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.pass2lead.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

The newer Macintosh Operating System is based on:

A. OS/2

B. BSD Unix

C. Linux

D. Microsoft Windows

Correct Answer: B

QUESTION 2

You have used a newly released forensic investigation tool, which doesn t meet the Daubert T est, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

A. The tool hasn t been tested by the International Standards Organization (ISO)

B. Only the local law enforcement should use the tool

C. The total has not been reviewed and accepted by your peers

D. You are not certified for using the tool

Correct Answer: C

QUESTION 3

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well- tested hardware write-blocking device to:

A. Automate Collection from image files

B. Avoiding copying data from the boot partition

C. Acquire data from host-protected area on a disk

D. Prevent Contamination to the evidence drive

Correct Answer: D

QUESTION 4

If you discover a criminal act while investigating a corporate policy abuse, it becomes a public- sector investigation and should be referred to law enforcement?

A. true

B. false

Correct Answer: A

QUESTION 5

During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore you report this evidence. This type of evidence is known as:

A. Inculpatory evidence

B. mandatory evidence

C. exculpatory evidence

D. Terrible evidence

Correct Answer: C

412-79 VCE Dumps 412-79 Practice Test 412-79 Study Guide