Packets & Frames

Learned:

- Every packet has headers that contain information like source and destination addresses, protocol type, and other data to help it reach the correct destination.

- The TCP Three-Way Handshake sets up reliable connections between devices, which helps ensure data is sent safely and in order.

- TCP connections such as FIN,ACK, and RST can help in identifying if connections just started or if there is any suspicious activities on a network.

- Knowing the ports and protocols for incoming/outgoing packets helps spot insecure services, for example unencrypted HTTP on port 80 or unusual ports that might be targeted.

Packets are small pieces of data that together form a larger message. A **packet** contains the **IP header** and **payload**. A **frame** adds extra information like **MAC addresses** so data reaches the correct device on a local network. Packets make communication across networks efficient.

Packet Headers

- **Time to Live (TTL):** Prevents packets from clogging the network.
- **Checksum:** Ensures data integrity; if data changes, the checksum will differ.
- **Source Address:** IP of the sending device.
- **Destination Address:** IP of the receiving device.

TCP vs UDP

- **TCP (Connection-based):** Ensures reliable delivery. Uses **Three-Way Handshake** to establish a connection.
- **UDP (Stateless):** Fast delivery without acknowledgment, less reliable.

TCP Three-Way Handshake

1. **SYN:** Client sends initial sequence number (ISN).
2. **SYN/ACK:** Server responds with its ISN and acknowledges client's ISN.
3. **ACK:** Client acknowledges server's ISN; data can now flow.

Closing TCP Connections

- **FIN:** Signals the end of a connection.
- **ACK:** Confirms closure.
- **RST:** Ends connection immediately if there’s a problem.

Ports

- Range: **0–65535**; common ports **0–1024**.
- Used to direct data to the correct application.
- Examples:
  - **HTTP:** 80
  - **HTTPS:** 443
  - **FTP:** 21
  - **SSH:** 22
  - **SMB:** 445
  - **RDP:** 3389

Protocols

- **HTTP / HTTPS:** Browsing the web (HTTPS is secure).
- **FTP:** File transfer between client and server.
- **SSH:** Secure text-based login.
- **SMB:** File and device sharing.
- **RDP:** Remote desktop access.