Network Scanning using NMAP (Beginner Guide)

February 28, 2016   By Raj Chandel

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

For detail visit nmap.org

Host Scan

Host scan is used by penetration tester to identify active host in a network by sending ARP request packets to all system in that network. As result it will show a message "Host is up" by receiving MAC address from each active host.

Syntax: nmap -sP <target IP range>

      nmap -sn <target IP range>

Above syntax describes how to execute a host scan, to discover live hosts in a network by using Nmap. By default nmap is in-built in kali Linux, now open the terminal and enter the following command which will send ARP request packet to each system one-by-one.

```
nmap -sP 192.168.1.1-225
```

From given below image you can observe result of response generated by nmap for active host.

```
root@kali:~# nmap -sP 192.168.1.1-255  ⬅

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-17 06:38 EST
Nmap scan report for 192.168.1.1
Host is up (0.00061s latency).
MAC Address: 60:E        :B6:2A (Tp-link Technologies)
Nmap scan report for 192.168.1.100
Host is up (0.071s latency).
MAC Address: AC:E0        47:89 (Liteon Technology)
Nmap scan report for 192.168.1.101
Host is up (0.50s latency).
MAC Address: F8:32        47:C2 (Asustek Computer)
Nmap scan report for 192.168.1.106
Host is up (0.11s latency).
MAC Address: 58:         CF:DF (Liteon Technology)
Nmap scan report for 192.168.1.110
Host is up (0.063s latency).
MAC Address: AC:E0:       :47:89 (Liteon Technology)
Nmap scan report for 192.168.1.111
Host is up (0.062s latency).
MAC Address: 02:0         43:8F (Unknown)
Nmap scan report for 192.168.1.112
Host is up (0.063s latency).
MAC Address: 02:0        :43:8F (Unknown)
Nmap scan report for 192.168.1.115
Host is up (0.0011s latency).
MAC Address: FC:A         :8C:CA (Giga-byte Technology)
Nmap scan report for 192.168.1.116
Host is up (0.00049s latency).
MAC Address: 74:         :C0:0E (Giga-byte Technology)
Nmap scan report for 192.168.1.124
Host is up (0.26s latency).
MAC Address: E0:F         B7:AA (Apple)
Nmap scan report for 192.168.1.125
Host is up (0.065s latency).
MAC Address: F8:C        03:33 (Motorola Mobility, a Lenovo Company)
Nmap scan report for 192.168.1.117
Host is up.
Nmap done: 255 IP addresses (12 hosts up) scanned in 31.29 seconds
```

How it Works

Nmap uses the –sP/-sn flag for host scan and broadcast ARP request packet to identify IP allocated to particular host machine.

It will broadcast ARP request for a particular IP [suppose 192.168.1.100] in that network which can be the part of IP range [192.168.1.1-225] or CIDR [192.168.1.1/24 for class C] is used to indicate that we want to scan all the 256 IPs in our network. After then active host will unicast ARP packet by sending its MAC address as reply which gives a message **Host is up**.

Port scan /TCP scan

If penetration testers want to identify open or close state of a particular port on target machine then they should go with nmap port scan.

