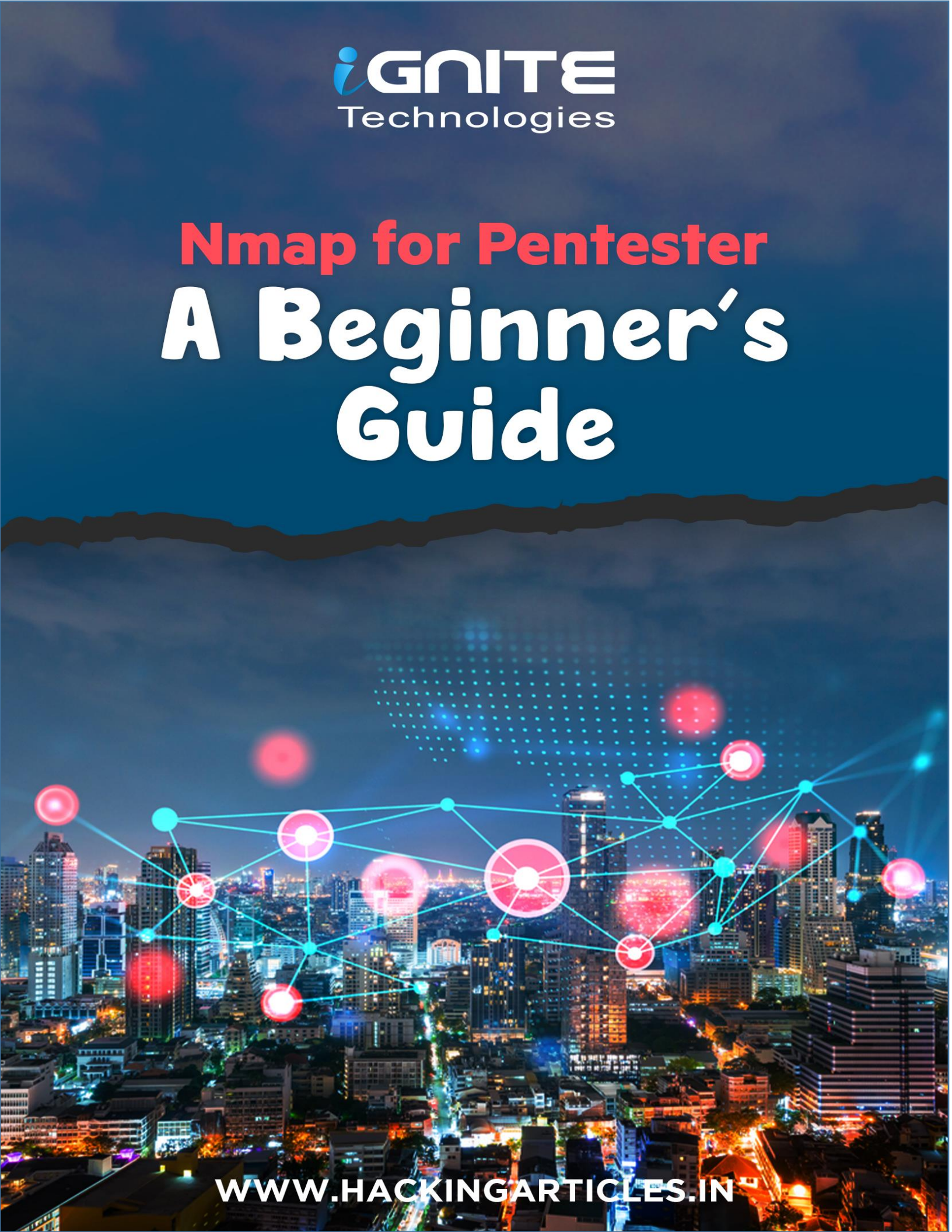
iGNITE Technologies

Nmap for Pentester

A Beginner's Guide



WWW.HACKINGARTICLES.IN

Contents

Introduction

Nmap ("Network Mapper") is a free and open-source (licenced) 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 it 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 details, visit nmap.org

Host Scan

A host scan is used by penetration testers to identify active hosts in a network by sending ARP request packets to all systems in that network. As a result of receiving the MAC address from each active host, it will display the message "Host is up."

