Vendor: EC-Council

Exam Code: 312-49

Exam Name: Computer Hacking Forensic Investigator (CHFI)

Version: DEMO

1.When an investigator contacts by telephone the domain administrator or controller listed by a whois lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?
A. Title 18, Section 1030
B. Title 18, Section 2703(d)
C. Title 18, Section Chapter 90
D. Title 18, Section 2703(f)
Answer: D

2.If you come across a sheepdip machine at your client site, what would you infer?
A. A sheepdip coordinates several honeypots
B. A sheepdip computer is another name for a honeypot
C. A sheepdip computer is used only for virus-checking.
D. A sheepdip computer defers a denial of service attack
Answer: C

3.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
Answer: C

4.How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?
A. 128
B. 64
C. 32
D. 16
Answer: C

5.What does the superblock in Linux define?
A. file system names
B. available space
C. location of the first inode
D. disk geometry
Answer: B, C, D

6.A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker . Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt. (Note: The student is being tested on concepts learnt during passive OS fingerprinting,

basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111

TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF

A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32

TCP Options (3) => NOP NOP TS: 23678634 2878772

=+=

03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111

UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84

Len: 64

01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 ....

00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....

00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....

00 00 00 11 00 00 00 00 ....

=+=

03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773

UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104

Len: 1084

47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8 G..c............

00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 20 ....

3A B1 5E E5 00 00 00 09 6C 6F 63 61 6C 68 6F 73 :.^.....localhost

=+=

+

03/15-20:21:36.539731 211.185.125.124:4450 -> 172.16.1.108:39168

TCP TTL:43 TOS:0x0 ID:31660 IpLen:20 DgmLen:71 DF

AP Seq: 0x9C6D2BFF Ack: 0x59606333 Win: 0x7D78 TcpLen: 32

TCP Options (3) => NOP NOP TS: 23679878 2880015

63 64 20 2F 3B 20 75 6E 61 6D 65 20 2D 61 3B 20 cd /; uname -a;

69 64 3B id;

A. The attacker has conducted a network sweep on port 111

B. The attacker has scanned and exploited the system using Buffer Overflow

C. The attacker has used a Trojan on port 32773

D. The attacker has installed a backdoor

Answer: A

7.The newer Macintosh Operating System is based on:

A. OS/2

B. BSD Unix

C. Linux

D. Microsoft Windows

Answer: B

8.Before you are called to testify as an expert, what must an attorney do first?

A. engage in damage control
B. prove that the tools you used to conduct your examination are perfect
C. read your curriculum vitae to the jury
D. qualify you as an expert witness
Answer: D

9.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 fileC
D. make a bit-stream disk-to-disk file
Answer: C

10.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
Answer: A

11.What file structure database would you expect to find on floppy disks?
A. NTFS
B. FAT32
C. FAT16
D. FAT12
Answer: D

12.What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?
A. digital attack
B. denial of service
C. physical attack

D. ARP redirect
Answer: B

13.When examining a file with a Hex Editor, what space does the file header occupy?
A. the last several bytes of the file
B. the first several bytes of the file
C. none, file headers are contained in the FAT
D. one byte at the beginning of the file
Answer: D

14.In the context of file deletion process, which of the following statement holds true?
A. When files are deleted, the data is overwritten and the cluster marked as available
B. The longer a disk is in use, the less likely it is that deleted files will be overwritten
C. While booting, the machine may create temporary files that can delete evidence
D. Secure delete programs work by completely overwriting the file in one go
Answer: C

15.A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.
A. Image the disk and try to recover deleted files
B. Seek the help of co-workers who are eye-witnesses
C. Check the Windows registry for connection data (You may or may not recover)
D. Approach the websites for evidence
Answer: A

16.A(n) _____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.
A. blackout attack
B. automated attack
C. distributed attack
D. central processing attack
Answer: B

17.The offset in a hexadecimal code is:
A. The last byte after the colon
B. The 0x at the beginning of the code
C. The 0x at the end of the code
D. The first byte after the colon
Answer: B

18.It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

A. by law, three

B. quite a few

C. only one

D. at least two

Answer: C

19.With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches _____.

A. 0

B. 10

C. 100

D. 1

Answer: A

20.When examining the log files from a Windows IIS Web Server, how often is a new log file created?

A. the same log is used at all times

B. a new log file is created everyday

C. a new log file is created each week

D. a new log is created each time the Web Server is started

Answer: A