EC1-349^{Q&As}

EC1-349^{Q&As}

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee

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

https://www.passapply.com/ec1-349.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

Which one of the following is not a consideration in a forensic readiness planning checklist?

A. Define the business states that need digital evidence

B. Identify the potential evidence available

C. Decide the procedure for securely collecting the evidence that meets the requirement fn a forensically sound manner

D. Take permission from all employees of the organization

Correct Answer: D

QUESTION 2

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 "2" for complete security

B. There is no way to always prevent an anonymous null session from establishing

C. RestrictAnonymous must be set to "10" for complete security

D. RestrictAnonymous must be set to "3" for complete security

Correct Answer: A

QUESTION 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 themThe files are hidden and he must use ? switch to view them

D. Only FAT system contains RECYCLED folder and not NTFS

Correct Answer: C

QUESTION 4

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

A. one who has NTFS 4 or 5 partitions

B. one who uses dynamic swap file capability

C. one who uses hard disk writes on IRQ 13 and 21

D. one who has lots of allocation units per block or cluster

Correct Answer: D

QUESTION 5

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company\\'s main office in Iowa. She states that she needs the receptionist\\'s network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, reQuested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Social Validation

B. Friendship/Liking

C. Reciprocation

D. Scarcity

Correct Answer: C