CYBERSECURITY DAILY DIARY

DAY-02
DATE- 24 June, 2025

Topics Covered:

- OSI model deep dive: understand 7 layers and map common protocols (HTTP, TCP, IP, Ethernet) to layers.

What did I learn:

Today I took a deep dive into the **OSI (Open Systems Interconnection) model**, the backbone of how data moves across networks. Understanding its **7 layers** helped me see how each part of a communication system plays a distinct role—from user-facing applications to physical transmission.

- I learned how the **Application Layer (Layer 7)** handles protocols like **HTTP**, which powers web browsing and API calls.
- The **Transport Layer (Layer 4)** introduced me to **TCP**, which ensures reliable delivery of packets—crucial for tools like Wireshark when analyzing retransmissions or dropped packets.
- The **Network Layer (Layer 3)** is where **IP** lives, routing packets across networks. This is the layer I'll be working with heavily during my network analysis project.
- The **Data Link Layer (Layer 2)** includes **Ethernet**, which defines how data frames are sent over physical media—important when I simulate LAN traffic or inspect MAC addresses.
- I also explored the **Physical Layer (Layer 1)**, which deals with actual cables and signals—less relevant for virtual labs, but vital for understanding real-world setups.

Mapping protocols to layers gave me clarity on how tools like Kali Linux, Wireshark, and NetFlow interact with different parts of the stack. It's like seeing the gears behind the machine—each layer has its own job, and together they make secure, efficient communication possible.

This knowledge will directly feed into my cybersecurity training and lab design. Whether I'm capturing packets, spoofing addresses, or analyzing traffic flows, knowing where each protocol fits helps me troubleshoot smarter and build more realistic simulations.