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.geekcert.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

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

QUESTION 1

If you come across a sheepdip machine at your client site, what would you infer?

A. Asheepdip coordinates several honeypots

B. Asheepdip computer is another name for a honeypot

C. Asheepdip computer is used only for virus-checking.

D. Asheepdip computer defers a denial of service attack

Correct Answer: C

QUESTION 2

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Open

B. Stealth

C. Closed

D. Filtered

Correct Answer: A

QUESTION 3

You should make at least how many bit-stream copies of a suspect drive?

A. 1

B. 2

C. 3

D. 4

Correct Answer: D

QUESTION 4

Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of

users and networks?

A. network-based IDS systems (NIDS)

B. host-based IDS systems (HIDS)

C. anomaly detection

D. signature recognition

Correct Answer: B

QUESTION 5

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Use attack as a launching point to penetrate deeper into the network

B. Demonstrate that no system can be protected against DoS attacks

C. List weak points on their network

D. Show outdated equipment so it can be replaced

Correct Answer: C