

## Assignment 8

**Aim:-** Installation of NMAP and using it with different options to scan open ports, perform OS fingerprinting, ping scan, TCP port scan, etc

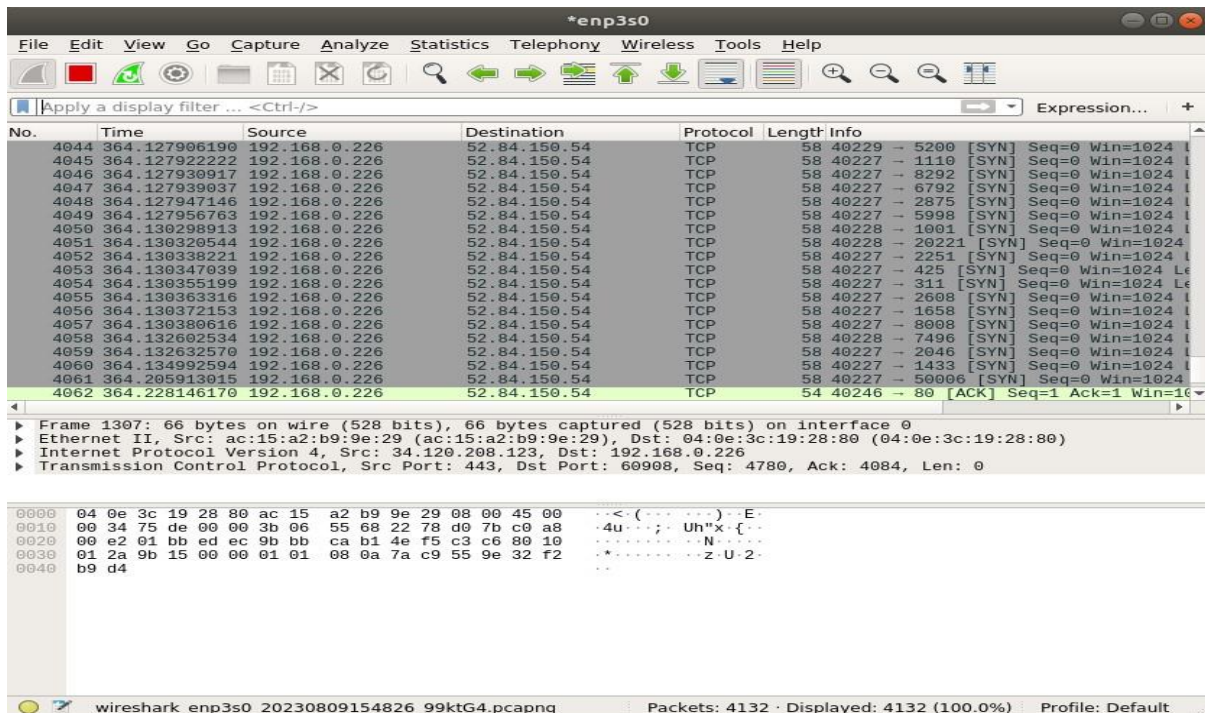
**LO mapped:** - LO4

**Theory:-**

Ping Sweep

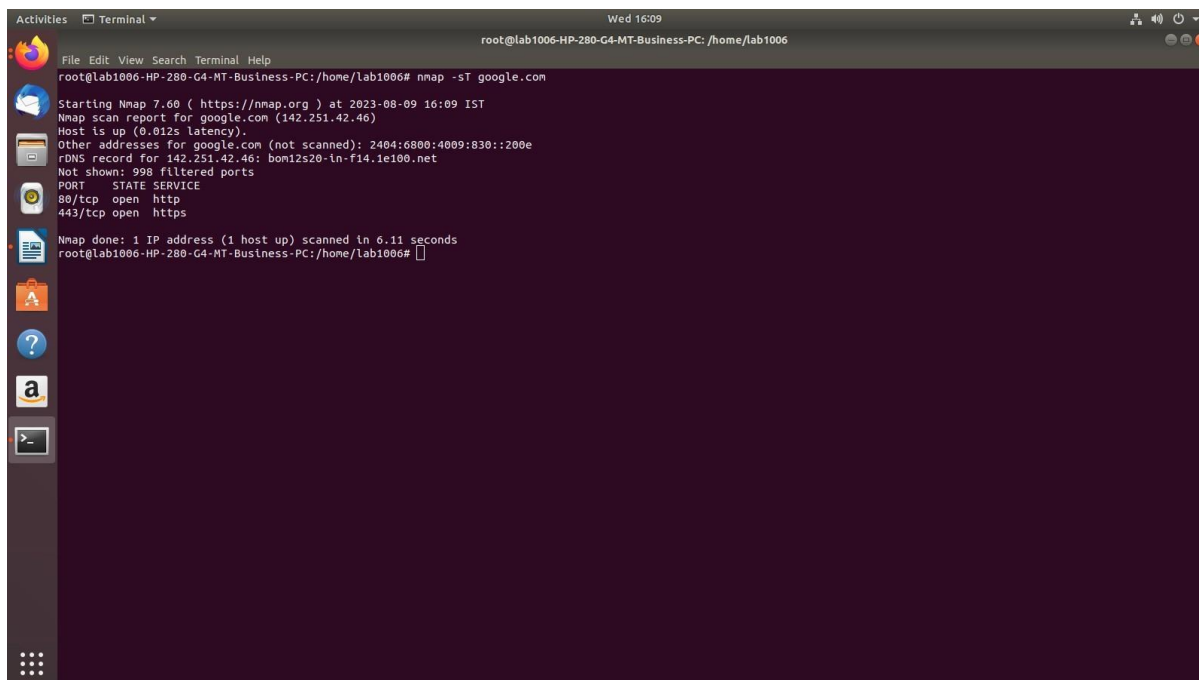
Nmap -sP <IP address(192.168.0.\*)>

1. -sS (TCP SYN scan)



SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections. It also works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NULL/Xmas, Maimon and idle scans do. It also allows clear, reliable differentiation between open, closed, and filtered states

## 2. -sT (TCP connect scan)



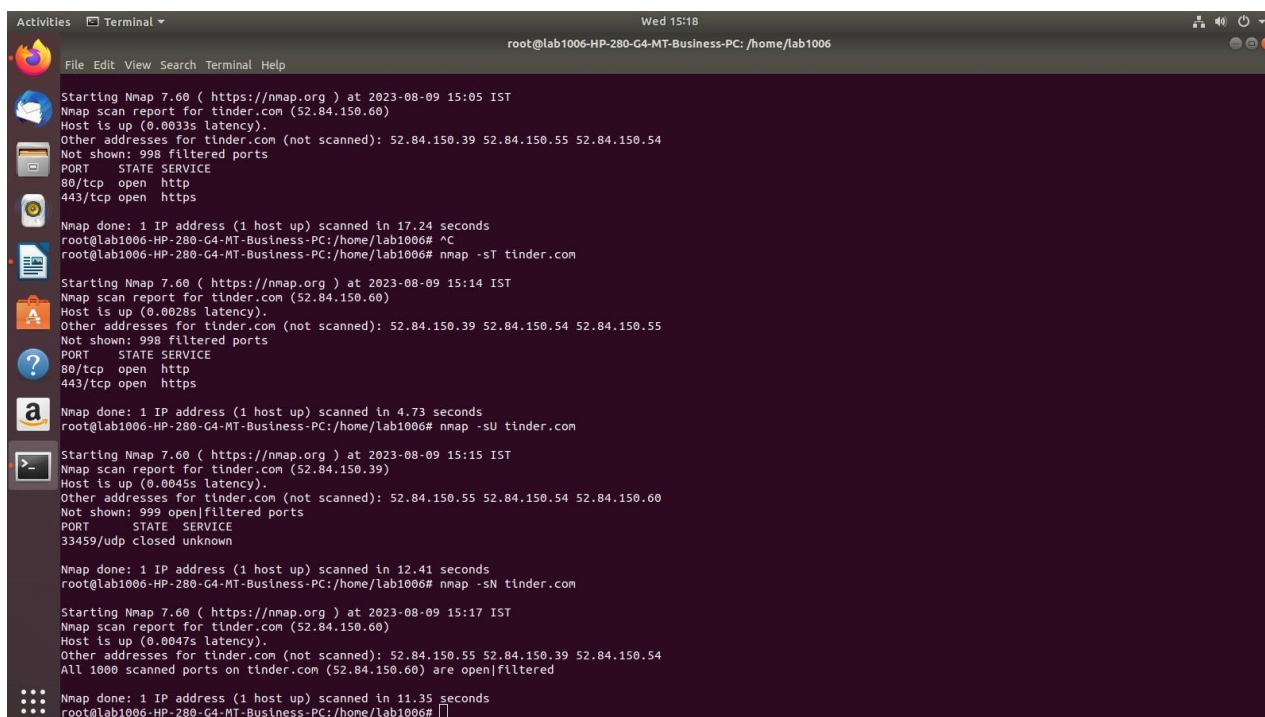
```
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sT google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 16:09 IST
Nmap scan report for google.com (142.251.42.46)
Host is up (0.012s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:830::200e
rDNS record for 142.251.42.46: bom12s20-in-f14.1e100.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 6.11 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006#
```

TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt. This and the FTP bounce scan ([the section called "TCP FTP Bounce Scan \( -b \)"](#)) are the only scan types available to unprivileged users.

