Networking Basics for Cyber Security

Basic networking concepts

Term	Meaning
IP Address	Unique address of a device on a network
MAC Address	Physical address of network card
DNS	Converts website name → IP address
TCP	Reliable connection-based protocol
UDP	Fast, connectionless protocol
Packet	Small unit of data sent over network

DNS:

In networking, DNS (Domain Name System) acts as the internet's phonebook, translating human-friendly domain names (like www.google.com) into machine-readable IP addresses (like 142.250.196.100) so browsers and devices can find and connect to websites and services, making the internet usable without memorizing complex numbers.

How it Works (Simplified)

1] User Request: You type a domain name (e.g., example.com) into your browser.

2] DNS Lookup: Your browser asks a DNS server for the IP address of example.com.

3] Server Response: The DNS server finds the corresponding IP address and sends it back to your browser.

4] Connection: Your browser uses that IP address to connect to the correct web server and load the website.

TCP/IP (The Protocol Suite/Model)

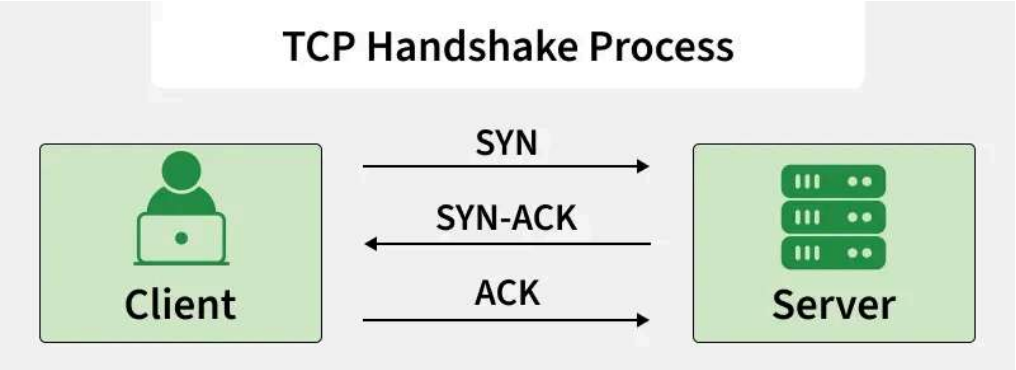
TCP/IP is a suite of protocols, a set of standardized rules that allow computers to communicate on a network like the internet.

It includes hundreds of other protocols beyond just TCP and IP, such as UDP, HTTP, FTP, and SMTP.

1. Transmission Control Protocol (TCP)

- TCP (Transmission Control Protocol) ensures that data reaches the destination correctly and in the right order, even if parts of the network are slow or unreliable.
- It works at the Transport Layer (Layer 4) of the OSI model

Three-Way Handshake:
TCP is connection-orientated, meaning a connection must be established before any data is sent. This is done using a three-way handshake:



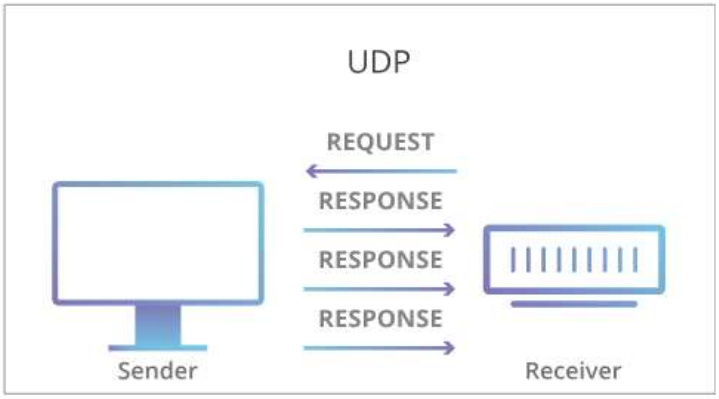
SYN (Synchronize): The sender sends a SYN segment to the receiver to request a connection.
SYN-ACK (Synchronize-Acknowledge): The receiver responds with a SYN-ACK segment, acknowledging the request and agreeing to the connection.
ACK (Acknowledge): The sender replies with an ACK, confirming the connection is established.

How TCP Works

1. Segmenting: TCP divides large data into smaller segments for efficient and reliable transmission.
2. Routing via IP: IP delivers TCP segments from sender to receiver using network addresses and routing paths.
3. Reassembly at Receiver: TCP rearranges received segments in the correct order using sequence numbers.
4. Acknowledgments (ACKs): The receiver confirms successful delivery of segments by sending acknowledgments.
5. Retransmission: TCP resends lost or unacknowledged segments to ensure complete data delivery.
6. Flow & Error Control: TCP controls data flow and detects errors to prevent congestion and corruption.

2. User Datagram Protocol (UDP)

- It is a Transport Layer protocol of the Internet Protocol (IP) that provides fast, connectionless, and lightweight communication between processes.
- It **does not guarantee delivery, order, or error checking,** making it suitable for real-time and time-sensitive applications such as video streaming, DNS, and VoIP (voice over IP).



How is UDP used in DDoS attacks?

- Since UDP does not require a handshake, attackers can 'flood' a targeted server with UDP traffic without first getting that server's permission to begin communication.
- A typical UDP flood attack sends a large number of UDP datagrams to random ports on its target computer.
- This forces the target to respond with an equally large number of ICMP packets, which indicate those ports were unreachable.
- The computing resources required to respond to each fraudulent datagram can exhaust the target, resulting in a denial-of-service to legitimate traffic.

Wireshark Observations (Based on Live Packet Capture)

- After starting live capture on the Wi-Fi interface, I observed continuous packets being generated in real time as network activity occurred.

- When the **DNS filter** was applied, multiple DNS queries and responses were visible, showing domain names such as *googleapis.com*, *chatgpt.com*, and *doubleclick.net* being resolved to IP addresses.

- DNS traffic mainly used **UDP port 53**, and both IPv4 and IPv6 addresses were observed in the responses.

- Applying the **TCP filter** displayed packets containing sequence numbers, acknowledgment numbers, ACK flags, and keep-alive packets, confirming reliable communication.

- TCP packets were mostly communicating over **port 443**, indicating secure HTTPS connections.

- The **TCP three-way handshake** was visible using SYN, SYN-ACK, and ACK packets before encrypted communication started.

- When the **UDP filter** was applied, several QUIC packets were observed, showing that modern web traffic uses UDP for faster communication.

- QUIC packets displayed protected payloads, indicating encrypted data transfer over UDP.

- Using the **TLS filter**, encrypted traffic was clearly visible as TLSv1.2 and TLSv1.3 application data.

- The encrypted payload could not be read, confirming that HTTPS traffic hides actual content from packet inspection.

- Client Hello packets were visible in some sessions, showing the beginning of secure TLS negotiation.

- During browsing activity, a large volume of packets was generated automatically, even without manual user input.

Interview Questions:

- What is a TCP handshake?
- Difference between TCP and UDP?
- What is DNS?
- What is packet sniffing?
- Why is HTTPS more secure than HTTP?