

DUMPSQUEEN

ECCouncil Computer Hacking Forensic Investigator

ECCouncil EC0-349

Version Demo

Total Demo Questions: 10

Total Premium Questions: 304

Buy Premium PDF

<https://dumpsqueen.com>

support@dumpsqueen.com

dumpsqueen.com

QUESTION NO: 1

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

- A. RestrictAnonymous must be set to "10" for complete security
- B. RestrictAnonymous must be set to "3" for complete security
- C. RestrictAnonymous must be set to "2" for complete security
- D. There is no way to always prevent an anonymous null session from establishing

ANSWER: C

QUESTION NO: 2

Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

- A. Two
- B. One
- C. Three
- D. Four

ANSWER: A

QUESTION NO: 3

An Expert witness give an opinion if:

- A. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
- B. To define the issues of the case for determination by the finder of fact
- C. To stimulate discussion between the consulting expert and the expert witness

D. To deter the witness from expanding the scope of his or her investigation beyond the requirements of the case

ANSWER: A

QUESTION NO: 4

Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

- A. Block all internal MAC address from using SNMP
- B. Block access to UDP port 171
- C. Block access to TCP port 171
- D. Change the default community string names

ANSWER: D

QUESTION NO: 5

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghitech.net What will this search produce?

- A. All sites that ghttech.net links to
- B. All sites that link to ghttech.net
- C. All search engines that link to .net domains
- D. Sites that contain the code: link:www.ghitech.net

ANSWER: B

QUESTION NO: 6

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: 7

A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

- A. Searching for evidence themselves would not have any ill effects
- B. Searching could possibly crash the machine or device
- C. Searching creates cache files, which would hinder the investigation
- D. Searching can change date/time stamps

ANSWER: D

QUESTION NO: 8

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 proper destination?

- A. Root Internet servers
- B. Border Gateway Protocol
- C. Gateway of last resort
- D. Reverse DNS

ANSWER: C

QUESTION NO: 9

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: 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