Port Status: After scanning, you may see some results with a port status like filtered, open, closed, etc. Let me explain this.
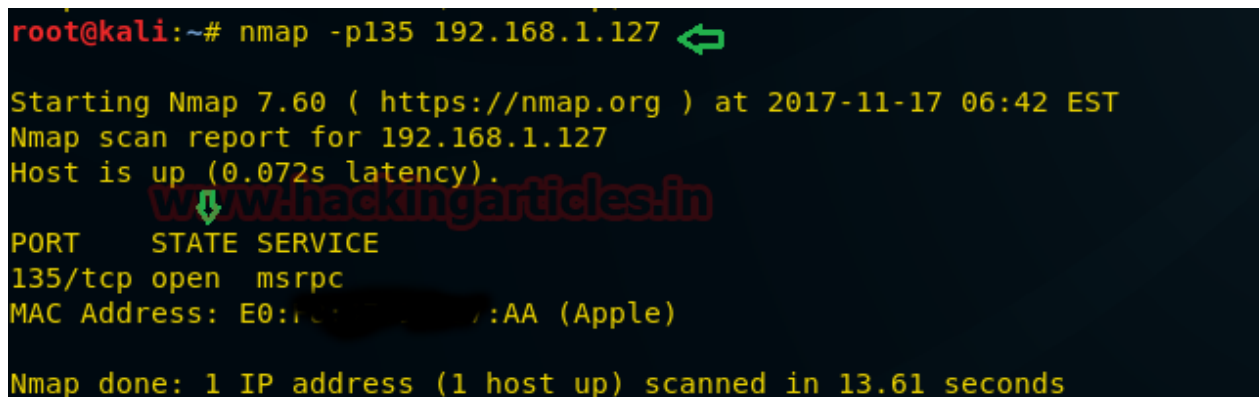
- Open: This indicates that an application is listening for connections on this port.
- Closed: This indicates that the probes were received but there is no application listening on this port.
- Filtered: This indicates that the probes were not received and the state could not be established. It also indicates that the probes are being dropped by some kind of filtering.
- Unfiltered: This indicates that the probes were received but a state could not be established.
- Open/Filtered: This indicates that the port was filtered or open but Nmap couldn't establish the state.
- Closed/Filtered: This indicates that the port was filtered or closed but Nmap couldn't establish the state.

Syntax: nmap -p [port number] <target IP range>

   nmap -sT [port number] <target IP range>

```
nmap -p135 192.168.1.127
```

Above command will try to connect with port 135 as result if port is open then it will display state "open" as well as "service" running on that particular port.

How it Works

Nmap uses the argument -p for defining the port range to be scanned. This flag can be combined with any scanning method. In the above example, we used the argument –p135 to indicate to Nmap that we are only interested in port 135. You can apply it the CIDR /24 in 192.168.1.1/24 which is used to indicate that we want to scan all of the 256 IPs in our network.

There are several accepted formats for the argument –p:

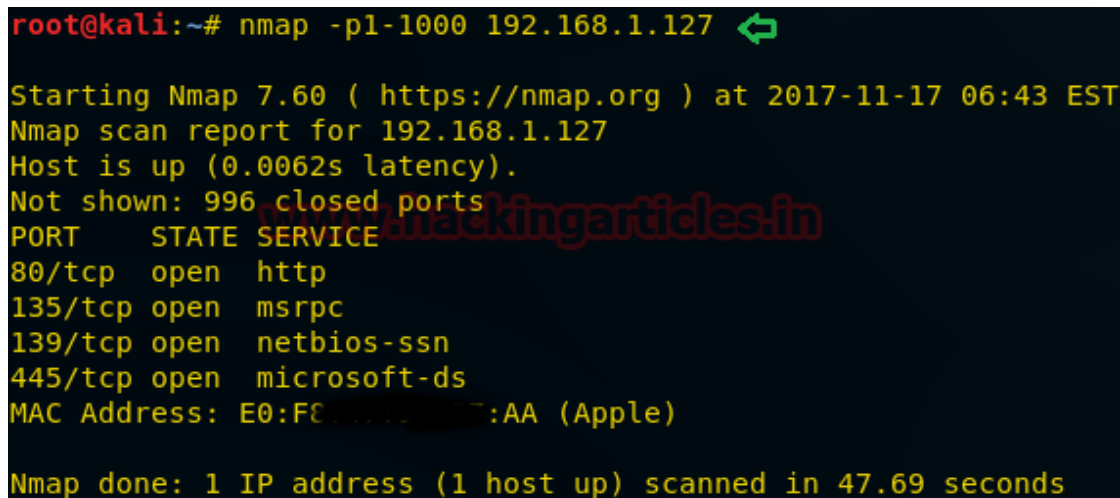# Port List

```
nmap -p135,139  192.168.1.127
```

If penetration testers want to scan more than one port of target then they should go with Port list scan where they can add multiple ports for scanning. This scan is quite useful to identify state of multiple selected ports which also describe status "host is up" if any single port is found to be opened.

