Certified Ethical Hacker

ECCouncil 312-49 Dumps Available Here at:

https://www.certification-questions.com/eccouncil-exam/312-49-dumps.html

Enrolling now you will get access to 316 questions in a unique set of 312-49 dumps

Question 1

When an investigator contacts by telephone the domain administrator or controller listed by a Who is 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?

Options:

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

Question 2

Item 2If you come across a sheepdip machine at your client site, what would you infer?

Options:

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

Question 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?

Options:

A. rules of evidence

B. law of probability

C. chain of custody

D. policy of separation

Answer: C

Question 4

How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

Options:

A. 128

B. 64

C. 32

D. 16

Answer: C

Question 5

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML,
DHTML, and other web-based languages and how they have evolved over the years.
You navigate to archive. org and view the HTML code of news.com. You then navigate to the current news.com
website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

Options:

A. Web bug

B. CGI code

C. Trojan.downloader

D. Blind bug

Answer: A

Question 6

You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the
primary hard drive. Which of the following formats correctly specifies these sectors?

Options:

A. 0:1000, 150

B. 0:1709, 150

C. 1:1709, 150

D. 0:1709-1858

Answer: B

Question 7

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
```

Options:

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

Question 8

The newer Macintosh Operating System is based on:

Options:

A. OS/2

B. BSD Unix

C. Linux

D. Microsoft Windows

Answer: B

Question 9

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

Options:

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

Question 10

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?

Options:

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

Answer: C