Syntax: nmap -sP <target IP range>

nmap -sn <target IP range>

The 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 an ARP request packet to each system one-by-one.

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

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

How it works

Nmap employs the -sP/–sn flags for host scanning and broadcasting ARP request packets to determine the IP address assigned to a specific host machine.

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

Port scan /TCP scan

If penetration testers want to identify the open or closed state of a particular port on a target machine, then they should use 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>

As a result, if the port is open, it will show the state "open" as well as the "service" that is running on that port.

nmap -p135 192.168.1.127

```
root@kali:~# nmap -p135 192.168.1.127

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-17 06:42 EST
Nmap scan report for 192.168.1.127
Host is up (0.072s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: E0:[redacted]:AA (Apple)

Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds
```


How it works

Nmap uses the argument -p to define 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 to 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 this argument.

Port List

nmap -p135,139 192.168.1.127

If penetration testers want to scan more than one port of a target, then they should go with a port list scan where they can add multiple ports for scanning. This scan is useful for determining the status of multiple selected ports, and it also describes the status "host is up" if any single port is found to be open.

Port Range

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

nmap -p1-1000 192.168.1.127

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

ALL Ports

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

Syntax: nmap -p- <target>

Keep patience while executing the above format because it will take some time to enumerate the open ports. Or you can also execute the given below command which uses parameter "--open" to perform the 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 prefers to enumerate the state of TCP ports, but if you want to scan TCP ports as well as UDP ports, then execute the following command given below:

Syntax: nmap -pT:25,U:53

Port Service name

If you don't know an accurate port number for enumeration, then you can also mention a service name for port state scanning.

Syntax: nmap -p[service]<target>

nmap -p msrpc 192.168.1.127

From the given image, you can observe that the same result has been obtained by executing the above command without referring to 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[redacted]: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 and be used to compromise a host. This method demonstrates how to utilise Nmap to list all open UDP ports on a host.

Syntax: nmap –sU <target>

nmap -sU 192.168.1.127

From the given below image, you can observe the result of the 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[redacted]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:

A UDP scan works by sending a UDP packet to every destination port and analysing 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 the 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 for OS fingerprinting. This scan is very helpful to penetration testers in order to conclude possible security vulnerabilities and determine the available system calls to set the specific exploit payloads.

Syntax: nmap -O <target>

The above command will dump the following information:

Device type: All fingerprints are classified into one or more high-level device types, such as router, printer, firewall, or general purpose. These are further described in the section called "Device and OS classification (Class lines)". As you can see in the image below, "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 look at the image given below again, you will observe the OS generations are 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 of 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 that is useful to a human reading the report. This can include more precise 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:[redacted]: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 company 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 categorised as **"banner grabbing"** in penetration testing.

Syntax: nmap -sV <target>

nmap -sV 192.168.1.127

The following command will dump the result for the installed version of the running services of the target machine.

From the given below image, you can observe that it shows the current installed version of the running application. Additional information will be enclosed in parenthesis. The hostname field and two more fields that version detection can discover are the operating system and device type. They are reported on a service info line following the port table.

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

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-17 06:53 EST
Nmap scan report for 192.168.1.127
Host is up (0.0020s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
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:[illegible]7:AA (Apple)
Service Info: Host: WIN-EHVJ41TLTLA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

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 informs nmap to work by sending different queries from nmap-service-probes to the list of assumed open ports for banner grabbing. As a result, it will give output as a table which has an additional column named "VERSION", displaying the particular service version. Additional information will be enclosed in parenthesis.

