Unit-III

1. **What does VPN stand for in the context of IP security?**
   a. Virtual Private Network
   b. Very Private Network
   c. Virtual Personal Network
   d. Volatile Private Network

2. **Which protocol is commonly used for secure communication over the internet?**
   a. HTTP
   b. FTP
   c. TCP
   d. HTTPS

3. **What is the primary purpose of IPsec in network security?**
   a. Intrusion detection
   b. Data encryption
   c. IP address allocation
   d. Bandwidth management

4. **Which IPsec mode is used for secure communication between two devices in a point-to-point scenario?**
   a. Transport mode
   b. Tunnel mode
   c. Secure mode
   d. Encryption mode

5. **What does NAT stand for in the context of IP security?**
   a. Network Address Translation
   b. Network Access Token
   c. National Authentication Technology
   d. Network Action Trigger

6. **In IPsec, what is AH used for?**
   a. Authentication Header
   b. Authorisation Header
   c. Access Header
   d. Advanced Header

7. **Which cryptographic algorithm is commonly used in IPsec for encryption?**
   a. RSA
   b. DES
   c. AES
   d. MD5

8. **What is the purpose of a firewall in IP security architecture?**
   a. Data encryption
   b. Network address translation
   c. Access control
   d. Bandwidth management

9. **Which protocol is commonly used for remote access VPNs?**
   a. SSL
   b. PPTP
   c. L2TP
   d. IPSec

10. **What is the role of a Proxy Server in IP security?**
    a. Data encryption
    b. Access control
    c. Load balancing
    d. Packet filtering

11. **What is the primary purpose of the Authentication Header (AH) in IPsec?**
    a. Data encryption
    b. Access control
    c. Payload compression
    d. Packet authentication

12. **Which field in the authentication header provides the integrity check value for the packet?**
    a. Authentication data
    b. Next header
    c. Security Parameters Index (SPI)
    d. Source address

13. **In the context of AH, what is the SPI (Security Parameters Index) used for?**
    a. Encryption Key
    b. Identifying Security Associations
    c. Authentication Key
    d. Source Address Verification

14. **Which IPsec mode is typically associated with the use of the authentication header?**
    a. Transport mode
    b. Tunnel mode
    c. Secure mode
    d. Encryption mode

15. **What type of information does the authentication header protect in an IP packet?**
    a. Only the payload data
    b. Header information only
    c. Both header and payload data
    d. Source and destination addresses

16. **Which cryptographic algorithm is commonly used for integrity protection in the authentication header?**
    a. RSA
    b. DES
    c. AES
    d. HMAC (Hash-based Message Authentication Code)

17. **What happens if the integrity check in the authentication header fails?**
    a. The packet is dropped
    b. The packet is forwarded without any changes
    c. The packet is automatically encrypted
    d. The packet is marked for further analysis

18. Which field in the authentication header specifies the cryptographic algorithm used for integrity protection?
a. Next header
b. Security Parameters Index (SPI)
c. Authentication data
d. Authentication algorithm

19. How does the authentication header handle NAT (Network Address Translation) environments?
a. Compatible with NAT
b. Incompatible with NAT
c. Requires additional configuration for NAT
d. Automatically bypasses NAT

20. In which layer of the OSI model does the authentication header operate?
a. Network layer (layer 3)
b. Data link layer (layer 2)
c. Transport layer (layer 4)
d. Application layer (layer 7)

21. What is the primary purpose of the Encapsulating Security Payload (ESP) in IPsec?
a. Packet authentication
b. Data encryption
c. Access control
d. Source address verification

22. In IPsec, which mode is typically associated with the use of the Encapsulating Security Payload (ESP)?
a. Transport mode
b. Tunnel mode
c. Secure mode
d. Encryption mode

23. What type of information does the Encapsulating Security Payload (ESP) protect in an IP packet?
a. Only the payload data
b. Header information only
c. Both header and payload data
d. Source and destination addresses

24. Which field in the ESP header indicates the presence of padding in the packet?
a. Next jeader
b. Security Parameters Index (SPI)
c. Padding length
d. Payload data

25. In IPsec, what is the role of the Security Parameters Index (SPI) in the ESP header?
a. Identifying security associations
b. Data encryption
c. Packet authentication
d. Source address verification

26. What does the term Security Association (SA) refer to in the context of IPsec?
a. The process of encrypting data
b. A one-way cryptographic key
c. A bundle of security parameters
d. The authentication algorithm used

27. How are Security Associations (SAs) identified in IPsec communication?
a. By the IP address of the source
b. By the SPI (Security Parameters Index)
c. By the destination port number
d. By the length of the payload data

28. What happens when multiple security associations are combined in IPsec?
a. Increased security risk
b. Improved performance
c. Enhanced encryption strength
d. Compatibility issues

29. In the ESP header, which field specifies the cryptographic algorithm used for encryption?
a. Next header
b. Security Parameters Index (SPI)
c. Encryption algorithm
d. Padding length

30. Which of the following is a drawback of using ESP in a NAT (Network Address Translation) environment?
a. Compatible with NAT
b. Incompatible with NAT
c. Requires additional configuration for NAT
d. Automatically bypasses NAT

31. What is the primary purpose of key management in cryptography?
a. Data compression
b. Data encryption
c. Packet authentication
d. Source address verification

32. Which term refers to the process of generating keys for use in cryptographic algorithms?
a. Key distribution
b. Key negotiation
c. Key establishment
d. Key generation

33. What is the main challenge addressed by key management in secure communication?
a. Ensuring high bandwidth
b. Protecting against malware
c. Securely distributing and maintaining cryptographic keys
d. Reducing latency in the network

34. **In a Public Key Infrastructure (PKI), what is the purpose of a Certificate Authority (CA)?**
    a. Key generation
    b. Key distribution
    c. Key authentication
    d. Key revocation

35. **Which key management protocol is commonly used for secure key exchange over an insecure network, such as the internet?**
    a. SSL/TLS
    b. IKE (Internet Key Exchange)
    c. SSH (Secure Shell)
    d. IPsec

36. **What is the purpose of a Key Distribution Center (KDC) in Kerberos authentication?**
    a. Key generation
    b. Key distribution
    c. Key authentication
    d. Key revocation

37. **What does the term 'symmetric key management' refer to in cryptography?**
    a. Managing public and private keys
    b. Distributing identical keys to communicating parties
    c. Using asymmetric encryption for key exchange
    d. Revoking compromised keys

38. **Which of the following is a benefit of using a Hardware Security Module (HSM) in key management?**
    a. Increased key distribution speed
    b. Enhanced key generation capabilities
    c. Improved key storage security
    d. Simplified key authentication process

39. **What is key rotation in the context of key management?**
    a. Periodically changing cryptographic algorithms
    b. Changing encryption keys during communication
    c. Revoking compromised keys
    d. Authenticating keys using a rotation mechanism

40. **In key management, what does the term 'key escrow' mean?**
    a. Storing keys securely
    b. Distributing keys to multiple parties
    c. Backing up keys with a trusted third party
    d. Exchanging keys through a secure channel