Unit-II

1. **What is the primary goal of network security?**
   a. Enhancing network speed
   b. Protecting data and ensuring the integrity, confidentiality and availability of network resources
   c. Maximising network bandwidth
   d. Improving network scalability

2. **Which of the following is not a common network security threat?**
   a. Malware
   b. Phishing
   c. Redundancy
   d. DDoS attacks

3. **What is the purpose of a firewall in network security?**
   a. Speed up network traffic
   b. Monitor and control incoming and outgoing network traffic based on predetermined security rules
   c. Enhance network connectivity
   d. Increase network redundancy

4. **Which encryption protocol is commonly used to secure data transmission over the internet?**
   a. SSL (Secure Sockets Layer)
   b. FTP (File Transfer Protocol)
   c. UDP (User Datagram Protocol)
   d. ICMP (Internet Control Message Protocol)

5. **What does VPN stand for in the context of network security?**
   a. Virtual Private Network
   b. Very Private Network
   c. Validated Public Network
   d. Virtual Personal Network

6. **What is the purpose of Intrusion Detection System (IDS) in network security?**
   a. To encrypt network traffic
   b. To identify and respond to suspicious activities or security breaches
   c. To enhance network speed
   d. To create network backups

7. **Which of the following is a social engineering attack?**
   a. Brute force attack
   b. SQL injection
   c. Phishing
   d. DDoS attack

8. **What is the purpose of Two-Factor Authentication (2FA)?**
   a. To encrypt network traffic
   b. To provide redundancy in network communication
   c. To enhance network speed
   d. To add an extra layer of security by requiring two forms of identification

9. **Which protocol is commonly used for secure file transfer?**
   a. FTP (File Transfer Protocol)
   b. HTTP (Hypertext Transfer Protocol)
   c. SFTP (Secure File Transfer Protocol)
   d. SMTP (Simple Mail Transfer Protocol)

10. **What is the purpose of a honeypot in network security?**
    a. To speed up network communication
    b. To detect and deflect potential attackers
    c. To increase network redundancy
    d. To encrypt network traffic

11. **What is the primary purpose of authentication in computer security?**
    a. Enhancing network speed
    b. Ensuring data confidentiality
    c. Verifying the identity of users or systems
    d. Maximising server bandwidth

12. **Which of the following is an example of a knowledge-based authentication method?**
    a. Fingerprint recognition
    b. Smart card authentication
    c. Password authentication
    d. Retina scanning

13. **What is biometric authentication based on?**
    a. Something you know
    b. Something you have
    c. Something you are
    d. Something you do

14. **Which factor of authentication involves physical devices like USB tokens or smart cards?**
    a. Something you know
    b. Something you have
    c. Something you are
    d. Something you do

15. **What does OTP stand for in the context of authentication?**
    a. One-Time Password
    b. Over-The-Phone
    c. Online Transaction Protocol
    d. Open Tokenisation Protocol

16. **Which authentication method requires users to provide both a password and a dynamically generated code?**
    a. Biometric authentication
    b. Two-Factor Authentication (2FA)
    c. Single Sign-On (SSO)
    d. Multi-Factor Authentication (MFA)

17. **What is the purpose of CAPTCHA in authentication?**
    a. To generate secure passwords
    b. To prevent automated bots from accessing a system
    c. To encrypt user credentials
    d. To improve network speed

18. **Which type of authentication uses a physical characteristic, such as fingerprints or facial features?**
    a. Token-based authentication
    b. Biometric authentication
    c. Knowledge-based authentication
    d. Smart card authentication

19. **What is the main advantage of using Multi-Factor Authentication (MFA)?**
    a. Simplifies the authentication process
    b. Increases the risk of unauthorised access
    c. Provides an additional layer of security
    d. Reduces the need for strong passwords

20. **Which authentication method involves users logging in once and gaining access to multiple systems or applications without the need to log in again?**
    a. Two-Factor Authentication (2FA)
    b. Single Sign-On (SSO)
    c. Multi-Factor Authentication (MFA)
    d. Passwordless Authentication

21. **What is Kerberos?**
    a. A type of encryption algorithm
    b. An authentication protocol
    c. A firewall system
    d. A network routing protocol

22. **Which of the following is a primary goal of Kerberos?**
    a. Ensuring data confidentiality
    b. Providing secure file transfer
    c. Verifying the identity of users and systems
    d. Maximising network speed

23. **In a Kerberos authentication system, what is the Key Distribution Center (KDC)?**
    a. A secure database of user passwords
    b. A central server responsible for distributing session keys
    c. A cryptographic algorithm used for encryption
    d. A hardware token used for authentication

