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

Which of the following encryption methods use the RC4 technology?

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

A. Dynamic WEP

B. TKIP

C. Static WEP

D. CCMP

Correct Answer: ABC

QUESTION 3

Which of the following prevents malicious programs from attacking a system?

A. Anti-virus program

B. Smart cards

C. Biometric devices

D. Firewall

Correct Answer: A

QUESTION 4

John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He is working on the Linux operating system and wants to install an Intrusion Detection System on the We-are-secure server so that he can receive alerts about any hacking attempts. Which of the following tools can John use to accomplish the task?

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

A. SARA

B. Snort

C. Tripwire

D. Samhain

Correct Answer: BD

QUESTION 5

Which of the following directories in Linux operating system contains device files, which refers to physical devices?

A. /boot

B. /etc

C. /dev

D. /bin

Correct Answer: C