CYBERSECURITY DAILY DIARY

DAY-09
DATE- 1 July, 2025

Topics Covered:

- DHCP & DORA: capture DHCP traffic
- Identify Discover/Offer/Request/Ack packets using Wireshark.

What did I learn:

Today I explored how **DHCP (Dynamic Host Configuration Protocol)** assigns IP addresses dynamically, and how the **DORA process** unfolds during client-server communication. Capturing this traffic in Wireshark gave me a clear view of how devices join a network.

- I learned the **DORA sequence**:
  - **Discover**: The client broadcasts a request for IP configuration.
  - **Offer**: The DHCP server responds with an available IP and configuration details.
  - **Request**: The client formally requests the offered IP.
  - **Ack**: The server acknowledges and finalizes the lease.
- Using **Wireshark**, I filtered traffic with `bootp` and `dhcp` to observe each packet in the sequence. Seeing the MAC address in the Discover and the offered IP in the Offer helped me understand how DHCP works at Layer 2 and Layer 3.
- I noted how DHCP uses **UDP ports 67 (server) and 68 (client)**, and how broadcast messages play a role in reaching the server before the client has an IP.
- I also learned how **DHCP spoofing** can be a threat—an attacker could respond with fake Offers and redirect traffic. Tools like DHCP snooping and port security help mitigate this.

This hands-on capture helped me connect theory to practice. Now I can interpret DHCP flows, troubleshoot IP assignment issues, and simulate DHCP behavior in my cybersecurity lab.