

Task 1: Scan Your Local Network for Open Ports

After scanning my local network using the TCP SYN scan (Nmap -sS), I identified **three open TCP ports** on one of the devices in my network. These open ports correspond to specific services running on that machine. Below is a breakdown of the ports and their associated services:

Port	State	Services
902	Open	iss-realsecure
912	Open	apex-mesh
5357	Open	wsdapi

1. Port 902 – VMware Service (iss-realsecure)

This port is usually used by **VMware**, a software for running virtual machines (like running Windows inside Linux). If this service is active, it means the device might be set up for managing virtual machines remotely.

➔ **Why it matters:** If you're not using VMware, this open port might be unnecessary and should be closed to prevent outsiders from trying to exploit it.

2. Port 912 – Unknown or Custom Service (apex-mesh)

This one is a bit of a mystery. It doesn't belong to any common service, which could mean it's used by **custom software**, an **IoT device**, or something that was installed manually.

➔ **Why it matters:** Unknown services can be **risky**, especially if you're not sure what they do. Hackers often look for these to find a way into your system.

➔ **What to do:** I would check what app is using it and turn it off if it's not needed.

3. Port 5357 – Windows Device Discovery (wsdapi)

This port is used by **Windows to find other devices** on the network like printers or scanners. It's part of something called "Web Services for Devices."

➔ **Why it matters:** This port is usually safe **inside a home network** but shouldn't be open on public networks because it can reveal device information.

What I Learned

➔ Every open port represents a **service or feature** running on a device.

➔ Some of them are important, others might be unnecessary or even dangerous.

- ➔ Tools like **Nmap** help you **see what's exposed** on your network so you can protect it.
- ➔ Keeping track of open ports helps improve your **network security** by closing or restricting the ones you don't need.

```
(brijesh@Hacker)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.245.128 netmask 255.255.255.0 broadcast 192.168.245.255
    inet6 fe80::20c:29ff:fe4a:177a prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:4a:17:7a txqueuelen 1000 (Ethernet)
    RX packets 1052 bytes 74549 (72.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5581 bytes 344318 (336.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2008 bytes 84480 (82.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2008 bytes 84480 (82.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(brijesh@Hacker)-[~]
$ nmap -sS 192.168.245.128/24 -oN scan_results.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 17:07 IST
Nmap scan report for 192.168.245.1
Host is up (0.0043s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.245.2
Host is up (0.00010s latency).
```

```
(brijesh@Hacker)-[~]
$ nmap -sS 192.168.245.128/24 -oN scan_results.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 17:07 IST
Nmap scan report for 192.168.245.1
Host is up (0.0043s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.245.2
Host is up (0.00010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:F1:15:54 (VMware)

Nmap scan report for 192.168.245.254
Host is up (0.00022s latency).
All 1000 scanned ports on 192.168.245.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E1:55:88 (VMware)

Nmap scan report for 192.168.245.128
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.245.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.89 seconds

(brijesh@Hacker)-[~]
$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  scan_results.txt  Templates  Videos
```

```
(brijesh@Hacker)-[~]
$ cd Desktop

(brijesh@Hacker)-[~/Desktop]
$ ls
scan_results.txt

(brijesh@Hacker)-[~/Desktop]
$ cat scan_results.txt
# Nmap 7.95 scan initiated Mon Jun 23 16:50:58 2025 as: /usr/lib/nmap/nmap --privileged -sS -oN scan_results.txt 192.168.245.1
28/24
Nmap scan report for 192.168.245.1
Host is up (0.00097s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
5357/tcp   open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.245.2
Host is up (0.000093s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:F1:15:54 (VMware)

Nmap scan report for 192.168.245.254
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.245.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E1:55:88 (VMware)

Nmap scan report for 192.168.245.128
Host is up (0.000030s latency)
```