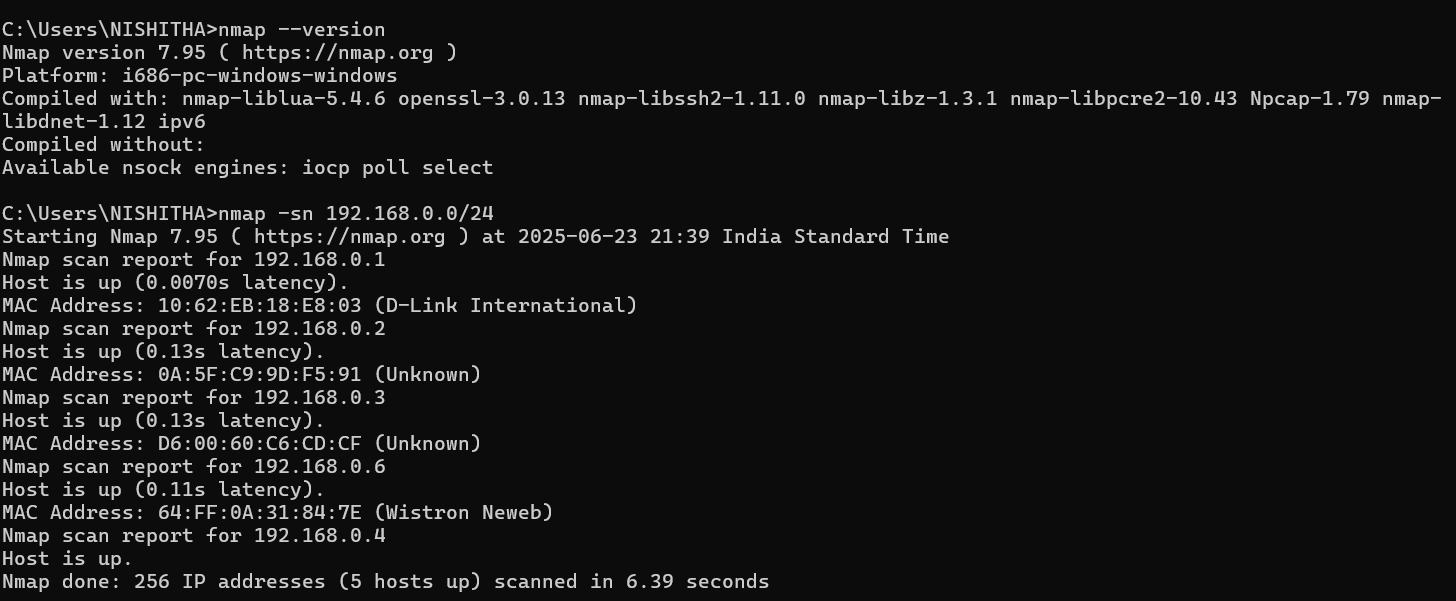
PORT SCANNING USING NMAP AND WIRESHARK

1. **Install Nmap from the official website.**

**Downloaded and Installed Nmap.**

1. **Find your local IP range (e.g., 192.168.1.0/24).**



After typing the command **'ipconfig'** in the terminal, the output shows:

IPv4 Address: 192.168.0.4

Subnet Mask: 255.255.255.0

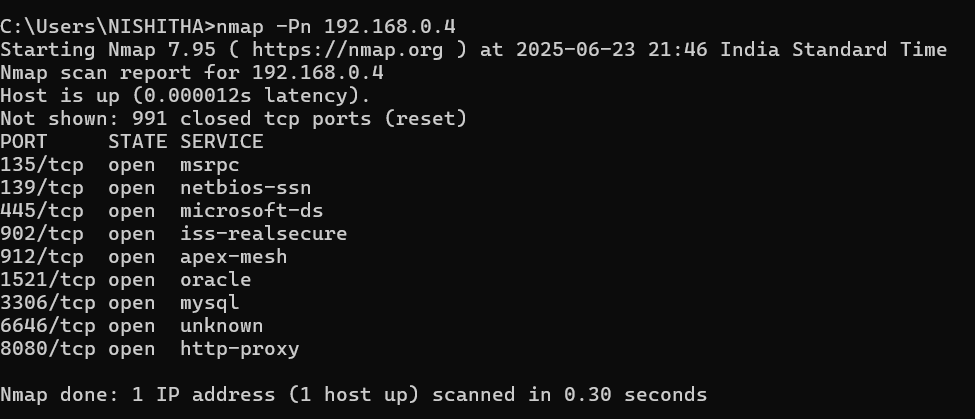
Based on this, the network range is 192.168.0.0/24.

