

DUMPS ARENA

EC Council Computer Hacking Forensic Investigator

EC Council EC0-349

Version Demo

Total Demo Questions: 10

Total Premium Questions: 304

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

- A. Closed
- B. Open
- C. Stealth
- D. Filtered

ANSWER: B**QUESTION NO: 2**

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

- 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: 3**

A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

- A. He should search in C:\Windows\System32\RECYCLED folder
- B. The Recycle Bin does not exist on the hard drive
- C. The files are hidden and he must use switch to view them
- D. Only FAT system contains RECYCLED folder and not NTFS

ANSWER: C

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? (Choose two.)

- A. 162
- B. 161
- C. 163
- D. 160

ANSWER: A B

QUESTION NO: 5

What does the superblock in Linux define?

- A. filesynames
- B. diskgeometr
- C. location of the firstinode
- D. available space

ANSWER: C

QUESTION NO: 6

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.

The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

- A. False negatives
- B. False positives
- C. True negatives

D. True positives

ANSWER: A

QUESTION NO: 7

What is one method of bypassing a system BIOS password?

- A. Removing the processor
- B. Removing the CMOS battery
- C. Remove all the system memory
- D. Login to Windows and disable the BIOS password

ANSWER: B

QUESTION NO: 8

While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

- A. Technical material related to forensics
- B. No particular field
- C. Judging the character of defendants/victims
- D. Legal issues

ANSWER: B

QUESTION NO: 9

What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

- A. A compressed file
- B. A Data stream file
- C. An encrypted file
- D. A reserved file

ANSWER: B

QUESTION NO: 10

What is the following command trying to accomplish?

- A.** Verify that UDP port 445 is open for the 192.168.0.0 network
- B.** Verify that TCP port 445 is open for the 192.168.0.0 network
- C.** Verify that NETBIOS is running for the 192.168.0.0 network
- D.** Verify that UDP port 445 is closed for the 192.168.0.0 network

ANSWER: A