Protocol Scan

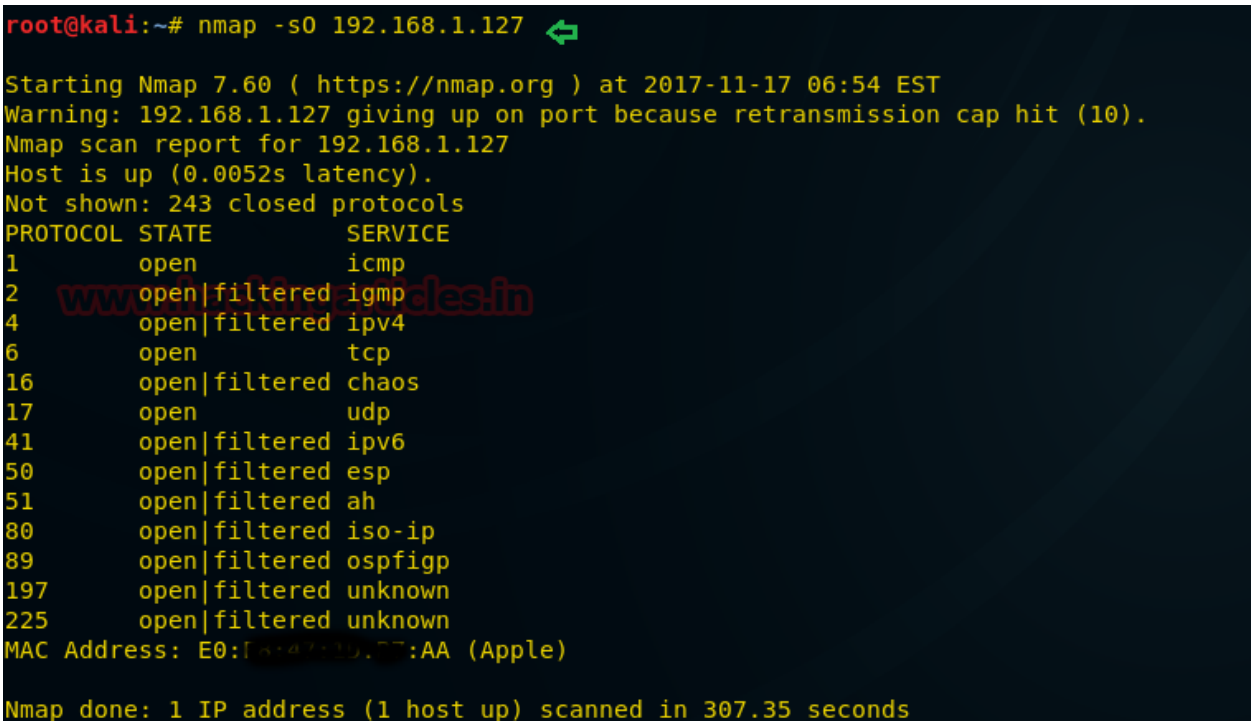
An IP Protocol scan is quite helpful for determining what communication protocols are being used by a host. This method shows how to use Nmap to enumerate all of the IP protocols by sending a raw IP packet without any additional protocol headers to each protocol on the target machine. For the IP protocols 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 the given below image, you can observe the result of the protocol scan for open and open|filtered state.



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 To specify what protocols should be scanned, we could set the argument "opened"

