CYBERSECURITY DAILY DIARY

DAY-10
DATE- 2 July, 2025

Topics Covered:

- NAT & PAT overview: private vs public addressing and port translation basics

- Optional ip tables simulation.

What did I learn:

Today I explored **Network Address Translation (NAT)** and **Port Address Translation (PAT)**—two techniques that allow devices with private IPs to communicate over the public internet. This is essential for building scalable, secure networks in both real-world and lab environments.

- I learned the difference between **private and public IP addressing**:
  - **Private IPs** (e.g., `192.168.x.x`, `10.x.x.x`) are used inside local networks and are not routable on the internet.
  - **Public IPs** are globally unique and assigned by ISPs for internet-facing communication.
- **NAT** translates private IPs to a public IP at the router level, allowing internal devices to access the internet while hiding their true addresses.
- **PAT** (a form of NAT) goes further by translating **both IP and port numbers**, enabling multiple devices to share a single public IP. It's like multiplexing—each session gets a unique port.
- I reviewed how NAT/PAT helps with:
  - **Security**: Internal IPs stay hidden.
  - **Scalability**: Thousands of devices can share one public IP.
  - **Session tracking**: PAT uses port numbers to keep track of who's talking to whom.

I optionally simulated NAT behavior using **ip tables** in Kali:
bash

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

- This command enables PAT by masquerading outgoing traffic from internal VMs—perfect for testing outbound connections in my lab.

Understanding NAT and PAT helps me design realistic network topologies, troubleshoot connectivity issues, and prepare for firewall and routing configurations in my cybersecurity training.