Port Range

Using port range scan you can scan a particular range of ports of target network as per your requirement.

```
nmap -p1-1000 192.168.1.127
```

Above command will perform scanning from port number 1 to till port number 1000 and identify the state and service for open ports.


```
root@kali:~# nmap -p1-1000 192.168.1.127

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-17 06:43 EST
Nmap scan report for 192.168.1.127
Host is up (0.0062s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: E0:F8          :AA (Apple)

Nmap done: 1 IP address (1 host up) scanned in 47.69 seconds
```

ALL Ports

If penetration testers want to scan all 65535 ports; then they should execute given below command which will enumerates the open ports of target system:

Syntax: nmap -p- <target>

Above syntax is used for scanning all ports of target network, keep patience while executing above format because it will take some time to enumerate open port or you can also execute given below command which uses parameter "–open" to perform same task in order to save time.

```
nmap -p1-65535 192.168.1.127 --open
```

```
root@kali:~# nmap -p1-65535 192.168.1.127 --open ⇐

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-24 04:45 EST
Nmap scan report for 192.168.1.127
Host is up (0.0020s latency).
Not shown: 65522 closed ports
PORT       STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
3389/tcp   open  ms-wbt-server
49152/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp open   unknown
49158/tcp open   unknown
49159/tcp open   unknown
MAC Address: FC:AA:        E6 (Giga-byte Technology)

Nmap done: 1 IP address (1 host up) scanned in 23.07 seconds
```

Specific Ports by Protocols

By default port scan prefer to enumerate the state of TCP ports but if you want to scan TCP port as well as UDP port then execute following command given below:

Syntax: nmap -pT:25,U:53 <target>

Port Service name

If you don't known accurate port number for enumeration then you can also mention service name for port state scanning .

Syntax: nmap –p[service]<target>

```
nmap -p msrpc 192.168.1.127
```

From given image you can observe that same result has been obtained by executing above command without referring any port number.

```
root@kali:~# nmap -p msrpc 192.168.1.127  ⬅

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-17 06:47 EST
Nmap scan report for 192.168.1.127
Host is up (0.078s latency).

PORT     STATE SERVICE
135/tcp open  msrpc
MAC Address: E0:F?          7:AA (Apple)

Nmap done: 1 IP address (1 host up) scanned in 13.79 seconds
```

UDP Scan

UDP services are mostly ignored during penetration tests, but fine penetration testers know that they often expose host essential information or can even be vulnerable moreover used to compromise a host. This method demonstrates how to utilize Nmap to list all open UDP ports on a host.

Syntax: nmap –sU <target>

```
nmap -sU 192.168.1.127
```

From given below image you can observe the result for UDP port scan.

```
root@kali:~# nmap -sU 192.168.1.127  ⬅

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-24 03:39 EST
Nmap scan report for 192.168.1.127
Host is up (0.0011s latency).
Not shown: 993 closed ports
PORT       STATE          SERVICE
137/udp    open           netbios-ns
138/udp    open|filtered netbios-dgm
500/udp    open|filtered isakmp
1900/udp   open|filtered upnp
4500/udp   open|filtered nat-t-ike
5355/udp   open|filtered llmnr
39632/udp open|filtered unknown
MAC Address: FC:AA          E:E6 (Giga-byte Technology)

Nmap done: 1 IP address (1 host up) scanned in 845.19 seconds
```

```
nmap -sU -p 137 192.168.1.127
```

In order to scan particular UDP port it is suggested that you should use the flag -p for Port selection. Here you can observe that we have chosen port 137 which is a UDP port for NetBIOS service.

There are so many way to perform UDP scan as per your requirement, for example read given below method to perform UDP scan:

UDP Port Range

If you want to scan multiple UDP ports or range of UDP ports then use –p flag to address the range of port.

Syntax: nmap -p1-500 -sU <target>

ALL UDP PORT

Syntax: nmap -sU -p- <target>

Above syntax is applicable for scanning all UDP ports of target's network.

How it Works

UDP scan works by sending a UDP packet to every destination port and analyzes the response to determine the port's state; it is a connection less protocol. For some common ports such as 53 and 161, a protocol-specific payload is sent to increase response rate, a service will respond with a UDP packet, proving that it is "open". If the port is "closed", an ICMP Port Unreachable message is received from the target. If no response is received after retransmissions, the port is classified as "open|filtered". This means that the port could be open, or perhaps packet filters are blocking the communication.

OS Detection Scan

Apart from open port enumeration nmap is quite useful in OS fingerprinting. This scan very helpful to penetration tester in order to conclude possible security vulnerabilities and determining the available system calls to set the specific exploit payloads.

Syntax: nmap -O <target>

```
nmap -O 192.168.1.127
```

Above command will dump following information:

Device type: All fingerprints are classified with one or more high-level device types, such as router, printer, firewall, general purpose. These are further described in the section called "Device and OS classification (Class lines)". If you notice given below image here "Device Type: general purpose".

Running: This field is also related to the OS classification scheme described in the section called "Device and OS classification (Class lines)". It shows the OS Family (Windows in this case) and OS generation if available. If there are multiple OS families, they are separated by commas. When Nmap can't narrow down OS generations to one

specific choice, options are separated by the pipe symbol ('|') Examples include OpenBSD 3.X, NetBSD 3.X|4.X and Linux 2.4.X|2.5.X|2.6.X.

If you will image given below again then here you will observe OS generations is specified as **7|2008|8.1**

OS CPE: This shows a Common Platform Enumeration (CPE) representation of the operating system when available. It may also have a CPE representation of the hardware type. OS CPE begins with cpe:/o and hardware CPE begins with cpe:/h.

OS details: This line gives the detailed description for each fingerprint that matches. While the Device type and Running lines are from predefined enumerated lists that are easy to parse by a computer, the OS details line contains free-form data which is useful to a human reading the report. This can include more exact version numbers, device models, and architectures specific to a given fingerprint.

```
root@kali:~# nmap -O 192.168.1.127  ⬅

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-17 06:51 EST
Nmap scan report for 192.168.1.127
Host is up (0.0027s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5000/tcp  open  upnp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: E0:        :AA (Apple)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:wind
ver_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Network Distance: 1 hop
```

How it Works

The option -O inform Nmap to enable OS detection that identify a wide variety of systems, including residential routers, IP webcams, operating systems, and many other hardware devices

You can also execute following command for os detection

Syntax: nmap -O -p- –osscan-guess <target>

In case OS detection fails, you can use the argument –osscan-guess to try to guess the operating system:

To launch OS detection only when the scan conditions are ideal, uses the argument –osscan-limit:

