Information Security

SET-8

By

BHARAT BHUSHAN @ B. K. NAL
Assistant Professor (Computer Science)
Director, BSTI, Kokar

&

SUPRIYA BHARATI
Assistant Professor (Computer Science)
Asst. Director, BSTI, Kokar

Buddha Science and Technical Institute (BSTI), Kokar
www.bharatsir.com

1. Forensic analysis involves the following :

A. assessment, experimentation, fusion, correlation, and validation
B. seizure and preservation
C. seizure and preservation
D. all of the above

2. An investigation can be hindered by the following:

A. preconceived theories
B. improperly handled evidence
C. offender concealment behavior
D. all of the above

3. The fact that with modern technology, a photocopy of a document has become acceptable in place of the original is known as:

A. best evidence rule
B. due diligence
C. quid pro quo
D. voir dire

4. When assessing the reliability of digital evidence, the investigator is concerned with whether the computer that generated the evidence was functioning normally, and:

A. whether chain of custody was maintained
B. whether there are indications that the actual digital evidence was tampered with
C. whether the evidence was properly secured in transit
D. whether the evidence media was compatible with forensic machines

5. The process of documenting the seizure of digital evidence and, in particular, when that evidence changes hands, is known as:

A. chain of custody
B. field notes
C. interim report
D. none of the above

6. The following specializations exist in digital investigations :

A. first responder (a.k.a. digital crime scene technician)
B. forensic examiner
C. digital investigator
D. all of the above

7. Computers can play the following roles in a crime:

A. target, object, and subject
B. evidence, instrumentality, contraband, or fruit of crime
C. object, evidence, and tool
D. Symbol ,instrumentality, and source of evidence

8. Personal computers and networks are often a valuable source of evidence. Those involved with _____should be comfortable with this technology.

A. criminal investigation
B. prosecution
C. defense work
D. all of the above

9. Cyber trails are advantageous because:

A. they are not connected to the physical world.
B. nobody can be harmed by crime on the internet.
C. they are easy to follow.
D. offenders who are unaware of them leave behind more clues than they otherwise would have.

10. In terms of digital evidence, the Internet is an example of :

A. open computer systems
B. communication systems
C. embedded computer systems
D. none of the above

11. What are the three general categories of computer systems that can contain digital evidence?

A. desktop, laptop, server
B. personal computer, internet, mobile telephone
C. hardware, software, networks
D. open computer systems, communication systems, embedded systems

12. A valid definition of digital evidence is:

A. none of the below
B. data stored or transmitted using a computer
C. digital data of probative value
D. any digital evidence on a computer

13. Which is true of a signature-based IDS?

A. it cannot work with an ips
B. it only identifies on known signatures

C. it detects never-before-seen anomalies
D. it works best in large enterprises.

14. When discussing IDS/IPS, what is a signature?

A. an electronic signature used to authenticate the identity of a user on the network
B. patterns of activity or code corresponding to attacks
C. "normal," baseline network behavior
D. none of the above

15. A full domain name is sequence of lables separated by_____.

A. Semicolons
B. Dots
C. Colons
D. none

16. The root of DNS tree is_____.

A. a string of characters
B. a string of 63 characters
C. an empty string
D. none

17. In the DNS the names are defined in ___ structure.

A. a linear list
B. an invertred tree
C. a graph
D. None

18. DNS can use services of_____using the well known port 53.

A. Udp
B. Tcp

C. either (a) or (b**)**

D. none of the above

19. The _____domains define registered hosts according to their generic behavior.

A. generic

B. country

C. inverse

D. none

20. The domain name space (tree) is divided into_____ different sections.

A. 3

B. 2

C. 4

D. none

21. Why would HTTP Tunneling be used?

A. to identify proxy servers

B. web activity is not scanned

C. to bypass a firewall

D. http is a easy protocol to work with

22. What is the most important activity in system hacking?

A. information gathering

B. cracking passwords

C. escalating privileges

D. covering tracks

23. SSL stands for?

A. secured socket layer

B. secured shell layer

C. system socket layer

D. system secured layer

24. What is Firewall?

A. firewalls are network based security measures that control the flow of incoming and outgoing traffic
B. firewall is a program that encrypts all programs that access the internet
C. a firewall is a program that keeps other programs from using the internet
D. firewall are the interrupts that automatically disconnect from the internet when a threat appears.

25. Why would a hacker use a proxy server?

A. to create a stronger connection with the target.
B. to create a ghost server on the network.
C. to obtain a remote access connection
D. to hide malicious activity on the network

ANSWER						
1.	A		11.	D	21.	C
2.	D		12.	C	22.	B
3.	A		13.	B	23.	A
4.	B		14.	B	24.	A
5.	A		15.	B	25.	D
6.	D		16.	C		
7.	B		17.	B		
8.	D		18.	C		
9.	D		19.	A		
10.	B		20.	A		