Cyber Security Internship — Task 1 (Steps 1–8)

1) Install Nmap

- Windows: Download installer from nmap.org
- macOS: brew install nmap
- Linux (Debian/Ubuntu): sudo apt update && sudo apt install nmap -y
- Verify: nmap --version

2) Find your local IP range (subnet)

- Windows: ipconfig
- macOS/Linux: ip a or ifconfig
- Typical range: 192.168.1.0/24

3) Run TCP SYN scan

Basic: nmap -sS 192.168.1.0/24 -oN nmap_results.txt
Verbose: sudo nmap -sS -sV -O 192.168.1.0/24 -oN nmap_results_verbose.txt

4) Note down IP addresses & ports

Record results in format:
Host: 192.168.1.12
Status: up
Open ports: 22/tcp ssh, 80/tcp http, 443/tcp https

5) (Optional) Wireshark capture

- Start Wireshark capture
- Run scan simultaneously
- Use filters like ip.addr==192.168.1.12 or tcp.flags.syn==1 && tcp.flags.ack==1
- Save as .pcapng

6) Research services

Common ports:
22=SSH, 80=HTTP, 443=HTTPS, 135/139/445=Windows SMB, 3389=RDP, 53=DNS

7) Identify potential security risks

- Ask: Is service needed? Exposed? Outdated?
- Examples:
  * 445/tcp SMB → risk: lateral movement → fix: disable SMBv1/firewall
  * 3389/tcp RDP → risk: brute-force → fix: restrict to VPN/firewall

8) Save results

- Save txt: nmap -sS 192.168.1.0/24 -oN nmap_results.txt
- Save XML: nmap -sS 192.168.1.0/24 -oX nmap_results.xml
- Convert to HTML: xsltproc nmap.xsl nmap_results.xml > nmap_results.html