CYBERSECURITY DAILY DIARY

DAY-13
DATE- 5 July, 2025

Topics Covered:

- TCP troubleshooting with packet capture
- Identify retransmits, latency and sequence/ack behavior.

What did I learn:

Today I dove into **TCP troubleshooting** using packet captures in Wireshark. This session helped me understand how to diagnose network issues by analyzing retransmissions, latency, and sequence/ack behavior—skills that are vital for my cybersecurity lab and network analysis project.

🔹 **Retransmissions**

- I learned how TCP handles **packet loss** by retransmitting unacknowledged segments.
- In Wireshark, I used the filter `tcp.analysis.retransmission` to spot repeated sequence numbers and delays.
- Retransmits often signal **congestion, unstable links, or firewall interference**—important clues when analyzing attack simulations or performance issues.

🔹 **Latency (Round-Trip Time)**

- I measured **RTT** using `tcp.analysis.ack_rtt`, which shows how long it takes for a packet to be acknowledged.
- High RTT values helped me identify **slow paths or overloaded nodes**, which could affect real-time applications or reveal bottlenecks in my lab setup.

🔹 **Sequence and ACK Behavior**

- I tracked **TCP sequence numbers** to understand how data flows and how acknowledgments confirm receipt.
- Watching the **ACK numbers increment** gave me insight into throughput and flow control.
- I also spotted **out-of-order packets**, which can indicate routing issues or aggressive scanning behavior.

This hands-on troubleshooting sharpened my ability to interpret packet flows, detect anomalies, and simulate realistic traffic in my lab. It also prepares me to document TCP behavior in my network analysis report and explain how attackers might exploit or disrupt these flows.