DUMPSARENA

EC-Council Certified Security Analyst (ECSA)

ECCouncil EC0-479

Version Demo

Total Demo Questions: 12

Total Premium Questions: 231

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.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

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: 2

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: 3

When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts _____ in the first letter position of the filename in the FAT database.

A. A Capital X

B. A Blank Space

C. The Underscore Symbol

D. The lowercase Greek Letter Sigma (s)

ANSWER: D

QUESTION NO: 4

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: 5

What is a good security method to prevent unauthorized users from "tailgating"?

A. Electronic key systems

B. Man trap

C. Pick-resistant locks

D. Electronic combination locks

ANSWER: B

QUESTION NO: 6

A law enforcement officer may only search for and seize criminal evidence with _____, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searcheD.

A. Mere Suspicion

B. A preponderance of the evidence

C. Probable cause

D. Beyond a reasonable doubt

ANSWER: C

QUESTION NO: 7

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: 8

Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

A. network-based IDS systems (NIDS)

B. host-based IDS systems (HIDS)

C. anomaly detection

D. signature recognition

ANSWER: B

QUESTION NO: 9

You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have founD. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subjects computer. You inform the officer that you will not be able to comply with that request because doing so would:

A. Violate your contract

B. Cause network congestion

C. Make you an agent of law enforcement

D. Write information to the subjects hard drive

ANSWER: C

QUESTION NO: 10

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\LSA

B. %systemroot%\repair

C. %systemroot%\system32\drivers\etc

D. %systemroot%\system32\LSA

ANSWER: B

QUESTION NO: 11

What is the target host IP in the following command?

```
C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP
```

A. Firewalk does not scan target hosts

B. 172.16.28.95

C. This command is using FIN packets, which cannot scan target hosts

D. 10.10.150.1

ANSWER: B

QUESTION NO: 12

Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

A. 18 U.S.C. 1029 Possession of Access Devices

B. 18 U.S.C. 1030 Fraud and related activity in connection with computers

C. 18 U.S.1343 Fraud by wire, radio or television

D. 18 U.S.C. 1361 Injury to Government Property
E.18 U.S.C. 1362 Government communication systems
G.18 U.S.C. 1832 Trade Secrets Act

ANSWER: B