Computer Hacking Forensic Investigator

1. Topic #: 1
During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

A. A. Rule 1003: Admissibility of Duplicates

B. B. Limited admissibility

C. C. Locard’s Principle

D. D. Hearsay

Answer(s): D

---

2. Question #: 358
Topic #: 1
Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

A. A. Windows 98

B. B. Linux

C. C. Windows 8.1

D. D. Windows XP

Answer(s): C

---

3. Question #: 117
Topic #: 1
You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case.
How would you permanently erase the data on the hard disk?

A. A. Throw the hard disk into the fire

B. B. Run the powerful magnets over the hard disk

C. C. Format the hard disk multiple times using a low level disk utility

D. D. Overwrite the contents of the hard disk with Junk data

Answer(s): A

---

4. Question #: 714
Topic #: 1
A cybersecurity investigator is working on a case involving a malicious executable suspected of being packed using a popular program packer. The investigator realizes that the packer used is password-protected. In such a scenario, what should be the investigator’s first course of action to analyze the packed file?

A. A. Mount compound files

B. B. Perform static analysis on the packed file

C. C. Decrypt the password to unpack the file

D. D. Run the packed file in a controlled environment for dynamic analysis

Answer(s): A

---

5. Question #: 295
Topic #: 1
Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?

A. A. Spycrack

B. B. Spynet

C. C. Netspionage

D. D. Hackspionage

Answer(s): C

---

6. Question #: 289
Topic #: 1
When operating systems mark a cluster as used but not allocated, the cluster is considered as __________

A. A. Corrupt

B. B. Bad

C. C. Lost

D. D. Unallocated

Answer(s): C

---

7. Question #: 268
Topic #: 1
Where are files temporarily written in Unix when printing?

A. A. /usr/spool

B. B. /var/print

C. C. /spool

D. D. /var/spool

Answer(s): D

---

8. Question #: 267

Topic #: 1

Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

A. A. Network

B. B. Transport

C. C. Physical

D. D. Data Link

Answer(s): C

---

9. Question #: 253

Topic #: 1

What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

A. A. NTOSKRNL.EXE

B. B. NTLDR

C. C. LSASS.EXE

D. D. NTDETECT.COM

Answer(s): A

---

10. Question #: 233

Topic #: 1

What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

A. A. hda

B. B. hdd

C. C. hdb

D. D. hdc

Answer(s): B

---

11. Question #: 229
Topic #: 1
Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?
22,164 cylinders/disk
80 heads/cylinder
63 sectors/track

A. A. 53.26 GB

B. B. 57.19 GB

C. C. 11.17 GB

D. D. 10 GB

Answer(s): A

---

12. Question #: 225
Topic #: 1
What is the smallest physical storage unit on a hard drive?

A. A. Track

B. B. Cluster

C. C. Sector

D. D. Platter

Answer(s): C

13. Question #: 204

Topic #: 1

How many possible sequence number combinations are there in TCP/IP protocol?

A. A. 1 billion

B. B. 320 billion

C. C. 4 billion

D. D. 32 million

Answer(s): B

14. Question #: 200

Topic #: 1

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. A. Only IBM AS/400 will reply to this scan

B. B. Only Windows systems will reply to this scan

C. C. A switched network will not respond to packets sent to the broadcast address

D. D. Only Unix and Unix-like systems will reply to this scan

Answer(s): C

15. Question #: 198

Topic #: 1

What does ICMP Type 3/Code 13 mean?

A. A. Host Unreachable

B. B. Administratively Blocked

C. C. Port Unreachable

D. D. Protocol Unreachable

Answer(s): B

---

16. Question #: 191
Topic #: 1
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. A. Polymorphic

B. B. Metamorphic

C. C. Oligomorhic

D. D. Transmorphic

Answer(s): A

---

17. Question #: 148
Topic #: 1
An “idle” system is also referred to as what?

A. A. PC not connected to the Internet

B. B. Zombie

C. C. PC not being used

D. D. Bot

Answer(s): C

---

18. Question #: 141
Topic #: 1
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using
Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. A. Closed

B. B. Open

C. C. Stealth

D. D. Filtered

Answer(s): B

---

19. Question #: 135
Topic #: 1
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. A. Passive IDS

B. B. Active IDS

C. C. Progressive IDS

D. D. NIPS

Answer(s): B

---

20. Question #: 59

Topic #: 1

Why should you note all cable connections for a computer you want to seize as evidence?

A. A. to know what outside connections existed

B. B. in case other devices were connected

C. C. to know what peripheral devices exist

D. D. to know what hardware existed

Answer(s): C
