CYBERSECURITY DAILY DIARY

DAY-08
DATE- 30 June, 2025

Topics Covered:

- ARP & MAC: observe ARP cache
- Learn ARP request/reply and risks of ARP spoofing.

What did I learn:

Today I explored the relationship between **ARP (Address Resolution Protocol)** and **MAC (Media Access Control) addresses**, which are essential for local network communication and a common target in cybersecurity attacks.

- I learned how **ARP maps IP addresses to MAC addresses** so devices on the same network can communicate. It's like asking, "Who has this IP?" and getting back, "I do—here's my MAC."
- I observed the **ARP cache** using commands like `arp -a`, which shows a table of IP-to-MAC mappings stored temporarily by the system.
- I studied the **ARP request/reply process**:
  - **Request**: A broadcast asking "Who has 192.168.1.5?"
  - **Reply**: The device with that IP responds with its MAC address.
- I discovered the risks of **ARP spoofing**, where an attacker sends fake ARP replies to poison the cache. This can redirect traffic, enable man-in-the-middle attacks, or disrupt communication.
- Tools like **Wireshark** can help detect suspicious ARP traffic, and techniques like **static ARP entries** or **dynamic ARP inspection** can help defend against spoofing.

This knowledge strengthens my ability to analyze local traffic, detect anomalies, and simulate attacks in my cybersecurity lab. It also prepares me to document ARP behavior in my network analysis project and explain how attackers exploit trust at the data link layer.