CYBERSECURITY DAILY DIARY

DAY-18
DATE- 10 July, 2025

Topics Covered:

- nmap techniques: practice SYN (-sS)
- TCP connect (-sT), UDP (-sU), OS detection (-O), and timing options.

What I Did Today

- **SYN Scan (`-sS`)** This is Nmap's default and most popular scan. It sends a SYN packet (like knocking on a door) and listens for a response. If it gets SYN-ACK, the port is open. It never completes the handshake, making it stealthy and fast — ideal for initial recon without alerting firewalls or intrusion detection systems.
- **TCP Connect Scan (`-sT`)** This scan completes the full TCP handshake (SYN → SYN-ACK → ACK), so it's more detectable. It's used when you don't have root privileges or raw socket access. Reliable, but noisier — think of it as ringing the doorbell instead of just tapping the window.
- **UDP Scan (`-sU`)** UDP is connectionless, so scanning is trickier. No handshake means Nmap relies on ICMP "port unreachable" messages to infer closed ports. If there's no response, the port might be open or filtered. It's slow and often inconclusive, but essential for discovering services like DNS, SNMP, or TFTP.
- **OS Detection (`-O`)** Nmap analyzes subtle differences in TCP/IP stack behavior — like how a system responds to malformed packets — to guess the operating system. It works best with multiple open ports and root access. Results can be fuzzy, but it's a powerful fingerprinting tool when combined with service detection (`-sV`).
- **Timing Options (`-T0` to `-T5`)** These control how aggressive your scan is:
  - `-T0`: paranoid — super slow, avoids detection
  - `-T3`: default — balanced
  - `-T4`: aggressive — fast, good for LAN
  - `-T5`: insane — fastest, but likely to trigger alarms Choosing the right timing helps balance stealth and speed, especially in live environments.