Vendor:EC-COUNCIL

Exam Code:312-49V10

Exam Name:ECCouncil Computer Hacking Forensic Investigator (V10)

Version: Demo

QUESTION 1

In an echo data hiding technique, the secret message is embedded into a _____as an echo.

A. Cover audio signal

B. Phase spectrum of a digital signal

C. Pseudo-random signal

D. Pseudo- spectrum signal

Correct Answer: A

QUESTION 2

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. Copyright law

B. Brandmark law

C. Trademark law

D. Printright law

Correct Answer: C

QUESTION 3

Area density refers to:

A. the amount of data per disk

B. the amount of data per partition

C. the amount of data per square inch

D. the amount of data per platter

Correct Answer: AC

QUESTION 4

What is the capacity of Recycle bin in a system running on Windows Vista?

A. 2.99GB

B. 3.99GB

C. Unlimited

D. 10% of the partition space

Correct Answer: C

QUESTION 5

Buffer Overflow occurs when an application writes more data to a block of memory, or buffer, than the buffer is allocated to hold. Buffer overflow attacks allow an attacker to modify the _____in order to control the process execution, crash the process and modify internal variables.

A. Target process\\'s address space

B. Target remote access

C. Target rainbow table

D. Target SAM file

Correct Answer: A

QUESTION 6

Identify the file system that uses $BitMap file to keep track of all used and unused clusters on a volume.

A. NTFS

B. FAT

C. EXT

D. FAT32

Correct Answer: A

QUESTION 7

Computer security logs contain information about the events occurring within an organization\\'s systems and networks. Application and Web server log files are useful in detecting web attacks. The source, nature, and time of the attack can be determined by _____of the compromised system.

A. Analyzing log files

B. Analyzing SAM file

C. Analyzing rainbow tables

D. Analyzing hard disk boot records

Correct Answer: A

QUESTION 8

NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DDR). Which of the following is not a part of DDF?

A. Encrypted FEK

B. Checksum

C. EFS Certificate Hash

D. Container Name

Correct Answer: B

QUESTION 9

Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

A. SWGDE and SWGIT

B. Daubert

C. Frye

D. IOCE

Correct Answer: C

QUESTION 10

One way to identify the presence of hidden partitions on a suspect hard drive is to:One way to identify the presence of hidden partitions on a suspect? hard drive is to:

A. Add up the total size of all known partitions and compare it to the total size of the hard drive

B. Examine the FAT and identify hidden partitions by noting an ?in the artition Type?fieldExamine the FAT and identify hidden partitions by noting an ??in the ?artition Type?field

C. Examine the LILO and note an ?in the artition Type?fieldExamine the LILO and note an ??in the ? artition Type?field It is not possible to have hidden partitions on a hard drive

Correct Answer: A

QUESTION 11

You are working as an independent computer forensics investigator and receive a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a implePC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a ?imple backup copy?of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a imple backup copy?will not provide deleted files or recover file fragments. What type of copy do you need to make toYou inform him that a ?imple backup copy?will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings?

A. Bit-stream copy

B. Robust copy

C. Full backup copy

D. Incremental backup copy

Correct Answer: A

QUESTION 12

Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_CONFIG

C. HKEY_LOCAL_MACHINE

D. HKEY_USERS

Correct Answer: A