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

nmap -p1-10 -sO <target>

Fast Scan

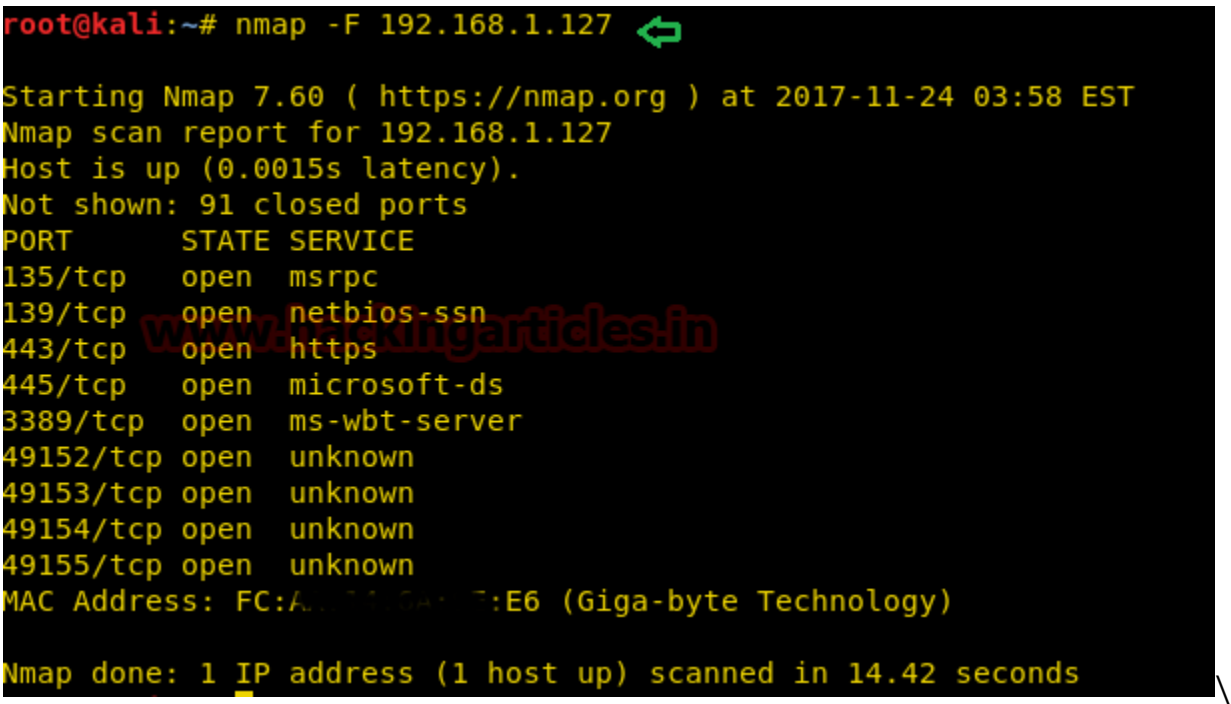
The -F option scans only those ports listed in the nmap_services file (or the protocols file if the scan type is -sO). This is far faster than scanning all 65,535 ports.

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

Syntax: nmap -F <target>

nmap -F 192.168.1.127

From the given below image, you can observe the **scanned time: 14.42 seconds**, where as in the above scanning method [protocol scan], the 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 to get the scan over and done with quicker. However, Nmap adjusts its timings automatically depending on the 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>

The above command will perform an aggressive scan and reduce the scanning time for enumeration of the target's system. Here, from the given below image, you can observe the **scanned time: 14.36 seconds.**

