CYBERSECURITY DAILY DIARY

DAY-17
DATE- 9 July, 2025

Topics Covered:

- Install nmap and verify: run basic scans and save outputs.

What I Did Today

- Installed Nmap using `sudo apt install nmap -y`
- Verified installation with `nmap --version` — confirmed version 7.94
- Ran basic scans:
  - `nmap -sn 192.168.1.0/24` for ping sweep
  - `nmap 192.168.1.10` for default port scan
  - `nmap -sV 192.168.1.10` for service version detection
  - `sudo nmap -O 192.168.1.10` for OS fingerprinting
- Saved outputs in `.txt`, `.xml`, and `.grep` formats using `-oN`, `-oX`, and `-oG` flags

What I Learned

- Nmap's output formats are versatile — `.xml` is great for parsing, `.grep` for quick filtering
- OS detection requires root privileges and isn't always precise — good reminder to cross-check
- Even basic scans reveal a lot about a target — ports, services, uptime, and more

What Challenged Me

- Remembering the right flags for output formats
- Interpreting ambiguous OS detection results
- Staying focused while waiting for scans to complete — tempted to multitask