROOT$WINDOWSREGISTRY

D. $SYSTEMROOT$WINDOWSSYSTEM32

Correct Answer: B

QUESTION 10

Which of the following needs to be documented to preserve evidences for presentation in court?

A. Separation of duties

B. Incident response policy

C. Chain of custody

D. Account lockout policy

Correct Answer: C

QUESTION 11

Which of the following registry hives stores information about the file extensions that are mapped to their corresponding applications?

A. HKEY_CURRENT_USER

B. HKEY_USERS

C. HKEY_CLASSES_ROOT

D. HKEY_LOCAL_MACHINE

Correct Answer: C

QUESTION 12

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 13

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 14

Fill in the blank with the appropriate file system.

Alternate Data Streams (ADS) is a feature of the file system, which allows more than one data stream to be associated with a filename.

Correct Answer: NTFS

QUESTION 15

Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?

A. Melissa

B. Tequila

C. Brain

D. I love you

Correct Answer: C