412-79Q&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 does the acronym POST mean as it relates to a PC?

A. Primary Operations Short Test

B. Power On Self Test

C. Pre Operational Situation Test

D. Primary Operating System Test

Correct Answer: B

QUESTION 2

What information do you need to recover when searching a victims computer for a crime committed with specific e-mail message?

A. Internet service provider information

B. E-mail header

C. Username and password

D. Firewall log

Correct Answer: B

QUESTION 3

Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?

A. the Microsoft Virtual Machine Identifier

B. the Personal Application Protocol

C. the Globally Unique ID

D. the Individual ASCII String

Correct Answer: C

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

Law enforcement officers are conducting a legal search for which a valid warrant was obtaineD. While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A. Plain view doctrine

B. Corpus delicti

C. Locard Exchange Principle

D. Ex Parte Order

Correct Answer: A