CYBERSECURITY DAILY DIARY

DAY-19
DATE- 11 July, 2025

Topics Covered:

- Install Wireshark: ensure capture permissions
- capture lab traffic between VMs

What I Did Today

Installing Wireshark is simple with `sudo apt install wireshark`, but capturing packets as a non-root user requires extra steps. You need to:

- Reconfigure permissions with `sudo dpkg-reconfigure wireshark-common` and select "Yes" to allow non-root captures.
- Add your user to the `wireshark` group using `sudo usermod -aG wireshark $USER`, then reboot or log out/in to apply changes.

Capture Permissions Matter because without them, Wireshark won't detect interfaces or allow live packet capture unless run as root — which isn't ideal for security or usability.

Capturing Lab Traffic Between VMs showed how much background communication happens even when systems seem idle:

- ARP requests for MAC address resolution
- DHCP traffic during IP lease negotiation
- ICMP pings and service discovery packets
- TCP handshakes when services like SSH or HTTP are accessed

Filters are Essential to make sense of the noise. Using expressions like:

- `ip.addr == 192.168.56.101` to isolate traffic from a specific VM
- `tcp.port == 22` to focus on SSH
- `icmp` to monitor ping activity helped narrow down the view and analyze meaningful interactions.

Seeing Protocols in Action — like the three-way TCP handshake or DNS query/response — made abstract networking concepts feel real and visual. It's one thing to read about them, another to watch them unfold packet by packet.