IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **II0-001**

Title : Certified Information Forensics Investigator(CIFI)

Version : DEMO

1.Firewalls are an excellent source of:
A. Details of system usage
B. Details of protocol usage
C. Forensic Evidence for malicious attacks
D. Port/service mappings
Answer: C

2 .What technique of layered security design will allow for both investigation and recovery after an incident?
A. RI Technology
B. Highly available systems
C. Overlap design approach
D. Honeypot placement
Answer: B

3 .If a CIFI violates the ISFA code of Ethics, her CIFI certification can be immediately revoked.
A. True
B. False
Answer: B

4 .The 1st amendment allows hackers to exercise free speech by altering content on websites to express opposing viewpoints.
A. True
B. False
Answer: B

5 .The term "Browser Artifacts" refer to:
A. Web browser cache, cookies, favorites, history, auto complete information
B. Older web browser applications that have little or no security and allow for unchecked use
C. Older web browser applications that can be used as a surveillance tool for investigators due to their lack of security
D. Web browser cookies
Answer: A

6 .All of the following are methods of auditing except:
A. Internal audit
B. External audit
C. Thorough audit
D. 3rd party audit
Answer: C

7 .In selecting Forensic tools for collecting evidence in the investigation of a crime the

standard for authenticating computer records is:
A. The same for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form.
B. Much more complex, and requires an expert to be present at each step of the process.
C. To convert the technical terms & definitions into a basic understandable language to be presented as evidence.
D. To ensure the tools are equipped with logging to document the steps of evidence collection.
Answer: C

8 ."Interesting data" is:
A. Data relevant to your investigation
B. Pornography
C. Documents, spreadsheets, and databases
D. Schematics or other economic based information
Answer: A

9 .Social engineer is legal in the United States, Great Britain, Canada, and Australia as long as the social engineer does not:
A. Attempt to extract corporate secrets
B. Lie
C. Apply the Frye Scenario
D. Live outside those countries
Answer: A

10.Drive geometry refers to
A. The algorithms used to computer a specific location of a particular segment.
B. The functional dimensions of a drive in terms of the number of heads, cylinders, and sectors per track.
C. Physical dimensions of the drive platters.
D. The depth of the pits on optical media or magnetic field charge on magnetic media
Answer: B

11 .Which of the following are characteristics of electronic Evidence?
A. Cannot be easily altered
B. Is not time sensitive
C. Should follow proper chain of custody
D. Must be decrypted
Answer: C

12 .Embedding a serial number or watermark into a data file is known as:
A. Hashing
B. Steganography

C. Message Digest
D. Imprinting
Answer: B

13 .What is the difference between a zombie host and a reflector host?
A. Unlike a zombie, a reflector is a laundering host that fundamentally transforms and/or delays the attacker's communications before they continue down the attack path. (Zombie technique)
B. Unlike a zombie, a Traceback through the stepping stone host requires determining if two communications streams, viewed at different points in the network, have the same origin and are essentially the same stream. (stepping stone Traceback technique)
C. Unlike a zombie host, the reflector is an uncompromised host that cooperates with the attack in an innocent manner consistent with its normal function.
D. A zombie is a version of a reflector host.
Answer: C

14 .The major disadvantage to techniques that attempt to mark IP packets as they move through the internet is:
A. A decrease in network efficiency
B. An increase in the packet load
C. An increase in bandwidth consumption
D. All of the above
Answer: C

15 .In normal operation, a host receiving packets can determine their source by direct examination of the source address field in the:
A. The IP packet header
B. Source code
C. Audit logs
D. Intrusion Detection System
Answer: A

16 .One caution an investigator should take when examining the source of a network attack is:
A. an occurrence of Social Engineering
B. relaxed physical security
C. the source IP address may have been spoofed
D. a sniffer could be on the network
Answer: C

17 .Stream comparison used as a Traceback technique focuses on what two factors?
A. the IP address and victim port
B. the packet contents and audit logs

C. inter-packet timing and the victim port
D. the packet contents and inter-packet timing
Answer: D

18 .To perform a successful traceback, the two most prominent problems that need to be solved are locating the source of IP packets and:
A. the timestamp of the event
B. determining the first node of a connection chain
C. the reflector host
D. the victim port
Answer: B

19 .The most important network information that should be observed from the logs during a Traceback is the intruder IP address, the victim IP address, the victim port, protocol information and the:
A. source port
B. operating system
C. MAC address
D. timestamp
Answer: D

20 .A new protocol that is designed to aid in intrusion protection and IP tracebacks is known as:
A. Intruder Detection and Isolation Protocol (IDIP)
B. Intrusion Detection and Traceback Protocol (IDTP)
C. Facilitating Traceback Protocol (FTP)
D. Intruder Detection and Internet Protocol (IDIP)
Answer: A