CYBERSECURITY DAILY DIARY

DAY-21
DATE- 13 July, 2025

Topics Covered:

- Consolidation lab: correlate nmap scans with Wireshark captures and write analysis.

What I Did Today

Nmap and Wireshark complement each other beautifully — Nmap reveals what's open and reachable, while Wireshark shows how those services behave in real time.

Correlating SYN scans (`-sS`) with Wireshark:

- Nmap sends SYN packets to probe ports.
- In Wireshark, I saw matching SYN requests and SYN-ACK responses from the target — confirming open ports.
- Closed ports responded with RST, which also appeared in the capture.

TCP Connect scans (`-sT`) showed full handshakes:

- Nmap completed the three-way handshake.
- Wireshark displayed SYN → SYN-ACK → ACK clearly, followed by immediate RST from Nmap to close the connection.

UDP scans (`-sU`) were harder to track:

- Nmap sent UDP probes.
- Wireshark showed some ICMP "port unreachable" replies — indicating closed ports.
- Open or filtered ports had no response, which matched Nmap's ambiguous results.

OS Detection (`-O`) triggered unique packet patterns:

- Wireshark revealed TCP packets with unusual flags and TTL values — part of Nmap's fingerprinting technique.
- These helped Nmap guess the OS based on how the target responded.

Timing options (`-T4`) affected packet frequency:

- With aggressive timing, Wireshark showed rapid bursts of packets.
- Slower timing (`-T2`) resulted in more spaced-out traffic — useful for stealth.

Analysis Takeaway:

- Watching Nmap's behavior in Wireshark deepened my understanding of how scans work under the hood.
- It's one thing to run a scan and read the output — it's another to *see* the packets fly and *feel* the network react.
- This lab bridged theory and practice — and made me more confident in interpreting both scan results and packet flows.