Cybersecurity Internship - Task 1

Objective: Scan local network for open ports and analyze exposure.

------------------------------------------------------------

Step 1: Install Nmap from official website

I installed Nmap from the official site

On Windows, I ran the installer and accepted the default options, including Npcap.

After installation I verified with:

nmap --version

Result: Nmap version 7.98 installed successfully.

------------------------------------------------------------

Step 2: Find your local IP range

Using 'ipconfig', my IPv4 Address = 192.168.56.1 and Subnet Mask = 255.255.255.0.

Therefore, my local network range is: 192.168.56.0/24.

------------------------------------------------------------

Step 3: Run Nmap SYN Scan

Command run:

nmap -sS 192.168.56.0/24

Result:

Host 192.168.56.1 is up.

Open ports: 135, 139, 445, 3580

------------------------------------------------------------

Step 4: Note down IP addresses and open ports.

Host: 192.168.56.1

Open Ports:

- 135/tcp — msrpc

- 139/tcp — netbios-ssn

- 445/tcp — microsoft-ds

- 3580/tcp — nati-svrloc

------------------------------------------------------------

Step 5: Optional Wireshark Analysis

I optionally used Wireshark during the scan.

Observed SYN → SYN/ACK packets confirming the open ports.

------------------------------------------------------------

Step 6: Research common services running on those ports

135/tcp (msrpc) — Windows RPC service for remote procedure calls.

Risk: Could be exploited for remote code execution if unpatched.

Mitigation: Keep system updated, restrict RPC access.

139/tcp (netbios-ssn) — Legacy Windows networking service.

Risk: Can leak system information and allow lateral movement.

Mitigation: Disable NetBIOS if not needed.

445/tcp (microsoft-ds) — SMB file sharing service.

Risk: Known target for ransomware and worms (e.g., EternalBlue).

Mitigation: Patch OS, disable SMBv1, restrict access.

3580/tcp (nati-svrloc) — NAT service location (uncommon).

Risk: Unknown, may expose vulnerabilities.

Mitigation: Investigate the application and disable if unnecessary.

------------------------------------------------------------

Step 7: Identify potential security risks

- Port 445 (SMB): High risk. Needs patching and restricted access.

- Port 139 (NetBIOS): Medium risk. Disable if unused.

- Port 135 (RPC): Medium risk. Ensure updates and access control.

- Port 3580: Unknown risk. Investigate and restrict if not required.

------------------------------------------------------------

Step 8: Save scan results

Commands used:

nmap -sS -sV -T4 192.168.56.0/24 -oN scan\_results.txt

nmap -sS -sV -T4 192.168.56.0/24 -oX scan\_results.xml

The output file 'scan\_results.txt' contains the full scan results.

------------------------------------------------------------

Final Notes:

- Task completed successfully.

- All scans were performed on my own local network.