Use the command 'nmap --version' to check if Nmap is correctly installed.

Run 'nmap -sn 192.168.0.0/24' to identify live hosts on the network.

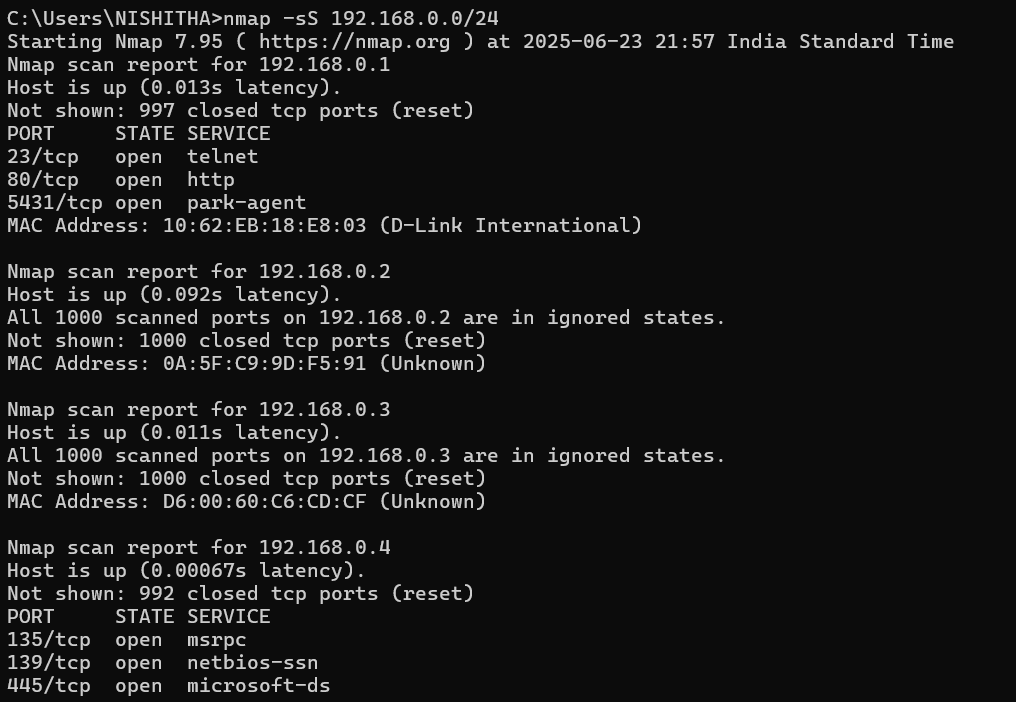
**3. Trying to ping one device:**

Normally, you can use 'nmap -sV IPAddress' to detect services on a device. However, if a firewall is blocking pings, use 'nmap -Pn IPAddress' instead.



**4. Run: 'nmap -sS 192.168.0.0/24' to perform a TCP SYN scan.**

This performs a TCP SYN handshake on each IP to detect open ports.



**5. Note down IP addresses and open ports found:**

For Device 1 (192.168.0.1):

- 23/tcp open (Telnet)

- 80/tcp open (HTTP)

- 5431/tcp open (park-agent)

For Device 2 (192.168.0.2):

- All ports are in ignored state (closed).

