CYBERSECURITY DAILY DIARY

DAY-14
DATE- 6 July, 2025

Topics Covered:

- Weekly review & documentation: write a lab report for DHCP capture
- ARP analysis and routing observations.

What did I learn:

This week felt like peeling back the layers of how devices talk, listen, and find their way across networks. I didn't just capture packets—I captured behavior, trust, and strategy.

🔹 **DHCP – DORA in Action**

I watched the **DORA dance** unfold in Wireshark:

- **Discover**: My VM shouted into the void, asking for an IP.
- **Offer**: The DHCP server replied with a lease proposal.
- **Request**: The VM accepted the offer.
- **Ack**: The server sealed the deal.

Seeing this in real time helped me understand how devices join networks and how attackers might sneak in with rogue DHCP replies. I now know how to filter `bootp` traffic and interpret lease details like subnet mask and gateway.

🔹 **ARP – Trust Without Verification**

ARP felt like a handshake with no ID check. I used `arp -a` to inspect the cache and saw how IPs map to MACs. In Wireshark, I filtered `arp` and watched:

- Broadcast requests: "Who has 192.168.1.5?"
- Unicast replies: "I do—here's my MAC."

It's elegant but vulnerable. ARP spoofing is real, and I'm planning to simulate it soon. This protocol taught me how trust at Layer 2 can be exploited—and how to spot it.

🔹 **Routing – Paths and Decisions**

I explored routing tables with `ip route show` and ran `traceroute google.com`. Each hop revealed:

- Gateway decisions
- RTT delays

- Possible bottlenecks

Static routes felt like hand-drawn maps. Dynamic routing? Like GPS with live traffic. I now understand how packets choose their path—and how I can trace or manipulate that path in my lab.

This week wasn't just technical—it was strategic. I saw how DHCP assigns identity, how ARP builds trust, and how routing defines movement. These are the foundations of network behavior, and now I can analyze, simulate, and secure them.