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.leads4pass.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

Sandra, a novice computer user, works on Windows environment. She experiences some problem regarding bad sectors formed in a hard disk of her computer. She wants to run CHKDSK command to check the hard disk for bad sectors and to fix the errors, if any, occurred. Which of the following switches will she use with CHKDSK command to accomplish the task?

A. CHKDSK /I

B. CHKDSK /C /L

C. CHKDSK /V /X

D. CHKDSK /R /F

Correct Answer: D

QUESTION 3

Which of the following tools is used to locate lost files and partitions to restore data from a formatted, damaged, or lost partition in Windows and Apple Macintosh computers?

A. Easy-Undelete

B. File Scavenger

C. Recover4all Professional

D. VirtualLab

Correct Answer: D

QUESTION 4

Peter works as a Technical Representative in a CSIRT for SecureEnet Inc. His team is called to investigate the

computer of an employee, who is suspected for classified data theft. Suspect\\'s computer runs on Windows operating system. Peter wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?

A. Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces

B. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps

C. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system

D. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces

Correct Answer: D

QUESTION 5

Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it to chess.exe. The size of chess.exe was 526,895 bytes originally, and after joining this chess file to the Trojan, the file size increased to 651,823 bytes. When he gives you this new game, you install the infected chess.exe file on your computer. He now performs various malicious tasks on your computer remotely. But you suspect that someone has installed a Trojan on your computer and begin to investigate it. When you enter the netstat command in the command prompt, you get the following results:

C:\WINDOWS>netstat -an | find "UDP"

UDP IP_Address:31337 *:*

Now you check the following registry address:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

In the above address, you notice a \\'default\\' key in the \\'Name\\' field having " .exe" value in the corresponding \\'Data\\' field. Which of the following Trojans do you think your friend may have installed on your computer on the basis of the above evidence?

A. Tini

B. Qaz

C. Donald Dick

D. Back Orifice

Correct Answer: D