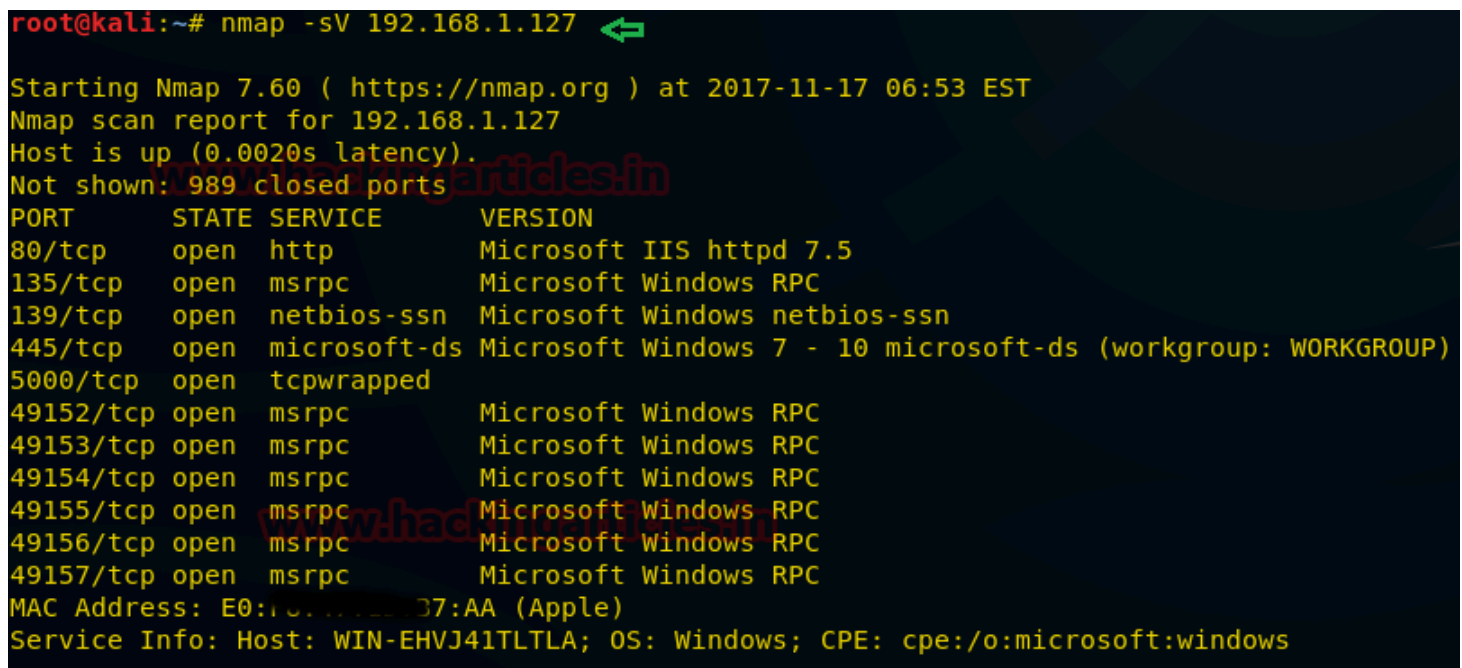**Syntax:** nmap -O –osscan-limit <target>

Version Scan

When doing vulnerability assessments of your companies or clients, you really want to know which mail and DNS servers and versions are running. Having an accurate version number helps dramatically in determining which exploits a server is vulnerable to. Version detection helps you obtain this information. Fingerprinting a service may also reveal additional information about a target, such as available modules and specific protocol information. Version scan is also categories as "**Banner Grabbing**" in penetration testing.

Syntax: nmap -sV <target>

Following command will dump the result for installed version of running services of target's machine.

```
nmap -sV 192.168.1.127
```

From given below image you can observed that it has shown current installed version of running application. . Additional information will be enclosed in parenthesis. The hostname field and two more fields that version detection can discover are operating system and device type is reported on a Service Info line following the port table.

Specific Port Version scan

For scanning version of a particular port or service you can use argument –p in the command as shown below.

