CYBERSECURITY DAILY DIARY

DAY-03
DATE- 25 June, 2025

Topics Covered:

- TCP vs UDP: study 3-way handshake
- Flags (SYN/ACK/FIN/RST)
- Common port numbers and use-cases.

What did I learn:

Today I explored the **differences between TCP and UDP**, two core transport protocols that shape how data moves across networks. This deep dive helped me understand not just how they work, but when and why to use each.

- I studied the **TCP 3-way handshake**—a reliable connection setup involving **SYN → SYN-ACK → ACK**. It ensures both sender and receiver are ready before data transmission begins.
- I learned about **TCP flags**:
  - **SYN**: Initiates a connection.
  - **ACK**: Acknowledges received data.
  - **FIN**: Gracefully ends a connection.
  - **RST**: Abruptly resets a connection—often seen in error handling or intrusion detection.
- In contrast, **UDP skips the handshake**, making it faster but less reliable. It's ideal for time-sensitive applications like **video streaming, DNS queries, and online gaming**.
- I mapped **common port numbers**:
  - **TCP 80** – HTTP
  - **TCP 443** – HTTPS
  - **TCP 22** – SSH
  - **UDP 53** – DNS
  - **UDP 123** – NTP (Network Time Protocol)
- I realized how **TCP's reliability** makes it perfect for secure file transfers and login sessions, while **UDP's speed** suits real-time communication where occasional packet loss is acceptable.

This knowledge is vital for my network analysis project. Understanding how TCP and UDP behave helps me interpret packet captures, detect anomalies, and simulate realistic traffic in my lab. It also prepares me to configure firewalls, analyze logs, and choose the right protocol for each cybersecurity use-case.