EC0-349 Q&As

Computer Hacking Forensic Investigator

Pass EC-COUNCIL EC0-349 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/ec0-349.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

As a security analyst, you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The IP address of the employees\\' computers

B. Bank account numbers and the corresponding routing numbers

C. The employees network usernames and passwords

D. The MAC address of the employees\\' computers

Correct Answer: C

QUESTION 2

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 subject\\'s 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 subject\\'s hard drive

Correct Answer: C

QUESTION 3

Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

A. Use a system that has a dynamic addressing on the network

B. Use a system that is not directly interacting with the router

C. Use it on a system in an external DMZ in front of the firewall

D. It doesn\\'t matter as all replies are faked

Correct Answer: D

QUESTION 4

You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

A. The X509 Address

B. The SMTP reply Address

C. The E-mail Header

D. The Host Domain Name

Correct Answer: C

QUESTION 5

Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?

A. The data is still present until the original location of the file is used

B. The data is moved to the Restore directory and is kept there indefinitely

C. The data will reside in the L2 cache on a Windows computer until it is manually deleted

D. It is not possible to recover data that has been emptied from the Recycle Bin

Correct Answer: A