VCE & PDF
Pass4itSure.com

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

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

A. Civil litigation testimony

B. Expert testimony

C. Victim advocate testimony

D. Technical testimony

Correct Answer: D

QUESTION 2

During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?

A. C:\Program Files\Exchsrvr\servername.log

B. D:\Exchsrvr\Message Tracking\servername.log

C. C:\Exchsrvr\Message Tracking\servername.log

D. C:\Program Files\Microsoft Exchange\srvr\servername.log

Correct Answer: A

QUESTION 3

Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

A. Point-to-point

B. End-to-end

C. Thorough

D. Complete event analysis

Correct Answer: B

QUESTION 4

You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a

string within a file on the bitmap image of the target computer?

A. Stringsearch

B. grep

C. dir

D. vim

Correct Answer: B

QUESTION 5

During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complaint with Police?

A. Yes, and all evidence can be turned over to the police

B. Yes, but only if you turn the evidence over to a federal law enforcement agency

C. No, because the investigation was conducted without following standard police procedures

D. No, because the investigation was conducted without warrant

Correct Answer: A

QUESTION 6

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

Correct Answer: C

QUESTION 7

Jason is the security administrator of ACMA metal Corporation. One day he notices the company\\'s Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.

Which organization coordinates computer crimes investigations throughout the United States?

A. Internet Fraud Complaint Center

B. Local or national office of the U.S. Secret Service

C. National Infrastructure Protection Center

D. CERT Coordination Center

Correct Answer: B

QUESTION 8

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. ATM

B. UDP

C. BPG

D. OSPF

Correct Answer: D

QUESTION 9

An Employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the Employees Computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the Employee before he leaves the building and recover the floppy disks and secure his computer. Will you be able to break the encryption so that you can verify that that the employee was in possession of the proprietary information?

A. EFS uses a 128-bit key that can\\'t be cracked, so you will not be able to recover the information

B. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information.

C. The EFS Revoked Key Agent can be used on the Computer to recover the information

D. When the Encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information.

Correct Answer: B

QUESTION 10

Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

A. Sector

B. Metadata

C. MFT

D. Slack Space

Correct Answer: D

QUESTION 11

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Packet filtering firewall

B. Circuit-level proxy firewall

C. Application-level proxy firewall

D. Stateful firewall

Correct Answer: D

QUESTION 12

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records

B. Enumerate MX and A records from DNS

C. Establish a remote connection to the Domain Controller

D. Enumerate domain user accounts and built-in groups

Correct Answer: D

QUESTION 13

How many sectors will a 125 KB file use in a FAT32 file system?

A. 32

B. 16

C. 256

D. 25

Correct Answer: C

QUESTION 14

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"

B. intitle:"exchange server"

C. locate:"logon page"

D. outlook:"search"

Correct Answer: A

QUESTION 15

Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Entrapment

B. Enticement

C. Intruding into a honeypot is not illegal

D. Intruding into a DMZ is not illegal

Correct Answer: A

[EC0-349 PDF Dumps](#)   [EC0-349 VCE Dumps](#)   [EC0-349 Study Guide](#)