nmap -T4 192.168.1.127

```
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 a host exception is required to avoid the scanning of certain machines. Such as a government website or IP, you may not have the authorization, or might find that the host has already been scanned. The Nmap option --exclude allows you to exclude a host or a list of hosts from a full network scan.

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

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

nmap -F 192.168.1.110-255 --exclude 192.168.1.114

The above command will perform a scan for all IPs between 192.168.1.110 and 192.168.1.255 except "192.168.1.114", which you can confirm from the 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:[illegible]: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:[illegible]: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:[illegible]: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[illegible]: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] on this private network, excluding the machines with the IP 192.168.1.114.

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

Leaving the host list out of your scans Nmap also supports the argument --exclude-file in order to exclude the targets listed in <filename>

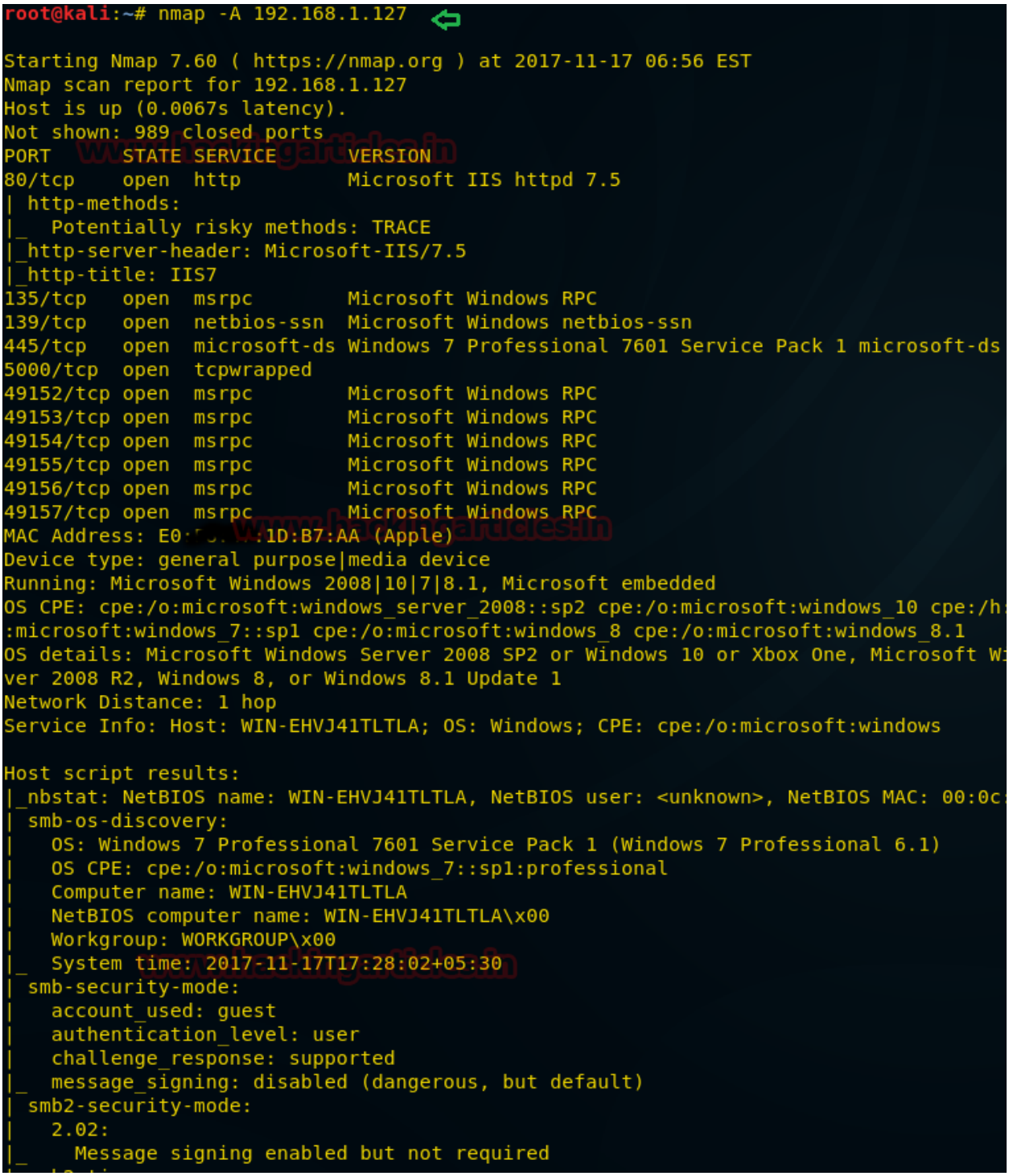
Aggressive Scan

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, 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 notice the given below image, then you will observe that the result obtained by it is a combination of multiple scans. As its dump, it shows the "version" of the running application, the "OS fingerprint," the "traceroute," and the "host script scanning," which shows some very important information about the host system.