Syntax: nmap -sV -p135 <target>

How it Works

The –sV flag inform nmap to works by sending different query from nmap-service-probes to the list of assumed open ports for banner grabbing. As result it will give output as table which has an additional column named VERSION, displaying the particular service version. Additional information will be enclosed in parenthesis.
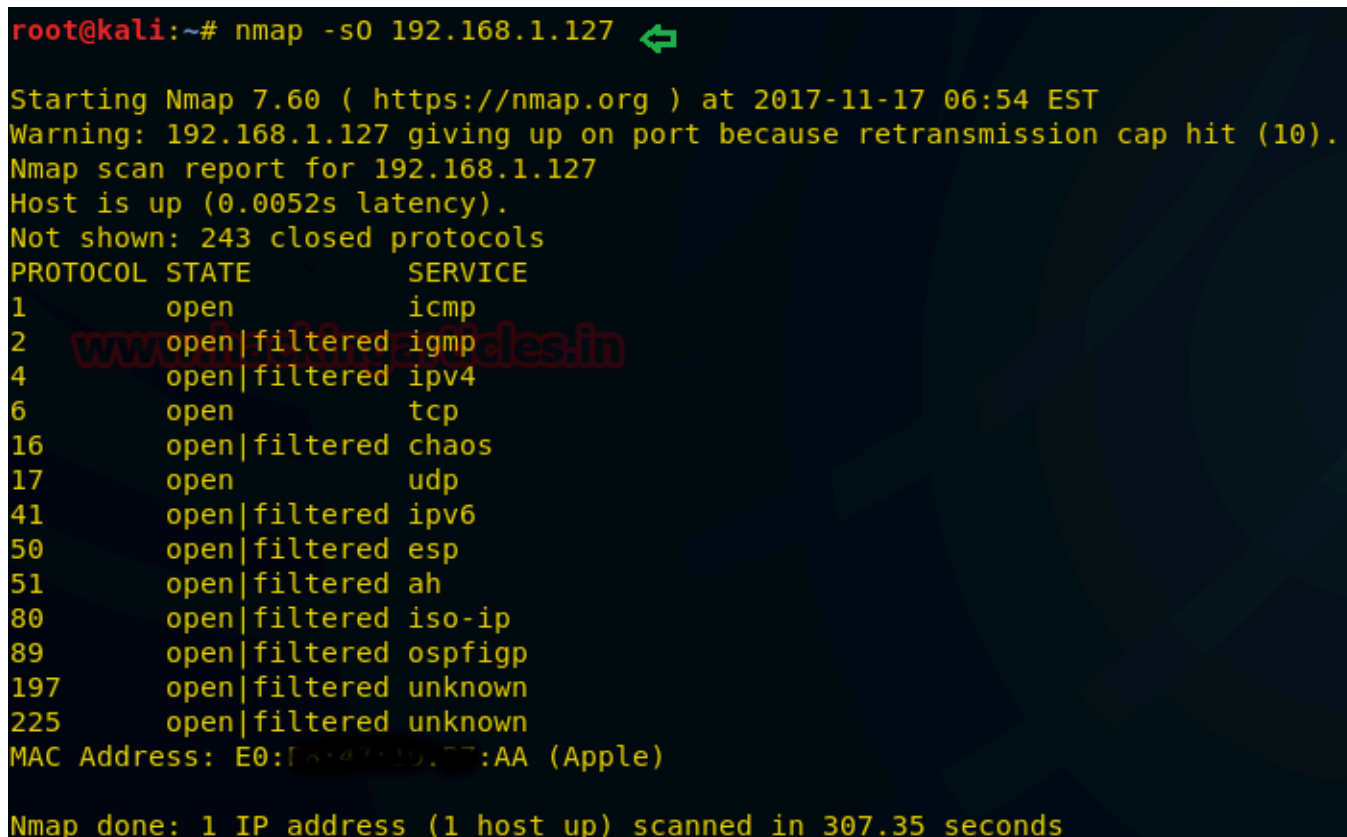
Protocol Scan

IP Protocol scan is quite helpful for determining what communication protocols are being used by a host. This method shows how to use Nmap to enumerate all of the IP protocols, where sends a raw IP packet without any additional protocol header, to each protocol on the target machine. For the IP protocols TCP, ICMP, UDP, IGMP, and SCTP, Nmap will set valid header values but for the rest, an empty IP packet will be used.

Syntax: **nmap -sO <target>**

The results will show what protocols are supported, along with their states.

```
nmap -sO 192.168.1.254
```

From given below image you can observer the result of protocol scan for open and open|filtered state.

```
root@kali:~# nmap -sO 192.168.1.127

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-17 06:54 EST
Warning: 192.168.1.127 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.127
Host is up (0.0052s latency).
Not shown: 243 closed protocols
PROTOCOL STATE           SERVICE
1        open            icmp
2        open|filtered igmp
4        open|filtered ipv4
6        open            tcp
16       open|filtered chaos
17       open            udp
41       open|filtered ipv6
50       open|filtered esp
51       open|filtered ah
80       open|filtered iso-ip
89       open|filtered ospfigp
197      open|filtered unknown
225      open|filtered unknown
MAC Address: E0:          :AA (Apple)

Nmap done: 1 IP address (1 host up) scanned in 307.35 seconds
```

How it Works

The flag -sO tells Nmap to perform an IP Protocol Scan, This kind of scan repeat throughout the protocols found in the file nmap-protocols, and creates IP packets for every entry.

