312-49V10^Q&As

ECCouncil Computer Hacking Forensic Investigator (V10)

Pass EC-COUNCIL 312-49V10 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-49v10.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

A. Swap space

B. Application data

C. Files and documents

D. Slack space

Correct Answer: A

QUESTION 2

Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

A. Profile/Fingerprint-Based Approach

B. Bayesian Correlation

C. Time (Clock Time) or Role-Based Approach

D. Automated Field Correlation

Correct Answer: B

Reference: https://info-savvy.com/summarize-the-event-correlation/#:~:text=Bayesian%20Correlation%20Approach,by%20studying%20statistics%20and%20probability

QUESTION 3

An expert witness is a _____ who is normally appointed by a party to assist the formulation and preparation of a party\\'s claim or defense.

A. Expert in criminal investigation

B. Subject matter specialist

C. Witness present at the crime scene

D. Expert law graduate appointed by attorney

Correct Answer: B

QUESTION 4

Data acquisition system is a combination of tools or processes used to gather, analyze and record Information about some phenomenon. Different data acquisition system are used depends on the location, speed, cost. etc. Serial communication data acquisition system is used when the actual location of the data is at some distance from the computer. Which of the following communication standard is used in serial communication data acquisition system?

A. RS422

B. RS423

C. RS232

D. RS231

Correct Answer: C

QUESTION 5

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\LSA

B. %systemroot%\system32\drivers\etc

C. %systemroot%\repair

D. %systemroot%\system32\LSA

Correct Answer: C