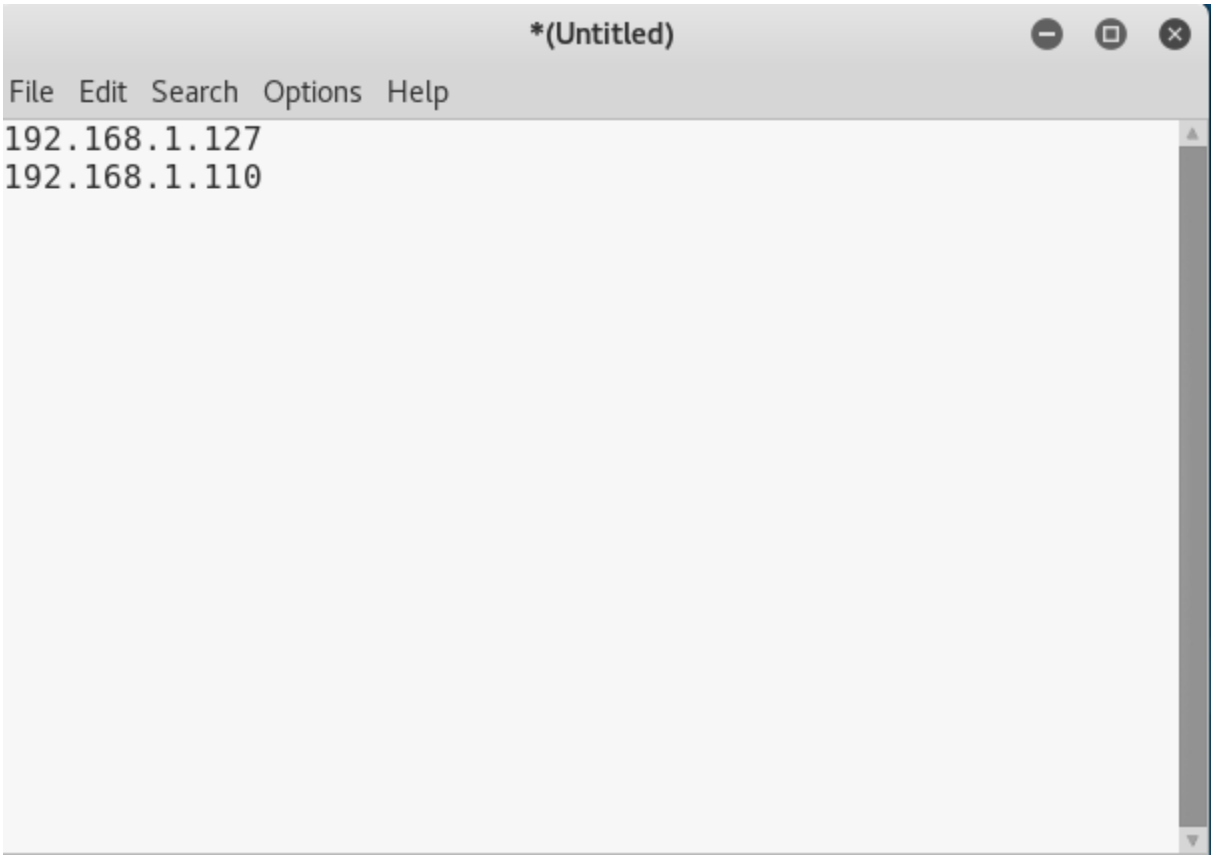


How it Works

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

List Scan

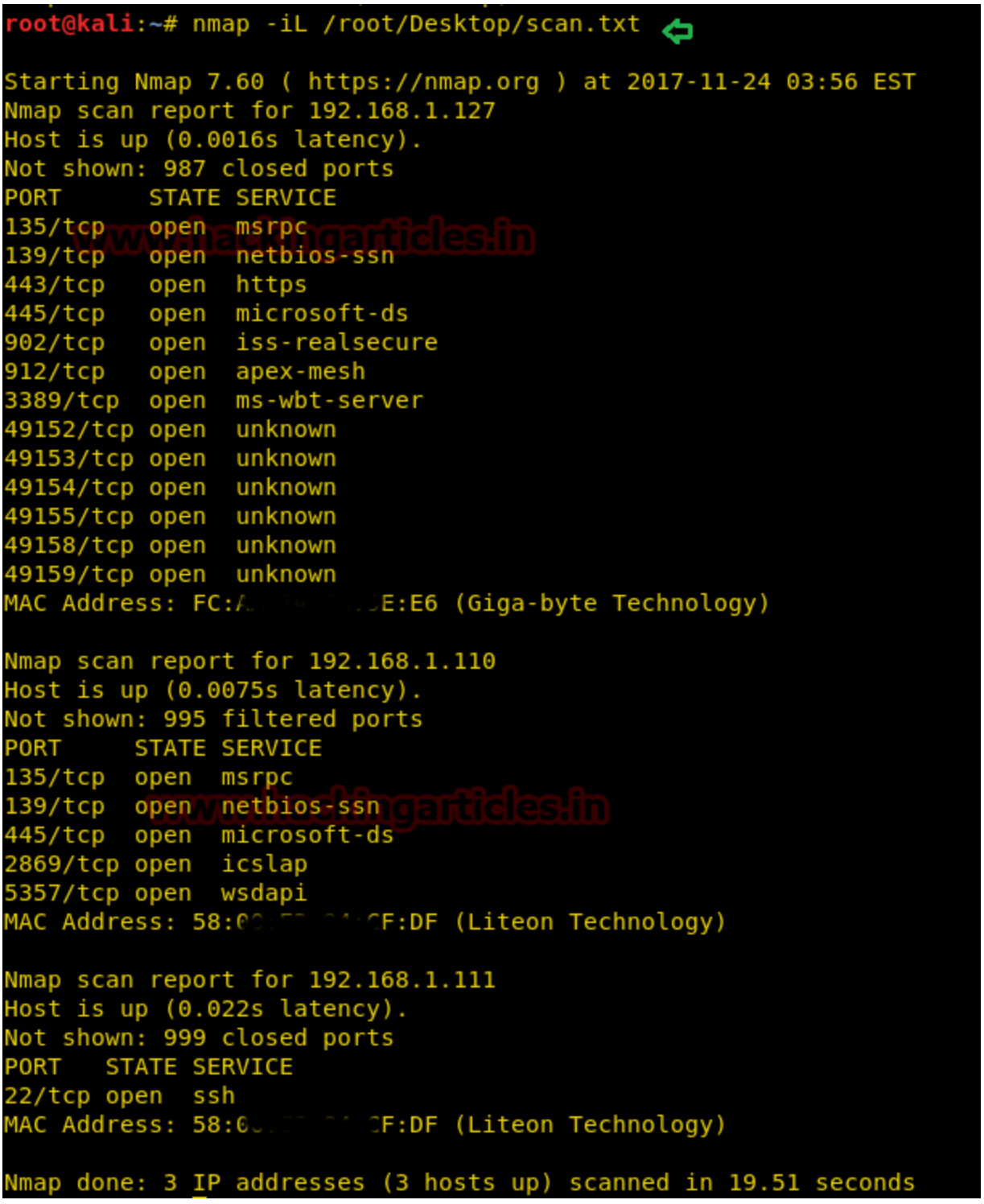
When you want to scan multiple hosts to perform more than one scan, then the –iL option is used, which supports nmap to load the targets from an external file. You only need to add all the targeted IPs in a text file and save them at a location.



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
```



Source:

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

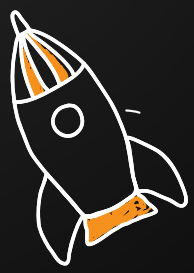
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

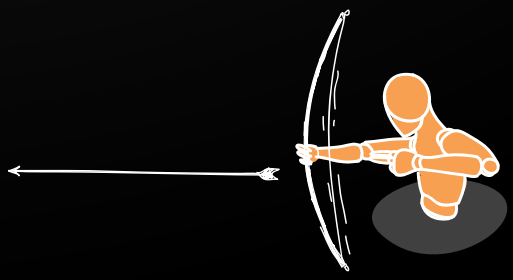
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux