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

It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

A. by law, three

B. quite a few

C. only one

D. at least two

Correct Answer: C

QUESTION 2

What TCP/UDP port does the toolkit program netstat use?

A. Port 7

B. Port 15

C. Port 23

D. Port 69

Correct Answer: B

QUESTION 3

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company\\'s clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

A. Ping sweep

B. Netcraft

C. Dig

D. Nmap

Correct Answer: B

QUESTION 4

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known

vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. CVE

B. IANA

C. RIPE

D. APIPA

Correct Answer: A

QUESTION 5

George is a senior security analyst working for a state agency in Florida. His state\\'s congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?

A. Pattern matching

B. Statistical-based anomaly detection

C. Real-time anomaly detection

D. Signature-based anomaly detection

Correct Answer: C