

Network Scanning Experiment: Scan Your Home Network Using Nmap

Priyanshu Kumar Sharma, 2022-B-17102004A, B.Tech CTIS, SEM-VI/B

February 18, 2025

1 Objective

To perform a basic scan of your home network using Nmap (Network Mapper) to identify active devices and open ports.

2 Steps to Perform the Experiment

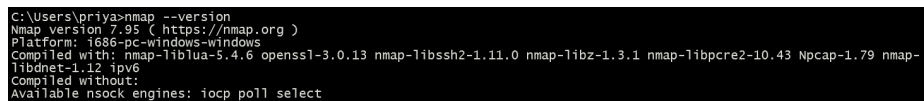
2.1 Step 1: Install Nmap (If Not Installed)

Nmap is available for Windows, Linux, and macOS. Follow the instructions below to install it.

Command:

```
nmap --version
```

Description: This command checks if Nmap is installed on your system and displays its version.



```
C:\Users\priya>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-libpcap-1.79 nmap-
libdnet-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select
```

Figure 1: Checking Nmap version

2.2 Step 2: Identify Your Home Network IP Range

To perform scanning, first identify your local IP address and subnet.

Windows Command:

```
ipconfig
```

Linux/macOS Command:

```
ipconfig
```

Description: These commands display network details, including your local IP address and subnet.

```
C:\Users\priya>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Unknown adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80
    IPv4 Address. . . . . : 192.
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

Figure 2: Finding local IP address

Check system availability

```
ping 10.11.217.229
```

```
C:\Users\priya>ping 10.11.217.229

Pinging 10.11.217.229 with 32 bytes of data:
Reply from 10.11.217.229: bytes=32 time=19ms TTL=64
Reply from 10.11.217.229: bytes=32 time=47ms TTL=64
Reply from 10.11.217.229: bytes=32 time=7ms TTL=64
Reply from 10.11.217.229: bytes=32 time=30ms TTL=64

Ping statistics for 10.11.217.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 47ms, Average = 25ms
```

Figure 3: This checks if the device is available

2.3 Step 3: Perform Basic Network Scan

A simple scan to detect all active devices on your network.

Command:

```
nmap -sn 10.11.217.229
```

Description: This scans all devices on the network without probing ports.

```
C:\Users\priya>nmap -sn 10.11.217.229
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-18 11:33 India Standard Time
Nmap scan report for 10.11.217.229
Host is up (0.081s latency).
MAC Address: D2 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 4.06 seconds
```

Figure 4: Basic network scan

2.4 Step 4: Perform a Port Scan on a Device

To check open ports on a specific device (e.g., router).

Command:

```
nmap -p- 10.11.217.229
```

Description: This scans all (0-65535) ports of the target device.

```
C:\Users\priya>nmap -p- 10.11.217.229
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-18 11:40 India Standard Time
Nmap scan report for 10.11.217.229
Host is up (0.035s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
1716/tcp  open  xmsg
46888/tcp open  unknown
MAC Address: D2:B3:32:42:A8:9D (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 150.87 seconds
```

Figure 5: Scanning ports of a device

2.5 Step 5: Detect Services and OS

To get detailed information about a device.

Command:

```
nmap -A 10.11.217.229
```

Description: This detects services (HTTP, SSH, etc.), operating system, and uptime.

2.6 Step 6: Scan for Vulnerabilities (Optional Ethical Use Only)

To check for common vulnerabilities on a device.

Command:

```

C:\Users\priya>nmap -A 10.11.217.229
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-18 11:47 India Standard Time
Nmap scan report for 10.11.217.229
Host is up (0.021s latency).
All 1000 scanned ports on 10.11.217.229 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: D2 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 20.95 ms 10.11.217.229

OS and Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/.
Nmap done: 1 IP address (1 host up) scanned in 19.95 seconds

```

Figure 6: Detecting services and OS

```
nmap --script vuln 10.11.217.229
```

Description: This scans for known vulnerabilities in the target system.

```

C:\Users\priya>nmap --script vuln 10.11.217.229
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-18 11:51 India Standard Time
Pre-scan script results:
  broadcast-avahi-dos:
    Discovered hosts:
      224.0.0.251
    After NULL UDP avahi packet DoS (CVE-2011-1002).
    Hosts are all up (not vulnerable).
Nmap scan report for 10.11.217.229
Host is up (0.011s latency).
All 1000 scanned ports on 10.11.217.229 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: D2 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 55.42 seconds

```

Figure 7: Scanning for vulnerabilities

3 Precautions Ethical Considerations

- Use Nmap only on networks you own or have permission to scan.
- Scanning unknown networks without authorization is illegal.
- Avoid aggressive scanning on shared networks (e.g., school, work).
- Ensure your firewall or security software allows scanning if needed.