CYBERSECURITY DAILY DIARY

DAY-04
DATE- 26 June, 2025

Topics Covered:

- IPv4 addressing basics: binary/decimal conversion
- Network vs host identification.

What did I learn:

Today I explored the building blocks of **IPv4 addressing**, a critical skill for network analysis and cybersecurity. Understanding how IP addresses work helps me interpret traffic, configure subnets, and detect anomalies in packet captures.

- I practiced **binary-to-decimal conversion** and vice versa. For example, the IP address `192.168.1.1` converts to binary as `11000000.10101000.00000001.00000001`. This skill is essential when analyzing subnet masks and CIDR notation.
- I learned how each IPv4 address is split into two parts:
  - The **network portion** identifies the subnet or group of devices.
  - The **host portion** identifies the specific device within that network.
- Using subnet masks like `255.255.255.0`, I saw how the first 24 bits (`/24`) represent the network, and the last 8 bits represent the host.
- I also explored how **CIDR notation** (e.g., `192.168.1.0/24`) simplifies network planning and helps define address ranges.
- This knowledge will help me configure virtual networks in my lab, analyze routing tables, and understand how firewalls and NAT devices handle traffic.

It’s empowering to decode IP addresses and see the logic behind how devices communicate. This will be a core skill when I start mapping traffic flows and identifying threats in my cybersecurity project.