CYBERSECURITY DAILY DIARY

DAY-12
DATE- 4 July, 2025

Topics Covered:

- Switching & VLANs: VLAN tagging basics and segmentation use-cases (simulate in virtual network if possible).

What did I learn:

Today I explored the fundamentals of **network switching** and **VLANs (Virtual Local Area Networks)**, which are essential for segmenting traffic and enhancing security in both physical and virtual environments.

🔹 **Switching Basics**

- I learned how **network switches** operate at Layer 2 of the OSI model, forwarding frames based on **MAC addresses**.
- Unlike hubs, switches create **dedicated paths** between devices, reducing collisions and improving performance.

🔹 **VLAN Tagging**

- VLANs allow logical segmentation of networks, even across the same physical switch.
- I studied **802.1Q tagging**, where a VLAN ID is inserted into Ethernet frames to identify which VLAN the traffic belongs to.
- VLAN tags help switches route traffic to the correct segment, maintaining isolation between departments, roles, or lab zones.

🔹 **Segmentation Use-Cases**

- In my lab, I can simulate VLANs to:
  - Isolate attacker and victim VMs for penetration testing.
  - Separate monitoring tools like Wireshark from active traffic zones.
  - Create secure zones for DNS, DHCP, and firewall testing.
- This segmentation reduces broadcast traffic and enhances security by limiting lateral movement during simulated attacks.

🔹 **Virtual Simulation**

- Using **VirtualBox internal networks** or **GNS3/VMware Workstation**, I can assign VMs to different VLANs and simulate tagged traffic.

- I plan to use **iptables and bridge-utils** to route traffic between VLANs and monitor behavior during spoofing or scanning exercises.

Understanding VLANs gives me control over traffic flow and security boundaries. It’s a powerful tool for building realistic, scalable lab environments that mirror enterprise-grade networks.