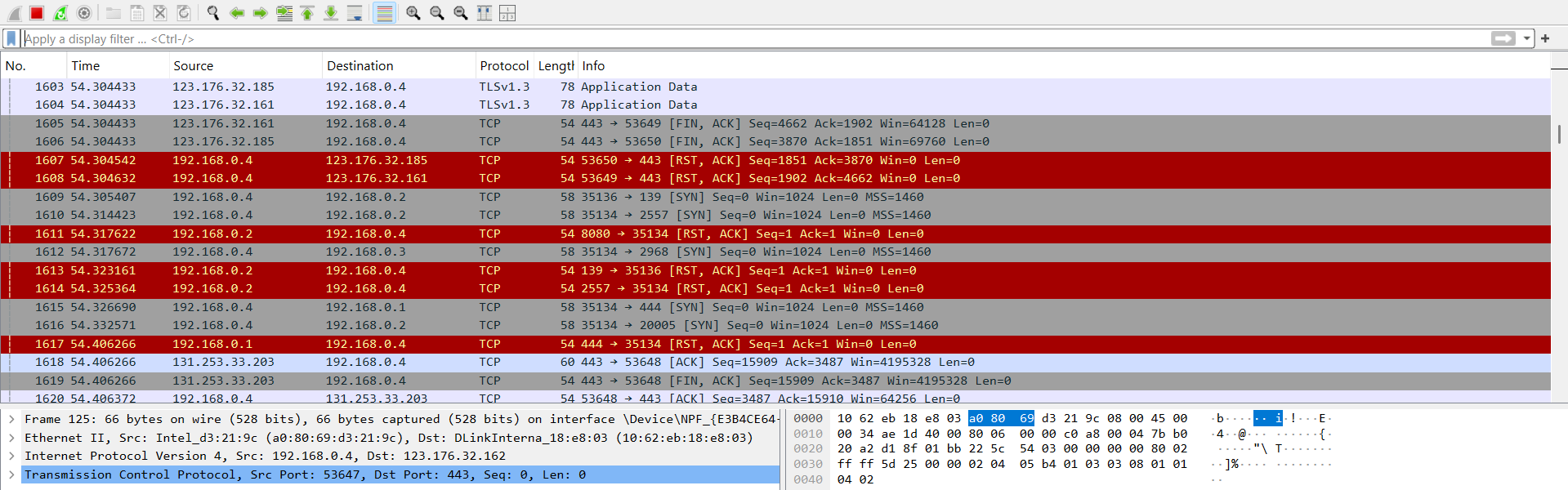
For Device 3 (192.168.0.3):

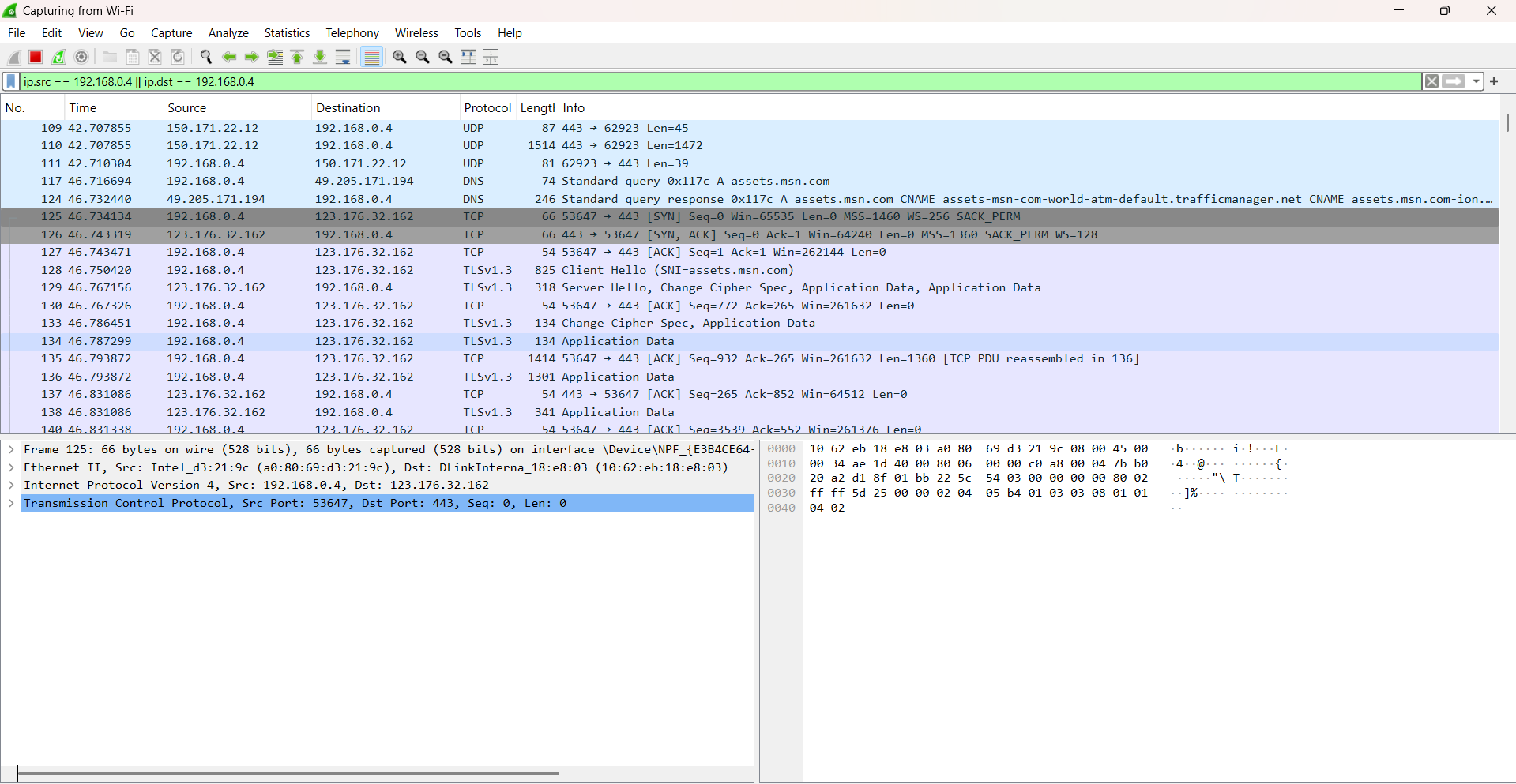
- All ports are in ignored state (closed).