To verify the port state, Nmap categorize the different responses received, as follows:

- When it received an ICMP protocol unreachable error type=3 or code=2, the port state is marked as "closed".
- ICMP unreachable errors type=3 or code 1,3,9,10 or 13 indicate that a port state is "filtered".
- If no response is received, the port state is marked as "filtered|open".
- Any other response will cause the port state to be marked as "opened".

To specify what protocols should be scanned, we could set the argument -p:

Syntax: nmap -p1,3,5 -sO <target>

 nmap -p1-10 -sO <target>

Fast Scan

The -F option scans only those ports listed in the nmap_services file (or the protocols file if the scan type is -sO). This is far faster than scanning all 65,535 ports.

If you will compare scanned time from above scanned result you will notice time difference between these scans, moreover it has not shown open ports of other running services which above scan has shown.

Syntax: nmap –F <target>

```
nmap -F 192.168.1.127
```

From given below image you can observe **scanned time: 14.42 seconds** where as in above scanning method [protocol scan] scanned time: 307.45 seconds

Timing Template Scan

The main timing option is set through the -T parameter if you may want more control over the timing in order get the scan over and done with quicker. However, Nmap adjusts its timings automatically depending on network speed and response times of the victim.

Nmap offers a simpler approach, with six timing templates. You can specify them with the -T option and their number (0–5) or their name as shown below:

- T0: paranoid
- T1: sneaky
- T2: polite
- T3: normal
- T4: aggressive
- T5: insane

Syntax: nmap T[option] <target>

```
nmap –T4 192.168.1.127
```

Above command will perform aggressive scan and reduce scanning timing for enumeration of target's system, here from given below image you can observe **scanned time: 14.36** seconds.


```
root@kali:~# nmap -T4 192.168.1.127

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-24 03:59 EST
Nmap scan report for 192.168.1.127
Host is up (0.0016s latency).
Not shown: 987 closed ports
PORT       STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
3389/tcp   open  ms-wbt-server
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49158/tcp  open  unknown
49159/tcp  open  unknown
MAC Address: FC:A       E:E6 (Giga-byte Technology)

Nmap done: 1 IP address (1 host up) scanned in 14.36 seconds
```

Exclude Scan

There will be circumstances where host exception is required to avoid scanning of certain machines. Such as government website or IP, you may not have the authorization, or might that the host has been already scanned. Nmap option **–exclude** help you to eliminate a host or list of hosts from complete network scan.

Syntax: nmap <IP range > –exclude <target IP>

Above syntax defines that from given range of IPs do not perform scanning for excluded target IP else dump the scanned result for remaining IPs.

```
nmap -F 192.168.1.110-255 --exclude 192.168.1.114
```

Above command will perform scan for all IPs between 192.168.1.110 and 192.168.1.255 except "192.168.1.114" which you can confirm from given below image.

```
root@kali:~# nmap -F 192.168.1.110-255 --exclude 192.168.1.114 ⇐

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-24 04:06 EST
Nmap scan report for 192.168.1.110
Host is up (0.026s latency).
Not shown: 96 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
MAC Address: 58:00          .DF (Liteon Technology)

Nmap scan report for 192.168.1.111
Host is up (0.099s latency).
Not shown: 99 closed ports
PORT    STATE SERVICE
22/tcp open   ssh
MAC Address: 58:00       F:DF (Liteon Technology)

Nmap scan report for 192.168.1.112
Host is up (0.00020s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 74:D4:        :0E (Giga-byte Technology)

Nmap scan report for winterfell.7kingdoms.ctf (192.168.1.113)
Host is up (0.0010s latency).
Not shown: 96 filtered ports
PORT     STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
554/tcp open  rtsp
MAC Address: FC:A           :A4:E9 (Giga-byte Technology)

Nmap scan report for 192.168.1.115
Host is up (0.036s latency).
Not shown: 97 filtered ports
PORT      STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

How it works

The arguments -F –exclude 192.168.1.114 inform Nmap to perform fast scanning for all IPs [between 192.168.1.110 and 192.168.1.255] in this private network, excluding the machines with the IPs 192.168.1.114.

