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.passapply.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 Windows XP system files handles memory management, I/O operations, and interrupts?

A. Ntoskrnl.exe

B. Win32k.sys

C. Advapi32.dll

D. Kernel32.dll

Correct Answer: D

QUESTION 2

Which of the following type of file systems is not supported by Linux kernel?

A. vFAT

B. NTFS

C. HFS

D. FAT32

Correct Answer: D

QUESTION 3

You work as a Forensic Investigator. Which of the following rules will you follow while working on a case? Each correct answer represents a part of the solution. Choose all that apply.

A. Prepare a chain of custody and handle the evidence carefully.

B. Examine original evidence and never rely on the duplicate evidence.

C. Never exceed the knowledge base of the forensic investigation.

D. Follow the rules of evidence and never temper with the evidence.

Correct Answer: ABCD

QUESTION 4

Adam works as a professional Computer Hacking Forensic Investigator, a project has been assigned to him to investigate and examine files present on suspect\\'s computer. Adam uses a tool with the help of which he can examine recovered deleted files, fragmented files, and other corrupted data. He can also examine the data, which was captured from the network, and access the physical RAM, and any processes running in virtual memory with the help of this tool.

Which of the following tools is Adam using?

A. Evidor

B. HxD

C. WinHex

D. Vedit

Correct Answer: C

QUESTION 5

Peter, an expert computer user, attached a new sound card to his computer. He then restarts the computer, so that the BIOS can scan the hardware changes. What will be the memory range of ROM that the BIOS scan for additional code to be executed for proper working of soundcard?

A. hC800 to hDF80

B. hCA79 to hAC20

C. hAA43 to hF345

D. hDF80 to hFF80

Correct Answer: A

QUESTION 6

In which of the following security tests does the security testing team simulate as an employee or other person with an authorized connection to the organization\\'s network?

A. Remote network

B. Remote dial-up network

C. Stolen equipment

D. Local network

Correct Answer: D

QUESTION 7

Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer. After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting. for ((i = 0;i