For Device 4 (192.168.0.4):

- Multiple open ports detected. Vulnerabilities discussed below.

1. **Optionally analyze packet capture using Wireshark.**

****

****

* **Install Wireshark**  
  Download and install Wireshark from the official website ([https://www.wireshark.org/](https://www.wireshark.org/" \t "_new)). Ensure that **Npcap** is installed during setup.
* **Open Wireshark and Select Interface**  
  Launch Wireshark as Administrator. Choose the **active network interface** (e.g., Wi-Fi or Ethernet) from the list of available adapters.
* **Start Packet Capture**  
  Click the **blue shark fin icon** or double-click the interface to begin capturing live network traffic.
* **Run Nmap Scan**  
  In a separate terminal window, run a network scan such as:

·nmap -sS 192.168.0.0/24

* **Apply Wireshark Filters**  
  To focus on relevant packets, use filters like:

tcp.flags.syn == 1 && tcp.flags.ack == 0 → Show SYN packets from Nmap TCP scan

ip.src == 192.168.0.4 || ip.dst == 192.168.0.4 → Filter packets related to my device.

* **Analyze Results**  
  Observe how different devices respond:

**SYN-ACK** responses indicate open ports.

**RST** responses indicate closed ports.

These packets help map out the network's behavior.

**7. Research common services running on open ports:**

No common services are shared between the devices based on the scan.

**8. Identify potential security risks from open ports:**

- Ports 445 and 139: Used for Windows file sharing; highly vulnerable to ransomware and worms.

- Ports 3306 and 1521: Used by MySQL and Oracle databases; attackers might try default credentials to steal data.

1. **Save scan results as a text or HTML file.**

**Windows IP Configuration**

**Wireless LAN adapter Local Area Connection\* 3:**

**Media State . . . . . . . . . . . : Media disconnected**

**Connection-specific DNS Suffix . :**

**Wireless LAN adapter Local Area Connection\* 4:**

**Media State . . . . . . . . . . . : Media disconnected**

**Connection-specific DNS Suffix . :**

**Ethernet adapter VMware Network Adapter VMnet1:**

**Connection-specific DNS Suffix . :**

**Link-local IPv6 Address . . . . . : fe80::ebab:803:ad0c:aa7%36**

**IPv4 Address. . . . . . . . . . . : 192.168.213.1**

**Subnet Mask . . . . . . . . . . . : 255.255.255.0**

**Default Gateway . . . . . . . . . :**

**Ethernet adapter VMware Network Adapter VMnet8:**

**Connection-specific DNS Suffix . :**

**Link-local IPv6 Address . . . . . : fe80::882a:80f2:1fb9:7bad%38**

**IPv4 Address. . . . . . . . . . . : 192.168.182.1**

**Subnet Mask . . . . . . . . . . . : 255.255.255.0**

**Default Gateway . . . . . . . . . :**

**Wireless LAN adapter Wi-Fi:**

**Connection-specific DNS Suffix . : domain.name**

**Link-local IPv6 Address . . . . . : fe80::ae30:cf84:d88d:6f4%19**

**IPv4 Address. . . . . . . . . . . : 192.168.0.4**

**Subnet Mask . . . . . . . . . . . : 255.255.255.0**

**Default Gateway . . . . . . . . . : fe80::1262:ebff:fe18:e803%19**

**192.168.0.1**

**nmap --version**

**Nmap version 7.95 ( https://nmap.org )**

**Platform: i686-pc-windows-windows**

**Compiled with: nmap-liblua-5.4.6 openssl-3.0.13 nmap-libssh2-1.11.0 nmap-libz-1.3.1 nmap-libpcre2-10.43 Npcap-1.79 nmap-libdnet-1.12 ipv6**