```
nmap -sV -O --exclude-file remove.txt 192.168.1.1/24
```

Excluding a host list from your scans Nmap also supports the argument –exclude-file <filename> in order to exclude the targets listed in <filename>

Aggressive Scan

This option enables additional advanced and aggressive options. Presently this enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (–traceroute). This option only enables features, and not timing options (such as -T4) or verbosity options (-v) that you might want as well. You can see this by using one of the following commands:

Syntax: nmap -A <target>

```
nmap –A 192.168.1.127
```

If you will notice given below image then you will observe that the result obtain by it is the combination of multiple scan. As its dump "version" of running application, "OS fingerprint", "traceroute" and "host script scanning"g which is showing some very essential information related to host system.

```
root@kali:~# nmap -A 192.168.1.127  ⇐

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-17 06:56 EST
Nmap scan report for 192.168.1.127
Host is up (0.0067s latency).
Not shown: 989 closed ports
PORT        STATE SERVICE      VERSION
80/tcp      open  http         Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
135/tcp     open  msrpc        Microsoft Windows RPC
139/tcp     open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp     open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds
5000/tcp    open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: E0:  :1D:B7:AA (Apple)
Device type: general purpose|media device
Running: Microsoft Windows 2008|10|7|8.1, Microsoft embedded
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_10 cpe:/h:
:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One, Microsoft W:
ver 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-EHVJ41TLTLA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WIN-EHVJ41TLTLA, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: WIN-EHVJ41TLTLA
|   NetBIOS computer name: WIN-EHVJ41TLTLA\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2017-11-17T17:28:02+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
```

How it Works

The argument –A inform nmap to perform advance aggressive scan to enumerate version of running service, OS detection, traceroute of hop and host script scanning of host machine. Therefore it will take some time in scanning, you can add –T4 timing template to increase the rate of scanning.

List Scan

When you want to scan multiple host to perform more than one scanning then –iL option is used which support nmap to load the targets from an external file. Only you need to add all targeted IP in a text file and save it at a location.

```
*(Untitled)

File  Edit  Search  Options  Help
192.168.1.127
192.168.1.110
```

To load the targets from the file targets.txt, the following command can be used:

Syntax: nmap -iL targets.txt [path of file]

```
nmap -iL /root/Desktop/scan.txt
```

```
root@kali:~# nmap -iL /root/Desktop/scan.txt  ⬅

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-24 03:56 EST
Nmap scan report for 192.168.1.127
Host is up (0.0016s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp    open   msrpc
139/tcp    open   netbios-ssn
443/tcp    open   https
445/tcp    open   microsoft-ds
902/tcp    open   iss-realsecure
912/tcp    open   apex-mesh
3389/tcp   open   ms-wbt-server
49152/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp open   unknown
49158/tcp open   unknown
49159/tcp open   unknown
MAC Address: FC:A           E:E6 (Giga-byte Technology)

Nmap scan report for 192.168.1.110
Host is up (0.0075s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
2869/tcp open   icslap
5357/tcp open   wsdapi
MAC Address: 58:0         F:DF (Liteon Technology)

Nmap scan report for 192.168.1.111
Host is up (0.022s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
22/tcp open   ssh
MAC Address: 58:0         F:DF (Liteon Technology)

Nmap done: 3 IP addresses (3 hosts up) scanned in 19.51 seconds
```

Source

https://nmap.org/book/osdetect-usage.html

I highly recommend this book. Click here