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.geekcert.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

Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot

records, or memory with a known and trusted baseline?

A. Signature-Based Detection

B. Integrity-Based Detection

C. Cross View-Based Detection

D. Heuristic/Behavior-Based Detection

Correct Answer: B

Reference: https://info-savvy.com/anti-forensics-techniques-rootkits/

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

When an investigator contacts by telephone the domain administrator or controller listed by a whois lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

A. Title 18, Section 1030

B. Title 18, Section 2703(d)

C. Title 18, Section Chapter 90

D. Title 18, Section 2703(f)

Correct Answer: D

QUESTION 4

Centralized logging is defined as gathering the computer system logs for a group of systems in a centralized location. It is used to efficiently monitor computer system logs with the frequency required to detect security violations and unusual activity.

A. True

B. False

Correct Answer: A

QUESTION 5

Damaged portions of a disk on which no read/Write operation can be performed is known as _____.

A. Lost sector

B. Bad sector

C. Empty sector

D. Unused sector

Correct Answer: B

312-49V10 PDF Dumps 312-49V10 Exam Questions 312-49V10 Braindumps