Information Security Fundamentals - MCQ Paper

Section A: CIA Triad & Security Fundamentals

1. Which of the following is not part of the CIA Triad?
A) Confidentiality
B) Integrity
C) Accessibility
D) Availability

2. The main challenge in security implementation is balancing between:
A) Cost and performance
B) Usability and security
C) Threats and vulnerabilities
D) Policies and compliance

3. Which attack primarily affects the availability aspect of the CIA Triad?
A) Data breach
B) Denial of Service (DoS)
C) Password theft
D) Insider threat

4. What is a vulnerability?
A) An external hacker attack
B) A weakness in a system that can be exploited
C) A type of malware
D) A form of encryption

5. Which type of security test is performed with no prior knowledge of the target system?
A) Gray box
B) Black box
C) White box
D) Internal test

Section B: AAA in Information Security

6. The "AAA" in information security stands for:
A) Authentication, Authorization, and Auditing
B) Authentication, Authorization, and Accounting
C) Access, Authentication, and Auditing
D) Access, Approval, and Accounting

7. What is the main goal of authentication?
A) To determine what actions a user can perform
B) To verify the identity of a user
C) To monitor user activities
D) To control network traffic

8. Authorization in AAA refers to:
A) Granting access based on verified identity
B) The process of verifying credentials
C) Recording user actions
D) Encrypting sensitive data

9. The Accounting component of AAA is primarily concerned with:
A) Data encryption
B) User identity verification
C) Tracking and logging user actions
D) Setting access permissions

10. Which tool is commonly used for accounting in network security?
A) IDS
B) SIEM
C) Firewall
D) Proxy server

11. In cloud environments, AAA faces challenges mainly due to:
A) Centralized hardware
B) Multi-tenant architecture
C) Simple access models
D) Lack of encryption

12. Passwordless authentication is an example of which AAA trend?
A) AI-driven authorization
B) Future of authentication
C) Advanced accounting
D) Multi-tenant compliance

13. In a Zero Trust Architecture, AAA supports which principle?
A) Trust but verify
B) Always verify and least privilege
C) Role-based access only
D) Open access for internal users

14. Event correlation in AAA refers to:
A) Combining multiple authentication methods
B) Matching logs to detect security patterns
C) Grouping users by role
D) Mapping IP addresses to devices

15. AI-driven identity management enhances AAA by:
A) Automating user provisioning
B) Detecting anomalous behavior dynamically
C) Reducing password length
D) Removing the need for authorization

Section C: Common Cyber Threats

16. A virus requires which of the following to spread?
A) Network vulnerability
B) User action
C) System reboot
D) Remote access

17. A worm differs from a virus because it:
A) Requires user action to execute
B) Needs a host program
C) Replicates itself without user intervention
D) Does not spread through networks

18. Which of the following is a Trojan Horse characteristic?
A) Self-replicates automatically
B) Disguises itself as legitimate software
C) Attacks network infrastructure directly
D) Spreads via email attachments only

19. The best defense against email spoofing is to:
A) Disable antivirus software
B) Open only unknown attachments
C) Verify sender addresses and avoid clicking unknown links
D) Allow scripts in emails