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.leads4pass.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

You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.

What method would be most efficient for you to acquire digital evidence from this network?

A. create a compressed copy of the file with DoubleSpace

B. create a sparse data copy of a folder or file

C. make a bit-stream disk-to-image file

D. make a bit-stream disk-to-disk file

Correct Answer: C

QUESTION 2

Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri\\'s duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company\\'s switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Terri\\'s computer

B. Poison the switch\\'s MAC address table by flooding it with ACK bits

C. Crash the switch with a DoS attack since switches cannot send ACK bits

D. Enable tunneling feature on the switch

Correct Answer: A

QUESTION 3

Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused. In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

A. Grill cipher

B. Null cipher

C. Text semagram

D. Visual semagram

Correct Answer: A

QUESTION 4

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Linux/Unix computers are easier to compromise

B. Linux/Unix computers are constantly talking

C. Windows computers are constantly talking

D. Windows computers will not respond to idle scans

Correct Answer: C

QUESTION 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.ghttech.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.ghttech.net

Correct Answer: B

QUESTION 6

Law enforcement officers are conducting a legal search for which a valid warrant was obtained.

While conducting the search, officers observe an item of evidence for an unrelated crime that was not

included in the warrant. The item was clearly visible to the officers and immediately identified as evidence.

What is the term used to describe how this evidence is admissible?

A. Plain view doctrine

B. Corpus delicti

C. Locard Exchange Principle

D. Ex Parte Order

Correct Answer: A

QUESTION 7

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 form expanding the scope of his or her investigation beyond the requirements of the case

Correct Answer: A

QUESTION 8

What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?

A. forensic duplication of hard drive

B. analysis of volatile data

C. comparison of MD5 checksums

D. review of SIDs in the Registry

Correct Answer: C

QUESTION 9

In a FAT32 system, a 123 KB file will use how many sectors?

A. 34

B. 25

C. 11

D. 56

Correct Answer: B

QUESTION 10

During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the

investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore, you report this evidence. This type of evidence is known as:

A. Inculpatory evidence

B. Mandatory evidence

C. Exculpatory evidence

D. Terrible evidence

Correct Answer: C

QUESTION 11

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A. The registry

B. The swap file

C. The recycle bin

D. The metadata

Correct Answer: B

QUESTION 12

Using Linux to carry out a forensics investigation, what would the following command accomplish? dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror

A. Search for disk errors within an image file

B. Backup a disk to an image file

C. Copy a partition to an image file

D. Restore a disk from an image file

Correct Answer: D

QUESTION 13

What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

A. Cracks every password in 10 minutes

B. Distribute processing over 16 or fewer computers

C. Support for Encrypted File System

D. Support for MD5 hash verification

Correct Answer: B

QUESTION 14

You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?

A. trademark law

B. copyright law

C. printright law

D. brandmark law

Correct Answer: A

QUESTION 15

Which response organization tracks hoaxes as well as viruses?

A. NIPC

B. FEDCIRC

C. CERT

D. CIAC

Correct Answer: D

[Latest EC0-349 Dumps](https://www.leads4pass.com/ec0-349.html)   [EC0-349 PDF Dumps](https://www.leads4pass.com/ec0-349.html)   [EC0-349 Braindumps](https://www.leads4pass.com/ec0-349.html)