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

What should you do when approached by a reporter about a case that you are working on or have worked on?

A. Refer the reporter to the attorney that retained you

B. Say, "no comment"

C. Answer all the reporters questions as completely as possible

D. Answer only the questions that help your case

Correct Answer: A

QUESTION 2

Jason is the security administrator of ACMA metal Corporation. One day he notices the company s Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crimes investigations throughout the United States?

A. Internet Fraud Complaint Center

B. Local or national office of the U.S. Secret Service

C. National Infrastructure Protection Center

D. CERT Coordination Center

Correct Answer: B

QUESTION 3

One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

A. the File Allocation Table

B. the file header

C. the file footer

D. the sector map

Correct Answer: B

QUESTION 4

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Fraggle

B. SYN flood

C. Trinoo

D. Smurf

Correct Answer: D

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