24. What is a Ticket Granting Ticket (TGT) in Kerberos?
a. A ticket for accessing network resources
b. A ticket issued by the Key Distribution Center (KDC) after user authentication
c. A ticket used for encrypting data
d. A one-time use password

25. Which of the following is not one of the components of the Kerberos authentication process?
a. Authentication Server (AS)
b. Ticket Granting Server (TGS)
c. Authorisation Server (AS)
d. Service Server (SS)

26. What is the purpose of the Ticket Granting Server (TGS) in Kerberos?
a. To issue Ticket Granting Tickets (TGTs)
b. To authenticate users
c. To distribute session keys
d. To encrypt data transmission

27. Which encryption technique is commonly used in Kerberos for secure communication?
a. RSA
b. DES (Data Encryption Standard)
c. AES (Advanced Encryption Standard)
d. MD5 (Message Digest Algorithm 5)

28. What is the purpose of the Ticket Granting Service (TGS) request in the Kerberos authentication process?
a. To obtain a Ticket Granting Ticket (TGT)
b. To request access to a specific service
c. To authenticate the user to the network
d. To encrypt the user's credentials

29. In Kerberos, what does the session key represent?
a. User's password
b. Encrypted data
c. Temporary cryptographic key for secure communication
d. Public key

30. What advantage does Kerberos provide in a network environment?
a. Increased network speed
b. Single sign-on capability
c. Simplified encryption methods
d. Redundancy in user authentication

31. What is X.509?
a. A networking protocol
b. An encryption algorithm
c. A standard for digital certificates
d. A firewall technology

32. What is the primary purpose of X.509 certificates?
a. Network routing
b. User authentication
c. Data compression
d. Secure communication

33. Which cryptographic algorithm is commonly used for digital signatures in X.509 certificates?
a. DES (Data Encryption Standard)
b. RSA (Rivest-Shamir-Adleman)
c. AES (Advanced Encryption Standard)
d. MD5 (Message Digest Algorithm 5)

34. What information does an X.509 certificate typically include?
a. User's password
b. Public key, issuer, subject, validity period, and digital signature
c. Session key and private key
d. Network address and subnet mask

35. In X.509, what is the purpose of the digital signature?
a. Encrypting data
b. Verifying the integrity of the certificate
c. Authenticating the user
d. Generating random numbers

36. What does the term 'issuer' refer to in an X.509 certificate?
a. The entity requesting a certificate
b. The person being authenticated
c. The organisation that issues the certificate
d. The cryptographic algorithm used in the certificate

37. What is the purpose of the Common Name (CN) field in an X.509 certificate?
a. Storing the user's password
b. Identifying the issuer of the certificate
c. Identifying the subject of the certificate
d. Encrypting the certificate data

38. Which file format is commonly used to store X.509 certificates?
a. .txt b. .pdf c. .pem d. .docx

39. What is the purpose of the validity period in an X.509 certificate?
a. To specify the encryption algorithm used in the certificate
b. To indicate the time frame during which the certificate is considered valid
c. To store information about the certificate issuer
d. To identify the subject's public key

40. **Which protocol is commonly used for the distribution of X.509 certificates?**
    a. FTP (File Transfer Protocol)
    b. HTTP (Hypertext Transfer Protocol)
    c. LDAP (Lightweight Directory Access Protocol)
    d. SMTP (Simple Mail Transfer Protocol)

41. **What is the primary purpose of a directory authentication service?**
    a. Data encryption
    b. User authorisation
    c. Centralised user management and authentication
    d. Network routing

42. **Which protocol is commonly used for communication between directory clients and servers?**
    a. HTTP (Hypertext Transfer Protocol)
    b. LDAP (Lightweight Directory Access Protocol)
    c. FTP (File Transfer Protocol)
    d. TCP/IP (Transmission Control Protocol/Internet Protocol)

43. **What is the role of a directory service in the context of authentication?**
    a. Encrypting user data
    b. Storing and organising user information
    c. Providing network redundancy
    d. Ensuring data confidentiality

44. **In a directory authentication service, what is the function of the Directory Information Tree (DIT)?**
    a. Storing user passwords
    b. Defining network routes
    c. Organising directory entries in a hierarchical structure
    d. Managing encryption keys

45. **Which of the following is a benefit of using a directory authentication service?**
    a. Increased network speed
    b. Centralised user authentication and management
    c. Complex encryption algorithms
    d. Decentralised user accounts

46. **What is the purpose of the LDAP bind operation in directory authentication?**
    a. To encrypt user data
    b. To establish a connection between the client and server
    c. To authenticate a user to the directory server
    d. To distribute session keys

