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.leads4pass.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

You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question weather evidence has been changed while at the laB. What can you do to prove that the evidence is the same as it was when it first entered the lab?

A. make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab

B. make an MD5 hash of the evidence and compare it to the standard database developed by NIST

C. there is no reason to worry about this possible claim because state labs are certified

D. sign a statement attesting that the evidence is the same as it was when it entered the lab

Correct Answer: A

QUESTION 2

One way to identify the presence of hidden partitions on a suspect s hard drive is to:

A. Add up the total size of all known partitions and compare it to the total size of the hard drive

B. Examine the FAT and identify hidden partitions by noting an H in the partition Type field

C. Examine the LILO and note an H in the partition Type field

D. It is not possible to have hidden partitions on a hard drive

Correct Answer: A

QUESTION 3

Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

A. 18 U.S.C. 1029

B. 18 U.S.C. 1362

C. 18 U.S.C. 2511

D. 18 U.S.C. 2703

Correct Answer: A

QUESTION 4

A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?

A. Root Internet servers

B. Border Gateway Protocol

C. Gateway of last resort

D. Reverse DNS

Correct Answer: C

QUESTION 5

_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

A. Network Forensics

B. Computer Forensics

C. Incident Response

D. Event Reaction

Correct Answer: B

[412-79 VCE Dumps](#)   [412-79 Practice Test](#)   [412-79 Braindumps](#)