DUMPSBOSS.

EC-Council Certified Security Analyst (ECSA)

ECCouncil EC0-479

Version Demo

Total Demo Questions: 12

Total Premium Questions: 231

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	49
Topic 2, Volume B	50
Topic 3, Volume C	49
Topic 4, Volume D	50
Topic 5, Volume E	33
Total	231

QUESTION NO: 1

In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

A. rules of evidence

B. law of probability

C. chain of custody

D. policy of separation

ANSWER: C

QUESTION NO: 2

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

ANSWER: B

QUESTION NO: 3

When conducting computer forensic analysis, you must guard against _____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expecteD.

A. Hard Drive Failure

B. Scope Creep

C. Unauthorized expenses

D. Overzealous marketing

ANSWER: B

QUESTION NO: 4

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

ANSWER: A

QUESTION NO: 5

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

A. Statefull firewalls do not work with packet filtering firewalls

B. NAT does not work with statefull firewalls

C. NAT does not work with IPSEC

D. IPSEC does not work with packet filtering firewalls

ANSWER: C

QUESTION NO: 6

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162

B. 160

C. 161

D. 163

ANSWER: A C

QUESTION NO: 7

Software firewalls work at which layer of the OSI model?

A. Data Link

B. Network

C. Transport

D. Application

ANSWER: A

QUESTION NO: 8

E-mail logs contain which of the following information to help you in your investigation? (Select up to 4)

A. user account that was used to send the account

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

ANSWER: A C D E

QUESTION NO: 9

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

ANSWER: C

QUESTION NO: 10

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162

B. 160

C. 163

D. 161

ANSWER: A D

QUESTION NO: 11

In the context of file deletion process, which of the following statement holds true?

A. When files are deleted, the data is overwritten and the cluster marked as available

B. The longer a disk is inuse, the less likely it is that deleted files will be overwritten

C. While booting, the machine may create temporary files that can delete evidence

D. Secure delete programs work by completely overwriting the file in one go

ANSWER: C D

QUESTION NO: 12

This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

A. Master Boot Record (MBR)

B. Master File Table (MFT)

C. File Allocation Table (FAT)

D. Disk Operating System (DOS)

ANSWER: C