47. **Which type of directory service is commonly used in microsoft environments?**
    a. OpenLDAP
    b. Novell eDirectory
    c. Active Directory
    d. Apache Directory Server

48. **What is the significance of the Root DSE (Directory Service Entry) in LDAP?**
    a. It contains information about the directory server's encryption keys
    b. It represents the root of the directory tree and provides information about the directory server
    c. It stores user passwords in plaintext
    d. It defines network routes for directory clients

49. **What is Single Sign-On (SSO) in the context of directory authentication?**
    a. Allowing users to sign in only once during a session
    b. Requiring multiple authentication steps for enhanced security
    c. Enabling users to access multiple systems with a single login
    d. Encrypting user credentials during authentication

50. **What is the purpose of the Lightweight Directory Access Protocol (LDAP) in directory services?**
    a. To provide a secure channel for data transfer
    b. To manage network bandwidth
    c. To define encryption algorithms
    d. To access and manipulate directory information

51. **What is Pretty Good Privacy (PGP)?**
    a. An encryption standard for wireless networks
    b. A file transfer protocol
    c. A cryptographic software suite for email encryption and data security
    d. A network routing protocol

52. **Who is the creator of Pretty Good Privacy (PGP)?**
    a. Linus Torvalds
    b. Phil Zimmermann
    c. Tim Berners-Lee
    d. Bruce Schneier

53. **What is the main purpose of PGP?**
    a. To enhance network speed
    b. To provide a secure file transfer protocol
    c. To encrypt email communication and files
    d. To manage user authentication in a directory service

54. How does PGP ensure the confidentiality of messages?
a. By using a public-key infrastructure
b. By implementing symmetric-key encryption
c. By applying digital signatures
d. By incorporating hash functions

55. What is the role of the PGP public key?
a. Encrypting messages
b. Decrypting messages
c. Verifying the sender's identity
d. Signing messages

56. What is a key pair in the context of PGP?
a. Two identical encryption keys
b. A combination of a public key and a private key
c. A pair of digital signatures
d. Two different public keys

57. What is the purpose of the PGP web of trust?
a. To verify the integrity of encrypted files
b. To establish a network of secure communication
c. To authenticate users in a directory service
d. To validate the authenticity of public keys

58. Which algorithm is commonly used for creating PGP digital signatures?
a. MD5 (Message Digest Algorithm 5)
b. SHA-256 (Secure Hash Algorithm 256-bit)
c. RSA (Rivest-Shamir-Adleman)
d. AES (Advanced Encryption Standard)

59. What does the term 'key fingerprint' refer to in PGP?
a. A summary of the public key
b. A unique identifier for a PGP key
c. A secure channel for key exchange
d. A visual representation of the key pair

60. How does PGP provide authentication in addition to encryption?
a. By using symmetric-key encryption
b. Through the use of digital signatures
c. By relying on a public-key infrastructure
d. Via hash functions

61. What is S/MIME?
a. A network routing protocol
b. A file transfer protocol
c. A standard for secure email communication
d. An encryption algorithm

62. What does S/MIME provide in the context of email communication?
a. Network speed optimisation
b. Secure file attachments
c. Encryption, authentication & digital signatures
d. Compression of email messages

63. Which cryptographic algorithm is commonly used in S/MIME for encrypting email messages?
a. AES (Advanced Encryption Standard)
b. DES (Data Encryption Standard)
c. RSA (Rivest-Shamir-Adleman)
d. MD5 (Message Digest Algorithm 5)

64. What is the purpose of S/MIME digital signatures?
a. Encrypting email content
b. Verifying the integrity and origin of the email message
c. Compressing email attachments
d. Routing email messages to the correct destination

65. Which type of keys are used in S/MIME for secure email communication?
a. Session keys
b. Symmetric keys
c. Public and private keys
d. Hash keys

66. What is the purpose of a digital certificate in S/MIME?
a. To authenticate the email server
b. To encrypt email attachments
c. To validate the identity of the email sender
d. To compress email messages

67. In S/MIME, what does the term 'PKCS' stand for?
a. Public Key Cryptography Standards
b. Pretty Key Compression Standard
c. Personal Key Certificate System
d. Public Key Compression Scheme

68. Which MIME types are commonly used in S/MIME for email encryption and signing?
a. text/plain and image/jpeg
b. application/pkcs7-mime and application/x-pkcs7-signature
c. audio/wav and video/mp4
d. application/json and application/xml

69. What is the primary benefit of using S/MIME in email communication?
a. Faster email delivery
b. Improved spam filtering
c. Enhanced security through encryption and digital signatures
d. Larger email attachment limits