**Compiled without:**

**Available nsock engines: iocp poll select**

**nmap --sn 192.168.0.0/24**

**nmap: unrecognized option `--sn'**

**See the output of nmap -h for a summary of options.**

**nmap -sn 192.168.0.0/24**

**Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-25 19:10 India Standard Time**

**Nmap scan report for 192.168.0.1**

**Host is up (0.025s latency).**

**MAC Address: 10:62:EB:18:E8:03 (D-Link International)**

**Nmap scan report for 192.168.0.2**

**Host is up (0.11s latency).**

**MAC Address: D6:00:60:C6:CD:CF (Unknown)**

**Nmap scan report for 192.168.0.4**

**Host is up.**

**Nmap done: 256 IP addresses (3 hosts up) scanned in 5.79 seconds**

**nmap -Pn 192.168.0.4**

**Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-25 19:11 India Standard Time**

**Nmap scan report for 192.168.0.4**

**Host is up (0.00029s latency).**

**Not shown: 991 closed tcp ports (reset)**

**PORT STATE SERVICE**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**902/tcp open iss-realsecure**

**912/tcp open apex-mesh**

**1521/tcp open oracle**

**2869/tcp open icslap**

**3306/tcp open mysql**

**8080/tcp open http-proxy**

**Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds**

**nmap -sS 192.168.0.0/24**

**Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-25 19:11 India Standard Time**

**Nmap scan report for 192.168.0.1**

**Host is up (0.021s latency).**

**Not shown: 997 closed tcp ports (reset)**

**PORT STATE SERVICE**

**23/tcp open telnet**

**80/tcp open http**

**5431/tcp open park-agent**

**MAC Address: 10:62:EB:18:E8:03 (D-Link International)**

**Nmap scan report for 192.168.0.4**

**Host is up (0.00095s latency).**

**Not shown: 991 closed tcp ports (reset)**

**PORT STATE SERVICE**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**902/tcp open iss-realsecure**

**912/tcp open apex-mesh**

**1521/tcp open oracle**

**2869/tcp open icslap**

**3306/tcp open mysql**

**8080/tcp open http-proxy**

**Nmap done: 256 IP addresses (2 hosts up) scanned in 9.52 seconds**

**nmap -sS 192.168.0.0/24**

**Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-25 19:19 India Standard Time**

**Nmap scan report for 192.168.0.1**

**Host is up (0.026s latency).**

**Not shown: 997 closed tcp ports (reset)**

**PORT STATE SERVICE**

**23/tcp open telnet**

**80/tcp open http**

**5431/tcp open park-agent**

**MAC Address: 10:62:EB:18:E8:03 (D-Link International)**

**Nmap scan report for 192.168.0.2**

**Host is up (0.012s latency).**

**All 1000 scanned ports on 192.168.0.2 are in ignored states.**

**Not shown: 1000 closed tcp ports (reset)**

**MAC Address: D6:00:60:C6:CD:CF (Unknown)**

**Nmap scan report for 192.168.0.3**

**Host is up (0.11s latency).**

**All 1000 scanned ports on 192.168.0.3 are in ignored states.**

**Not shown: 1000 closed tcp ports (reset)**

**MAC Address: 0A:5F:C9:9D:F5:91 (Unknown)**

**Nmap scan report for 192.168.0.4**

**Host is up (0.00080s latency).**

**Not shown: 991 closed tcp ports (reset)**

**PORT STATE SERVICE**

**135/tcp open msrpc**

**139/tcp open netbios-ssn**

**445/tcp open microsoft-ds**

**902/tcp open iss-realsecure**

**912/tcp open apex-mesh**

**1521/tcp open oracle**

**2869/tcp open icslap**

**3306/tcp open mysql**

**8080/tcp open http-proxy**

**Nmap done: 256 IP addresses (4 hosts up) scanned in 32.62 seconds**