**SNS COLLEGE OF ENGINEERING**

Kurumbapalayam (Po), Coimbatore – 641 107

**AN AUTONOMOUS INSTITUTION**

Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai

## Transport Layer

1. **What is the primary function of the Transport Layer in the OSI model?**
    - A) Data framing and error detection
    - B) End-to-end communication and error recovery
    - C) Packet routing and addressing
    - D) Network segmentation

    **Answer: B) End-to-end communication and error recovery**

2. **Which two main protocols operate at the Transport Layer?**
    - A) TCP and UDP
    - B) IP and ARP
    - C) HTTP and FTP
    - D) OSPF and BGP

    **Answer: A) TCP and UDP**

3. **What does TCP stand for?**
    - A) Transmission Control Protocol
    - B) Transport Control Protocol
    - C) Terminal Control Protocol
    - D) Transfer Control Protocol

    **Answer: A) Transmission Control Protocol**

4. **Which of the following is a characteristic of TCP?**
    - A) Connectionless
    - B) Unreliable
    - C) Error detection and correction
    - D) No flow control

    **Answer: C) Error detection and correction**

5. **What does UDP stand for?**
    - A) User Datagram Protocol
    - B) Universal Datagram Protocol
    - C) Unified Data Protocol
    - D) User Data Protocol

**Answer: A) User Datagram Protocol**

6. **Which of the following is a characteristic of UDP?**
   - A) Connection-oriented
   - B) Reliable and guarantees delivery
   - C) Connectionless and provides no guarantees
   - D) Provides error correction

   **Answer: C) Connectionless and provides no guarantees**

7. **What is the purpose of a port number in the Transport Layer?**
   - A) To identify a specific process or service on a device
   - B) To route packets between different networks
   - C) To encrypt data for secure transmission
   - D) To provide physical addressing

   **Answer: A) To identify a specific process or service on a device**

8. **Which protocol uses a three-way handshake to establish a connection?**
   - A) UDP
   - B) HTTP
   - C) TCP
   - D) FTP

   **Answer: C) TCP**

9. **In TCP, what is the purpose of the ACK (Acknowledgment) number?**
   - A) To indicate the total number of packets sent
   - B) To confirm receipt of data and ensure reliable delivery
   - C) To identify the sender’s port number
   - D) To request retransmission of lost packets

   **Answer: B) To confirm receipt of data and ensure reliable delivery**

10. **What is a "port scan"?**
    - A) A technique to monitor network traffic
    - B) A method to detect open ports on a device
    - C) A process to secure network communications
    - D) A way to manage IP address assignments

    **Answer: B) A method to detect open ports on a device**

## Transport Layer Protocols

11. **Which protocol is used to provide secure communication over the Internet?**
    - A) FTP

- B) SSL/TLS
- C) Telnet
- D) ICMP

**Answer: B) SSL/TLS**

12. **What is the default port number for HTTP?**
    - A) 21
    - B) 80
    - C) 443
    - D) 25

**Answer: B) 80**

13. **What is the default port number for HTTPS?**
    - A) 80
    - B) 443
    - C) 21
    - D) 25

**Answer: B) 443**

14. **Which Transport Layer protocol is commonly used for streaming media?**
    - A) TCP
    - B) UDP
    - C) HTTP
    - D) FTP

**Answer: B) UDP**

15. **What is the purpose of flow control in TCP?**
    - A) To prevent network congestion
    - B) To manage the speed of data transmission between sender and receiver
    - C) To ensure data integrity
    - D) To encrypt data packets

**Answer: B) To manage the speed of data transmission between sender and receiver**

16. **Which TCP flag is used to initiate a connection?**
    - A) SYN
    - B) ACK
    - C) FIN
    - D) RST

**Answer: A) SYN**

17. **What is the function of the FIN flag in TCP?**
    - A) To establish a connection
    - B) To acknowledge receipt of data
    - C) To terminate a connection
    - D) To reset a connection

    **Answer: C) To terminate a connection**

18. **Which of the following is a feature of TCP's congestion control?**
    - A) Slow start
    - B) Fast retransmit
    - C) Fast recovery
    - D) All of the above

