Ministry of MSME, Govt. of India

Task 1 – Scan Local Network for Open Ports using Nmap

Objective: To perform a basic network reconnaissance scan using Nmap to identify devices and open ports on the local network, understand which services are exposed, and assess potential security risks.

Tools Used:

• Nmap v7.97 (installed via Homebrew on macOS)
• Terminal (macOS)

Target Network:
• IP Range Scanned: 192.168.152.0/24
• Device IP Identified: 192.168.152.209

Command Executed:

nmap 192.168.152.0/24 -oN scan_results.txt

Output Summary:

```
# Nmap 7.97 scan initiated Mon Aug 4 14:21:58 2025 as: nmap -oN scan_results.txt
192.168.152.0/24
Nmap scan report for 192.168.152.209 Host is up
(0.000039s latency).
Not shown: 998 closed tcp ports (conn-refused) PORT STATE
SERVICE
5000/tcp open upnp
7000/tcp open afs3-fileserver

# Nmap done at Mon Aug 4 14:23:48 2025 -- 256 IP addresses (1 host up) scanned in
109.57 seconds
```

Screenshot of Nmap Output:

```
sarfarajahamed@sarfarajs-MacBook-Air Desktop % cat scan_results.txt

# Nmap 7.97 scan initiated Mon Aug  4 14:21:58 2025 as: nmap -oN scan_results.txt 192.168
.152.0/24
Nmap scan report for 192.168.152.209
Host is up (0.000039s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
5000/tcp open  upnp
7000/tcp open  afs3-fileserver

# Nmap done at Mon Aug  4 14:23:48 2025 -- 256 IP addresses (1 host up) scanned in 109.57
 seconds
sarfarajahamed@sarfarajs-MacBook-Air Desktop %
```

Name: Sarfaraj Ahamed

Observation: The local network scan detected 1 active host (192.168.152.209) with two open TCP ports (5000 and 7000). These ports may indicate UPnP and AFS3 file server services.
Further investigation or firewall restrictions may be required to secure these services.

Name: Sarfaraj Ahamed