Task – 1 Submission

Objective:

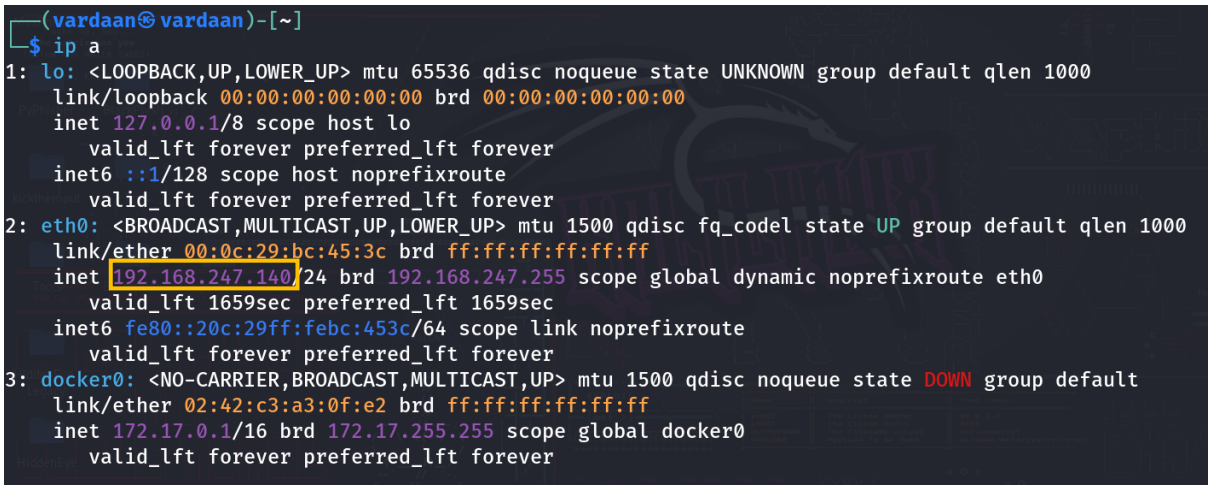
Learn to discover open ports on devices in your local network to understand network exposure.

Tools:

Nmap, Kali Linux

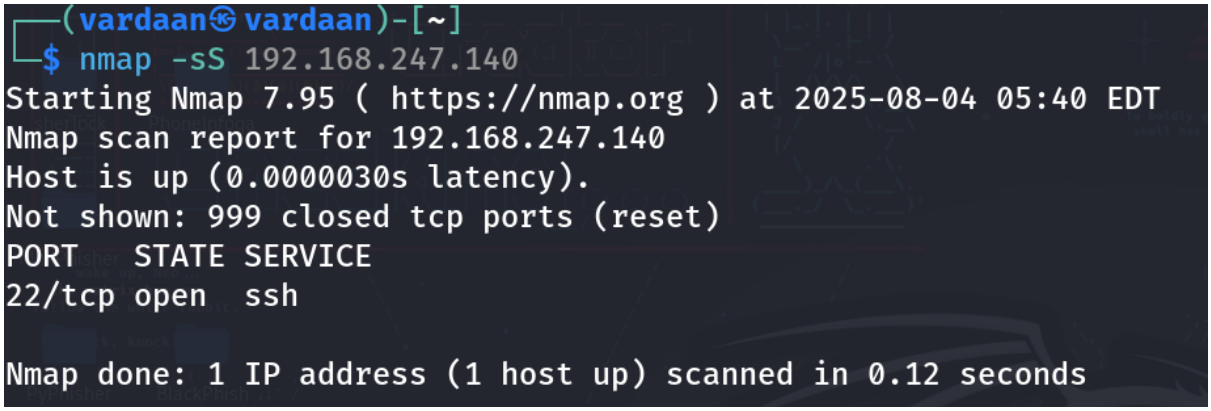
Procedure:

- Ip of my kali virtual machine –



IP of my kali virtual machine is 192.168.247.140

- Performing -sS Stealth Scan using Nmap tool



- Performing -sS Stealth Scan on whole subnet

```
┌──(vardaan㉿vardaan)-[~]
└─$ nmap -sS 192.168.247.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 05:41 EDT
Nmap scan report for 192.168.247.1
Host is up (0.0051s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.247.2
Host is up (0.00017s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EB:1E:3F (VMware)

Nmap scan report for 192.168.247.254
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.247.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F2:F4:A4 (VMware)

Nmap scan report for 192.168.247.140
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.43 seconds
```

- Performing TCP scan on my kali machine

```
┌──(vardaan㉿vardaan)-[~]
└─$ nmap -sT 192.168.247.140
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 05:43 EDT
Nmap scan report for 192.168.247.140
Host is up (0.00011s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

- Performing TCP Comprehensive Scan

```
┌──(vardaan㉿vardaan)-[~]
└─$ sudo nmap -p- -sS -T4 192.168.247.140
[sudo] password for vardaan:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 05:44 EDT
Nmap scan report for 192.168.247.140
Host is up (0.0000030s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
1716/tcp open  xmsg
```

- -p- scans all 65535 ports
- -sS uses SYN scan (requires root)
- -T4 sets aggressive timing template

- Scanning for all open ports

```
┌──(vardaan㉿vardaan)-[~]
└─$ nmap -p- 192.168.247.140
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 05:46 EDT
Nmap scan report for 192.168.247.140
Host is up (0.0000030s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
1716/tcp open  xmsg

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

Result:

We found only two ports open in the machine and that is ssh (Port 22) and xmsg (Port 1716)

Details of the open ports:

SSH: Secure Shell (SSH) is used for secure remote administration. While essential for management, an exposed SSH service can be targeted by brute-force attacks if weak credentials are used. Ensure strong passwords, key-based authentication, and firewall restrictions to trusted IPs.

XMSG: XMSG is often associated with messaging services or specific applications (e.g., Xplico for network analysis). If this service is unexpected, it may indicate unauthorized software or misconfiguration. Verify its purpose and restrict access if unnecessary.

Potential Risk of the open ports:

1. **SSH (Port 22):**

   - Brute-Force Attacks: Exposed SSH ports are prime targets for automated login attempts. Attackers may use tools like Hydra or Metasploit to guess weak credentials.
   - Vulnerable SSH Versions: Outdated SSH implementations may contain unpatched exploits (e.g., CVE-2023-38408 for remote code execution).
   - Privilege Escalation: If default or weak credentials (e.g., admin:admin, root:password) are used, attackers can gain full system control.
   - Man-in-the-Middle (MITM) Attacks: If SSH encryption is misconfigured, session hijacking may occur.

2. **XMSG (Port 1716):**

   - **Unknown Service Exposure:** XMSG is not a standard port—could indicate:

     a. A custom/obscure messaging service with unpatched vulnerabilities.
     b. A backdoor or malware communication channel (e.g., botnet C2 server).

   - **Data Leakage Risk:** If XMSG handles sensitive data, lack of encryption may expose it to sniffing.
   - **Exploitable Vulnerabilities:** If running outdated software (e.g., Xplico, if applicable), it may be susceptible to RCE or DoS attacks.