412-79 Q&As

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/412-79.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

An Employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the Employees Computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekenD. You detain the Employee before he leaves the building and recover the floppy disks and secure his computer. Will you be able to break the encryption so that you can verify that that the employee was in possession of the proprietary information?

A. EFS uses a 128- bit key that can t be cracked, so you will not be able to recover the information

B. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information

C. The EFS Revoked Key Agent can be used on the Computer to recover the information

D. When the Encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information.

Correct Answer: B

QUESTION 2

You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA

class. He asks about the methodology you will be using to test the company\\'s network.

How would you answer?

A. IBM Methodology

B. LPT Methodology

C. Google Methodology

D. Microsoft Methodology

Correct Answer: B

QUESTION 3

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Windows computers are constantly talking

B. Linux/Unix computers are constantly talking

C. Linux/Unix computers are easier to compromise

D. Windows computers will not respond to idle scans

Correct Answer: A

QUESTION 4

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers clocks are synchronize D. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

A. Universal Time Set

B. Network Time Protocol

C. SyncTime Service

D. Time-Sync Protocol

Correct Answer: B

QUESTION 5

What does the superblock in Linux define?

A. filesynames

B. diskgeometr

C. location of the firstinode

D. available space

Correct Answer: C