    **Answer: D) All of the above**

19. **What does the term "sequence number" refer to in TCP?**
    - A) A number used for data encryption
    - B) A number that identifies the order of bytes in a TCP segment
    - C) A number for error detection
    - D) A number for flow control

    **Answer: B) A number that identifies the order of bytes in a TCP segment**

20. **Which protocol is used for remote command-line access to network devices?**
    - A) SSH
    - B) HTTP
    - C) FTP
    - D) SNMP

    **Answer: A) SSH**

## Network Security Basics

21. **What is the primary purpose of a firewall?**
    - A) To manage network traffic
    - B) To prevent unauthorized access to or from a private network
    - C) To encrypt data packets
    - D) To route packets between networks

    **Answer: B) To prevent unauthorized access to or from a private network**

22. **What does the acronym VPN stand for?**
    - A) Virtual Private Network
    - B) Virtual Public Network
    - C) Verified Private Network

- D) Variable Private Network

**Answer: A) Virtual Private Network**

23. **Which of the following is a type of VPN protocol?**
    - A) FTP
    - B) SSL/TLS
    - C) IPsec
    - D) HTTP

**Answer: C) IPsec**

24. **What is the function of encryption in network security?**
    - A) To prevent unauthorized access to data
    - B) To ensure data integrity
    - C) To improve network performance
    - D) To manage IP address allocation

**Answer: A) To prevent unauthorized access to data**

25. **Which encryption algorithm is commonly used in SSL/TLS for securing web traffic?**
    - A) DES
    - B) AES
    - C) RSA
    - D) MD5

**Answer: B) AES**

26. **What is a "man-in-the-middle" attack?**
    - A) An attack that disrupts network traffic by injecting malicious packets
    - B) An attack where the attacker intercepts and potentially alters communications between two parties
    - C) An attack that exploits software vulnerabilities to gain unauthorized access
    - D) An attack that floods a network with excessive traffic

**Answer: B) An attack where the attacker intercepts and potentially alters communications between two parties**

27. **Which security mechanism ensures data integrity?**
    - A) Encryption
    - B) Hash functions
    - C) Access control
    - D) Authentication

**Answer: B) Hash functions**

28. **What is the purpose of an Intrusion Detection System (IDS)?**
    - A) To block unauthorized access to the network
    - B) To monitor and analyze network traffic for signs of malicious activity
    - C) To manage IP address assignments
    - D) To encrypt data packets

    **Answer: B) To monitor and analyze network traffic for signs of malicious activity**

29. **What does the acronym SSL stand for?**
    - A) Secure Sockets Layer
    - B) Secure System Layer
    - C) Server Sockets Layer
    - D) Secure Software Layer

    **Answer: A) Secure Sockets Layer**

30. **Which protocol is used to secure email communications?**
    - A) SMTP
    - B) IMAP
    - C) POP3
    - D) S/MIME

    **Answer: D) S/MIME**

## Advanced Security Concepts

31. **What is a "denial-of-service" (DoS) attack?**
    - A) An attack that encrypts data to prevent access
    - B) An attack that floods a network or server with excessive traffic to disrupt services
    - C) An attack that intercepts and alters network communications
    - D) An attack that exploits vulnerabilities in software

    **Answer: B) An attack that floods a network or server with excessive traffic to disrupt services**

32. **What is two-factor authentication (2FA)?**
    - A) A method of authentication that requires two different passwords
    - B) A security process that requires two forms of identification from different categories
    - C) A process of encrypting data with two keys
    - D) A method of verifying identity through biometric data

    **Answer: B) A security process that requires two forms of identification from different categories**

33. **Which security protocol is used to establish a secure, encrypted connection between a web browser and a server?**
    - A) HTTP
    - B) FTP
    - C) SSL/TLS
    - D) SNMP

    **Answer: C) SSL/TLS**

34. **What is the purpose of a digital certificate?**
    - A) To provide a secure communication channel
    - B) To verify the identity of an entity and enable encrypted communication
    - C) To manage network traffic
    - D) To monitor network performance

