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 statements are NOT true about volume boot record or Master Boot Record? Each correct answer represents a complete solution. Choose all that apply.

A. The end of MBR marker is h55CC.

B. The actual program can be 512 bytes long.

C. Volume boot sector is present at cylinder 0, head 0, and sector 1 of the default boot drive.

D. Four 16 bytes master partition records are present in MBR.

Correct Answer: AB

QUESTION 2

The MBR of a hard disk is a collection of boot records that contain disk information such as disk architecture, cluster size, and so on. The main work of the MBR is to locate and run necessary operating system files that are required to run a hard disk. In the context of the operating system, MBR is also known as the boot loader. Which of the following viruses can infect the MBR of a hard disk?

Each correct answer represents a complete solution. Choose two.

A. Stealth

B. Boot sector

C. Multipartite

D. File

Correct Answer: BC

QUESTION 3

Which of the following statements is NOT true about the file slack spaces in Windows operating system?

A. File slack may contain data from the memory of the system.

B. Large cluster size will decrease the volume of the file slack.

C. File slack is the space, which exists between the end of the file and the end of the last cluster.

D. It is possible to find user names, passwords, and other important information in slack.

Correct Answer: B

QUESTION 4

You are reviewing a Service Level Agreement between your company and a Web development vendor.

Which of the following are security requirements you should look for in this SLA?

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

A. Time to respond to bug reports

B. Encryption standards

C. Security Monitoring

D. Guarantees on known security flaws

Correct Answer: ABCD

QUESTION 5

Which of the following diagnostic codes sent by POST to the internal port h80 refers to the system board error?

A. 200 to 299

B. 100 to 199

C. 400 to 499

D. 300 to 399

Correct Answer: B