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.passapply.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 running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-open

B. The firewall failed-bypass

C. The firewall failed-closed

D. The firewall ACL has been purged

Correct Answer: A

QUESTION 2

You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?

A. 70 years

B. the life of the author

C. the life of the author plus 70 years

D. copyrights last forever

Correct Answer: C

QUESTION 3

Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

A. Use Vmware to be able to capture the data in memory and examine it

B. Give the Operating System a minimal amount of memory, forcing it to use a swap file

C. Create a Separate partition of several hundred megabytes and place the swap file there

D. Use intrusion forensic techniques to study memory resident infections

Correct Answer: C

QUESTION 4

In Microsoft file structures, sectors are grouped together to form:

A. Clusters

B. Drives

C. Bitstreams

D. Partitions

Correct Answer: A

QUESTION 5

What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

A. mcopy

B. image

C. MD5

D. dd

Correct Answer: D

Latest 412-79 Dumps 412-79 VCE Dumps 412-79 Study Guide