PRACTICE QUESTIONS

NCFM Pro – Cyber Security

1. Which of the following is a type of cyber threat? **[1Mark]**
   a) Phishing
   b) Email
   c) Antivirus
   d) Firewall

   Correct Answer: Phishing

2. What is the main purpose of encryption? **[1Mark]**
   a) Convert data into a secret code
   b) Speed up data transmission
   c) Decrease file size
   d) Create data backups

   Correct Answer: Convert data into a secret code

3. Which type of malware is designed to encrypt the victim's files and demand ransom for decryption? **[2Marks]**
   a) Virus
   b) Trojan
   c) Worm
   d) Ransomware

   Correct Answer: Ransomware

4. What distinguishes an Advanced Persistent Threat (APT) from other cyber threats?

   [3 Marks]

   a) Its use of malware
   b) Its focus on individual users
   c) Its long-term presence in a network
   d) Its targeting of financial data

   Correct Answer: Its long-term presence in a network

5. What aspect of the CIA Triad ensures data is accessible when needed? **[2 Marks]**
   a) Confidentiality
   b) Availability
   c) Integrity
   d) Authentication

   Correct Answer: Availability

6. Which component of the CIA Triad ensures data remains accurate and unaltered? **[2 Marks]**

   a) Integrity
   b) Confidentiality
   c) Availability
   d) Authorization

   Correct Answer: Phishing

7. What is a major benefit of implementing Micro-Segmentation in the Zero Trust Model? **[2 Marks]**

   a) It restricts lateral movement of attackers within the network
   b) It simplifies network management
   c) It allows unrestricted access to data
   d) It decreases the need for authentication

   Correct Answer: It restricts lateral movement of attackers within the network

8. How does Continuous Monitoring in the Zero Trust Model enhance an organization's security posture? **[2 Marks]**

   a) By only focusing on external security threats
   b) By simplifying the authentication process
   c) Through ongoing scrutiny of network traffic and user behaviours
   d) By reducing the need for security protocols

   Correct Answer: Through ongoing scrutiny of network traffic and user behaviours

9. What does VPN stand for? **[1 Mark]**

   a) Virtual Private Network
   b) Virtual Public Network
   c) Variable Private Network
   d) Vital Protection Network

   Correct Answer: Virtual Private Network

10. What type of encryption does a VPN typically use to secure data transmission? **[2 Marks]**

   a) AES
   b) Base64
   c) MD5
   d) RSA

Correct Answer: AES

11. What is the primary function of Intrusion Prevention Systems (IPS) in network security? **[2 Marks]**
    a) Monitoring network traffic
    b) Providing encryption
    c) Actively preventing security threats
    d) Logging user activities

    Correct Answer: Actively preventing security threats

12. What does DDoS stand for? **[1 Mark]**
    a) Distributed Denial of Service
    b) Digital Data of Service
    c) Direct Denial of Service
    d) Dynamic Denial of Service

    Correct Answer: Distributed Denial of Service

13. IoT-based attacks primarily target? **[2 Marks]**
    a) Cloud storage
    b) Network servers
    c) Offline computers
    d) Internet-connected devices

    Correct Answer: Internet-connected devices

14. What is a Zero-Day Exploit? **[3 Marks]**
    a) Unknown software vulnerability
    b) Known software vulnerability
    c) New software feature
    d) Recently patched software

    Correct Answer: Unknown software vulnerability

15. Which of the following is a method to ensure data integrity? **[1 Mark]**
    a) Digital signatures
    b) Data compression
    c) Data replication
    d) Data encryption

    Correct Answer: Digital signatures

16. What is the main purpose of using a VPN? **[1 Mark]**

a) To secure data transmission
b) To increase internet speed
c) To bypass network restrictions
d) To monitor network traffic

Correct Answer: To secure data transmission

17. What is a primary security concern with IoT devices? **[2 Marks]**

a) Lack of robust security features
b) High power consumption
c) Incompatibility with older networks
d) Difficulty in connecting to Wi-Fi networks

Correct Answer: Lack of robust security features

18. What is the main security benefit of using DNSSEC? **[3 Marks]**

a) Increasing browsing speed
b) Reducing data usage
c) Encrypting website content
d) Authenticating DNS data

Correct Answer: Authenticating DNS data

19. Why is regular firmware updating crucial for IoT device security? **[3 Marks]**

a) To patch security vulnerabilities
b) To maintain device compatibility
c) To improve device aesthetics
d) To increase battery life

Correct Answer: To patch security vulnerabilities

20. Which protocol is used for file transfers? **[1 Mark]**

a) HTTP
b) SMTP
c) IMAP
d) FTP

Correct Answer: FTP

21. In a network, what is the primary purpose of a subnet mask? **[1 Mark]**

a) To divide IP addresses into network and host parts
b) To encrypt data
c) To increase bandwidth
d) To identify the type of network

Correct Answer: To divide IP addresses into network and host parts

22. Which protocol is commonly used for secure communication over the Internet? **[1 Mark]**

a) HTTP
b) FTP
c) HTTPS
d) SMTP

Correct Answer: HTTPS

23. Why is regular software updating important in web security? **[1 Mark]**

a) A list of the most critical web application security risks
b) A list of top ten web designers
c) A ranking of the best web servers
d) A collection of the most popular web technologies

Correct Answer: A list of the most critical web application security risks

24. What is the OWASP Top Ten? **[1 Mark]**

a) A list of the most critical web application security risks
b) A list of top ten web designers
c) A ranking of the best web servers
d) A collection of the most popular web technologies

Correct Answer: A list of the most critical web application security risks

25. Which algorithm is commonly used in Public Key Cryptography? **[2 Marks]**

a) SHA-256
b) AES
c) MD5
d) RSA

Correct Answer: RSA