Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap, Wireshark

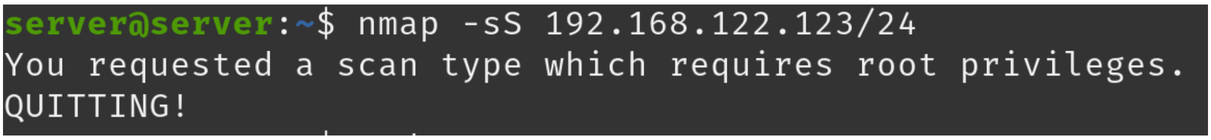
Steps:

1. Install Nmap in Linux System

   $ sudo apt install nmap

2. Giving root privileges for the Nmap scan

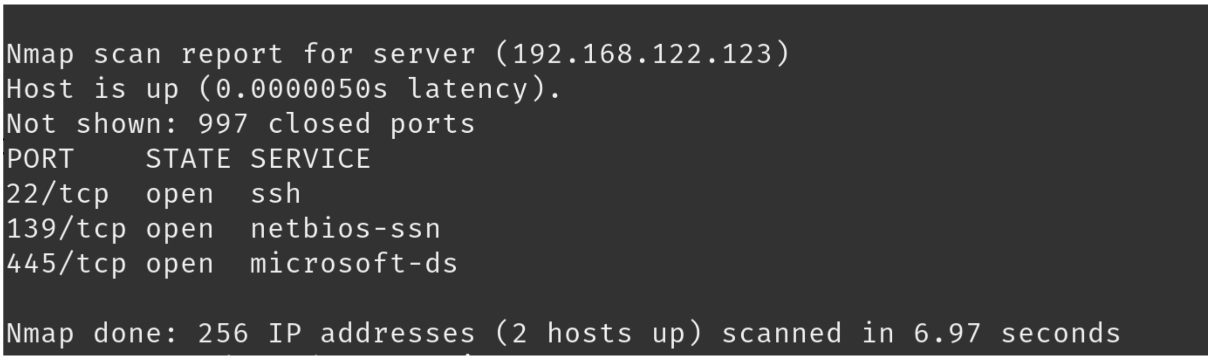
   $ sudo su



```
server@server:~$ nmap -sS 192.168.122.123/24
You requested a scan type which requires root privileges.
QUITTING!
```

3. Nmap scan

   nmap -sS 192.168.122.123/24



```
Nmap scan report for server (192.168.122.123)
Host is up (0.0000050s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 256 IP addresses (2 hosts up) scanned in 6.97 seconds
```

4. Open TCP Ports:

`22/tcp` – SSH

`139/tcp` – NetBIOS Session Service

`445/tcp` – Microsoft Directory Services (SMB)

5. Potential Security risks

22 - Susceptible to brute-force attacks, credential reuse, or outdated SSH daemons

139 - Vulnerable to NetBIOS-related exploits or information disclosure

445- Common target for ransomware (e.g., WannaCry), SMB exploits (EternalBlue)

6. Mitigation Suggestions

- Restrict access to SSH using a firewall (`ufw`, `iptables`)
- Use SSH keys, disable root login and password auth
- Disable SMBv1 if not needed; patch against SMB vulnerabilities
- Use network segmentation and VPNs for file sharing