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 attacks saturates network resources and disrupts services to a specific computer?

A. Teardrop attack

B. Polymorphic shell code attack

C. Denial-of-Service (DoS) attack

D. Replay attack

Correct Answer: C

QUESTION 2

John works as a Technical Support Executive in ABC Inc. The company\\'s network consists of ten computers with Windows XP professional installed on all of them. John is working with a computer on which he has enabled hibernation. He shuts down his computer using hibernation mode. Which of the following will happen to the data after powering off the system using hibernation?

A. Data will be saved automatically before the system is switched off.

B. Data will be stored on the ROM.

C. Data will be saved before the system is switched off if you have configured hibernation to save data.

D. Unsaved data will be lost when hibernation switches off the system.

Correct Answer: A

QUESTION 3

Normally, RAM is used for temporary storage of data. But sometimes RAM data is stored in the hard disk, what is this method called?

A. Cache memory

B. Static memory

C. Virtual memory

D. Volatile memory

Correct Answer: C

QUESTION 4

Based on the case study, to implement more security, which of the following additional technologies should you implement for laptop computers?

(Click the Exhibit button on the toolbar to see the case study.)

Each correct answer represents a complete solution. Choose two.

A. PAP authentication

B. Encrypting File System (EFS)

C. Digital certificates

D. Two-factor authentication

E. Encrypted Data Transmissions

Correct Answer: BC

QUESTION 5

TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?

A. Solaris

B. Red Hat

C. Knoppix

D. Windows

Correct Answer: D