Information Security

SET-7

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. Which One of them is Passive attack?

A. denial of service
B. modify message in transit
C. replay previous message
D. obtain message contain

2. Protection against Denial by one of these parties in a communication refers to?

A. non-repudiation
B. data integrity
C. authentication
D. none of these

3. Prevention of the unauthorized used of Resources refers too?

A. data integrity
B. data confidentiality
C. access control
D. none of these

4. __________ means knowledge obtained from investigation, study , intelligence new ,facts .

A. Security
B. Data
C. Information
D. none of these

5. Security Measures Needed to protect ________ during their transmission.

A. File
B. Data
C. Packet
D. all of above

6. In the course of conducting forensic analysis, which of following actions are carried out ?

A. critical thinking
B. fusion
C. validation
D. all of the above

7. Computers and mobile devices are treated as _______crime scenes in violent crime investigations.

A. Temporary
B. Immediate
C. Remote
D. secondary

8. When reconstructing evidence surrounding a crime, it is generally helpful to:

A. lay out all the evidence so it can be viewed in its entirety
B. work with the crime scene technicians so that a better understanding of the crime is achieved
C. construct a timeline of events from digital evidence
D. begin the process of converting field notes to a final report

9. When you have developed a theory, what can you do to confirm that your hypothesis is correct?

A. predict, based on your hypothesis, where artifacts should be located
B. perform experiments to test results and rule out alternate explanations

C. conclude, based on your findings, whether the evidence supports the hypothesis
D. all of the above

10. The _______ documentation specifies who handled the evidence, when, where, and for what purpose.

A. evidence inventory
B. chain of custody
C. evidence intake
D. preservation notes

11. That part of cyber stalking where the offender is using the Internet to find a victim is known as:

A. Profiling
B. Trolling
C. surreptitious monitoring
D. none of the above

12. When a cyber stalking case is stalled, it is a good idea to interview the victim again, because:

A. the victim might have been withholding information during the first interview.
B. the information that investigators have gathered might help the victim recall additional details.
C. the time between the first and second interviews has given the victim time to seek counseling.
D. none of the above

13. An implication from studies indicating that many stalkers had prior acquaintance with their victims is that:

A. part of the blame can be assigned to the victim.
B. the offender is likely to be found in the same area as the victim
C. investigators should pay particular attention to acquaintances of the victim
D. investigators should always check the immediate family

14. In confirming an alibi involving an obscure piece of equipment, if no documentation is available, the manufacturer is no longer in business, or the equipment/network is so complicated that nobody fully understands how it works, you should:

A. state that the alibi is considered unproven
B. search the internet for any pertinent information
C. recreate the events surrounding the alibi
D. contact other investigators and average their opinions

15. To demonstrate that someone is lying about an alibi, it is necessary to:

A. find evidence that clearly demonstrates the lie
B. require the suspect to submit to a polygraph
C. interrogate the suspect using a number of methods
D. show that no evidence confirming the alibi is available

16. Types of digital evidence that might corroborate an alibi include:

A. evidence of computer usage when the offense was supposed to occurred

B. computer records from credit cards, the telephone company, or subway ticket usage

C. gps information from mobile devices indicating the user's location and time

D. all of the above

17. It is quite difficult to fabricate an alibi on a network successfully because:

A. an offender may not have the proper access.

B. an offender would need system administrator access level to make the necessary changes.

C. an individual rarely has the ability to falsify digital evidence on all the computers that are involved.

D. creating an alibi on a network could take months of work.

18. Investigators should not rely on one piece of digital evidence when examining an alibi – they should look for an associated _______.

A. Cyber trail

B. piece of physical evidence

C. statement

D. none of the above

19. Creating a histogram of times to reveal periods of high activity is an example of which form of investigative reconstruction?

A. Functional
B. intentional
C. relational
D. temporal

20. The type of report that is a preliminary summary of findings is known as:

A. Sitrep
B. threshold assessment report
C. full investigative report
D. field notes

21. In crimes against individuals the ______ period leading up to the crime often contains the most important clues regarding the relationship between the offender and the victim.

A. 24-hour
B. 28-hour
C. 60-minute
D. 15-minute

22. Investigative reconstruction is composed of three different forms. Which of the following is NOT one of those three forms?

A. Functional
B. intentional
C. relational
D. temporal

23. The crime scene preservation process includes all but which of the following:

A. protecting against unauthorized alterations
B. acquiring digital evidence

C. confirming system date and time

D. controlling access to the crime scene

24. The process model whose goal is to completely describe the flow of information in a digital investigation is known as:

A. the physical model

B. the staircase model

C. the evidence flow model

D. the sub phase model

25. The first step in applying the scientific method to a digital investigation is to:

A. form a theory on what may have occurred

B. experiment or test the available evidence to confirm or refute your prediction

C. make one or more observations based on events that occurred

D. form a conclusion based on the results of your findings

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