Self-Assessment: Unit 1 – Introduction to Cybersecurity

Answer the following questions after reading the lecture resource Unit 1 – Introduction to Cybersecurity. The answers are found at the end of this self-assessment. For an authentic self-evaluation, it is recommended not to consult any resources or answers while attempting the assessment.

1. Which of the following best defines computer security?
   A. Measures and controls that ensure confidentiality, integrity and availability of information systems' assets.
   B. Regulations and laws that protect computer systems and resource misuse and abuse.
   C. Security guaranteed by anti-malware systems.
   D. The level of protection provided by a given computer system.

2. _____ assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
   A. Availability
   B. System Integrity
   C. Privacy
   D. Data Integrity

3. Which of the following types of attacks are classified as active?
   A. Network monitoring and traffic analysis
   B. Denial of Service attack
   C. Eavesdropping and wiretapping
   D. Shoulder surfing

4. _____ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
   A. Data Integrity
   B. Availability
   C. System Integrity
   D. Confidentiality

5. A loss of _____ is the unauthorized disclosure of information.
   A. integrity
   B. authenticity
   C. availability
   D. confidentiality

6. A _____ level breach of security could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
   A. high
   B. normal
   C. moderate
   D. low

7. A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy is a(n) _____.
   A. vulnerability
   B. countermeasure
   C. adversary

D. risk

8. An assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system is a(n) _____.
   A. risk
   B. asset
   C. attack
   D. vulnerability

9. The main difference between active and passive attacks in computer security is that _____.
   A. Active attacks are dangerous whereas passive attacks are inoffensive.
   B. Passive attacks are easier to detect than active attacks.
   C. Active attacks requires the involvement of a human being whereas passive attacks are automatic.
   D. Active attacks alter system resources or affect their operation whereas passive attacks do not.

10. A(n) _____ is an attempt to learn or make use of information from the system that does not affect system resources.
    A. passive attack
    B. inside attack
    C. outside attack
    D. active attack

11. Masquerade, falsification, and repudiation are threat actions that cause _____ threat consequences.
    A. unauthorized disclosure
    B. disruption
    C. deception
    D. usurpation

12. A threat action in which sensitive data are directly released to an unauthorized entity is _____.
    A. corruption
    B. exposure
    C. disruption
    D. intrusion

13. An example of _____ is an attempt by an unauthorized user to gain access to a system by posing as an authorized user.
    A. interception
    B. repudiation
    C. inference
    D. masquerade

14. The _____ prevents or inhibits the normal use or management of communications facilities.
    A. denial of service attack
    B. passive attack
    C. traffic encryption
    D. masquerade

15. A _____ is any action that compromises the security of information owned by an organization.
    A. security attack
    B. security mechanism
    C. security policy
    D. security service

16. The assurance that data received are exactly as sent by an authorized entity is known as _____.
    A. authentication
    B. data confidentiality
    C. access control
    D. data integrity

17. _____ is the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
    A. Traffic padding
    B. Traffic routing
    C. Traffic control
    D. Traffic integrity

18. Which security design principle states that a user or process should have only the minimum rights necessary to complete its task?
    A. Defence in Depth
    B. Least Privilege
    C. Complete Mediation
    D. Separation of Privilege

19. The concept of using multiple layers of security controls to protect resources aligns with:
    A. Economy of Mechanism
    B. Least Privilege
    C. Defence in Depth
    D. Separation of Privilege

20. Which characteristic best defines a system's "attack surface"?
    A. The physical location of servers
    B. The sum of all vulnerabilities and entry points accessible to attackers
    C. The encryption protocols used in network communications
    D. The frequency of software updates

ANSWERS

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