    **Answer: B) To verify the identity of an entity and enable encrypted communication**

35. **What does the acronym VPN stand for?**
    - A) Virtual Public Network
    - B) Virtual Private Network
    - C) Verified Private Network
    - D) Variable Private Network

    **Answer: B) Virtual Private Network**

36. **Which encryption standard is commonly used for securing wireless networks?**
    - A) WEP
    - B) WPA
    - C) WPA2
    - D) WPA3

    **Answer: C) WPA2**

37. **What is the primary goal of a security policy in an organization?**
    - A) To configure network hardware
    - B) To define security measures and guidelines for protecting the organization’s information assets
    - C) To manage IP address allocation
    - D) To optimize network performance

    **Answer: B) To define security measures and guidelines for protecting the organization’s information assets**

38. **What is a “zero-day” vulnerability?**
    - A) A vulnerability that is publicly known and has a known fix

- B) A vulnerability that is discovered and exploited before a patch or fix is available
- C) A vulnerability that occurs after a security update
- D) A vulnerability that is fixed within a day of discovery

**Answer: B) A vulnerability that is discovered and exploited before a patch or fix is available**

39. **What is a common technique used to protect against SQL injection attacks?**
    - A) Using prepared statements and parameterized queries
    - B) Encrypting the database
    - C) Implementing firewalls
    - D) Regularly updating software

**Answer: A) Using prepared statements and parameterized queries**

40. **Which technology is used to protect data in transit over a network?**
    - A) Data masking
    - B) Encryption
    - C) Compression
    - D) Data deduplication

**Answer: B) Encryption**

## Security Tools and Practices

41. **What is a "honeypot" in network security?**
    - A) A device used to trap and analyze malicious activity
    - B) A tool for encrypting network traffic
    - C) A type of firewall rule
    - D) A method for authenticating users

**Answer: A) A device used to trap and analyze malicious activity**

42. **What is the purpose of a vulnerability scanner?**
    - A) To monitor network traffic
    - B) To identify and assess vulnerabilities in a system or network
    - C) To manage IP address assignments
    - D) To encrypt data packets

**Answer: B) To identify and assess vulnerabilities in a system or network**

43. **Which of the following is a common method of securing data at rest?**
    - A) Encryption
    - B) VPN
    - C) Firewalls

- D) IDS

**Answer: A) Encryption**

44. **What does the acronym IDS stand for in network security?**
    - A) Intrusion Detection System
    - B) Integrated Defense System
    - C) Internet Defense Strategy
    - D) Information Detection Service

    **Answer: A) Intrusion Detection System**

45. **What is the purpose of a security information and event management (SIEM) system?**
    - A) To manage user authentication
    - B) To provide real-time analysis and monitoring of security events and incidents
    - C) To encrypt network traffic
    - D) To perform vulnerability assessments

    **Answer: B) To provide real-time analysis and monitoring of security events and incidents**

46. **Which practice is essential for maintaining a secure network environment?**
    - A) Regularly updating software and applying patches
    - B) Disabling firewalls
    - C) Using outdated encryption methods
    - D) Allowing unrestricted network access

    **Answer: A) Regularly updating software and applying patches**

47. **What is a “phishing” attack?**
    - A) An attack that floods a network with traffic
    - B) An attempt to deceive individuals into revealing sensitive information
    - C) An attack that exploits software vulnerabilities
    - D) An attack that involves physical access to devices

    **Answer: B) An attempt to deceive individuals into revealing sensitive information**

48. **Which of the following is a principle of network security?**
    - A) Availability
    - B) Confidentiality
    - C) Integrity
    - D) All of the above

    **Answer: D) All of the above**

49. **What is a “patch” in the context of software security?**
    - A) A physical device used to protect network access
    - B) A software update designed to fix vulnerabilities or bugs
    - C) A method of data encryption
    - D) A tool for managing network traffic

    **Answer: B) A software update designed to fix vulnerabilities or bugs**

50. **What is the role of access control in network security?**
    - A) To monitor network performance
    - B) To regulate who can access and use resources in a network
    - C) To encrypt network traffic
    - D) To manage IP address allocations

    **Answer: B) To regulate who can access and use resources in a network**