Vendor: IISFA

Exam Code: II0-001

Exam Name: Certified Information Forensics Investigator (CIFI)

Version: DEMO

QUESTION 1
In order to prevent footprinting of an environment, one method that is effective is:

A. Footprint shunting
B. Network address translation at a perimeter security device
C. ISPs monitoring and filtering footprinting activity
D. None of the above

Answer: B

QUESTION 2
Because of overlapping security domains, it is impossible to have two perimeter security devices (firewalls) in successive layers.

A. True
B. False

Answer: B

QUESTION 3
The "Stealth Rule" in a perimeter security device prevents it from being footprinted.

A. True
B. False

Answer: A

QUESTION 4
If a file is properly encrypted, it can not be read except by the file owner.

A. True
B. False

Answer: B

QUESTION 5
When electronic evidence has been encrypted, the best method of discovery is:

A. Brute force to compromise the encryption.
B. Attempt to brute force the key.
C. Use a reverse MD5 Hash utility.
D. You can not break contemporary encryption techniques.

Answer: B

QUESTION 6
What method can be used to detect the use of rogue servers providing services such as illegal software distribution, music files, pornography in an environment?

A. A network protocol sniffer/analyzer
B. Keymapping on all workstations in the environment
C. Port 4090 listening
D. Port 4099 listening

Answer: A

QUESTION 7
How many port/services are available using the TCP/IP suite?

A. 6,553
B. unlimited
C. 65,535
D. 65,353

Answer: C

QUESTION 8
A rule that allows any traffic from the trusted network through to untrusted networks is a security risk because:

A. It will allow a trojan program within the trusted network to operate.
B. The firewall will perform poorly and violate the Availability principle of information security.
C. Trusted networks should always be treated the same as untrusted networks.
D. This is not a security risk.

Answer: A

QUESTION 9
For many ISPs, placing a network protocol sniffer in their infrastructure allows them to be very effective in support law enforcement during an investigation.

A. True
B. False

Answer: B

QUESTION 10
A syslog server and a protocol sniffer perform the same basic function.

A. True
B. False

Answer: B

QUESTION 11
When investigating a malicious attack sourced from the Internet, the investigator would look for

forensic evidence in:

A. The point of entry firewall log
B. The application logs of the target system
C. The IDS log
D. All of the above

Answer: D

QUESTION 12
During a brute force attack, an active trace may be initiated using what tool?

A. Firewall log
B. ARP
C. Traceroute
D. ARP/Traceroute

Answer: A

QUESTION 13
Many malicious attacks are sourced to ISP dial up accounts, what makes this type of attack source a challenge for an investigator?

A. Because ISPs refuse to cooperate with investigations
B. Dial up accounts are too slow for effective countermeasures.
C. Dial up accounts typically have dynamic IP addresses
D. Dial up use SLIP not TCP/IP protocol

Answer: C

QUESTION 14
A "listening post" usually refers to:

A. A sound recording device using in physical security.
B. Video/audio devices used to record an investigation.
C. Eavesdropping on electronic communications
D. An IDS point of presence.

Answer: D

QUESTION 15
During an incident, an incident response team springs into action. What is one of the first steps the team will take?

A. Contact local law enforcement
B. Triage of the incident
C. Determine the source of the attack
D. Determine the target of the attack

Answer: B

QUESTION 16
As a private investigator, you are not required to report most crimes discovered during your investigation unless the crime is in the planning stages, is child exploitation, or issues of national security.

A. True
B. False

Answer: A

QUESTION 17
The common practices of legal requirements of record retention is dependant upon the type of information.

A. True
B. False

Answer: A

QUESTION 18
When a hard drive is formatted. (other than partition table, boot record, root directory and other system areas) what character would be found over the entire disk

A. Hex E5
B. Hex F6
C. Hex F8
D. Indeterminable

Answer: D

QUESTION 19
What is the currently accepted hashing algorithm used for digital signature standard (DSS) based on NIST documentation

A. 32 Bit CRC
B. 128 Bit MD5
C. 160 Bit SHA-1
D. 256 Bit SHA-2

Answer: C