## 3. -sU (UDP scans)



```
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sT tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:05 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0033s latency).
Other addresses for tinder.com (not scanned): 52.84.150.39 52.84.150.55 52.84.150.54
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.24 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# ^C
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sT tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:14 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0028s latency).
Other addresses for tinder.com (not scanned): 52.84.150.39 52.84.150.54 52.84.150.55
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sU tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:15 IST
Nmap scan report for tinder.com (52.84.150.39)
Host is up (0.0045s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.54 52.84.150.60
Not shown: 999 open/filtered ports
PORT      STATE SERVICE
33459/udp  closed unknown

Nmap done: 1 IP address (1 host up) scanned in 12.41 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sN tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:17 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0047s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.39 52.84.150.54
All 1000 scanned ports on tinder.com (52.84.150.60) are open/filtered

Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006#
```

```
Activities Terminal Wed 15:18
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006

Nmap done: 1 IP address (1 host up) scanned in 17.24 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# ^C
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sT tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:14 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0028s latency).
Other addresses for tinder.com (not scanned): 52.84.150.39 52.84.150.54 52.84.150.55
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sU tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:15 IST
Nmap scan report for tinder.com (52.84.150.39)
Host is up (0.0045s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.54 52.84.150.60
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
33459/udp  closed unknown

Nmap done: 1 IP address (1 host up) scanned in 12.41 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sN tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:17 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0047s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.39 52.84.150.54
All 1000 scanned ports on tinder.com (52.84.150.60) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sF tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:18 IST
Nmap scan report for tinder.com (52.84.150.54)
Host is up (0.0028s latency).
Other addresses for tinder.com (not scanned): 52.84.150.39 52.84.150.55 52.84.150.60
All 1000 scanned ports on tinder.com (52.84.150.54) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

These three scan types (even more are possible with the `--scanflags` option described in the next section) exploit a subtle loophole in the [TCP RFC](#) to differentiate between open and closed ports. Page 65 of RFC 793 says that "if the [destination] port state is CLOSED .... an incoming segment not containing a RST causes a RST to be sent in response." Then the next page discusses packets sent to open ports without the SYN, RST, or ACK bits set, stating that: "you are unlikely to get here, but if you do, drop the segment, and return."

When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK. Nmap exploits this with three scan types: Null scan (`-sN`)

Does not set any bits (TCP flag header is 0)

FIN scan (`-sF`)

Sets just the TCP FIN bit.

Xmas scan (`-sX`)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

```
Activities Terminal Wed 15:20
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006

File Edit View Search Terminal Help
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sU tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:15 IST
Nmap scan report for tinder.com (52.84.150.39)
Host is up (0.0045s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.54 52.84.150.60
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
33459/udp  closed unknown

Nmap done: 1 IP address (1 host up) scanned in 12.41 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sN tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:17 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0047s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.39 52.84.150.54
All 1000 scanned ports on tinder.com (52.84.150.60) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sF tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:18 IST
Nmap scan report for tinder.com (52.84.150.54)
Host is up (0.0028s latency).
Other addresses for tinder.com (not scanned): 52.84.150.39 52.84.150.55 52.84.150.60
All 1000 scanned ports on tinder.com (52.84.150.54) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sX tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:19 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0032s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.54 52.84.150.39
All 1000 scanned ports on tinder.com (52.84.150.60) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 21.45 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006#
```

#### 4-sA (TCP ACK scan)

```
Activities Terminal Wed 15:21
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006

File Edit View Search Terminal Help
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
33459/udp  closed unknown

Nmap done: 1 IP address (1 host up) scanned in 12.41 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sN tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:17 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0047s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.39 52.84.150.54
All 1000 scanned ports on tinder.com (52.84.150.60) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sF tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:18 IST
Nmap scan report for tinder.com (52.84.150.54)
Host is up (0.0028s latency).
Other addresses for tinder.com (not scanned): 52.84.150.39 52.84.150.55 52.84.150.60
All 1000 scanned ports on tinder.com (52.84.150.54) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sX tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:19 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0032s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.54 52.84.150.39
All 1000 scanned ports on tinder.com (52.84.150.60) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 21.45 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006# nmap -sA tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:21 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0029s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    unfiltered http
443/tcp   unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 11.22 seconds
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006#
```

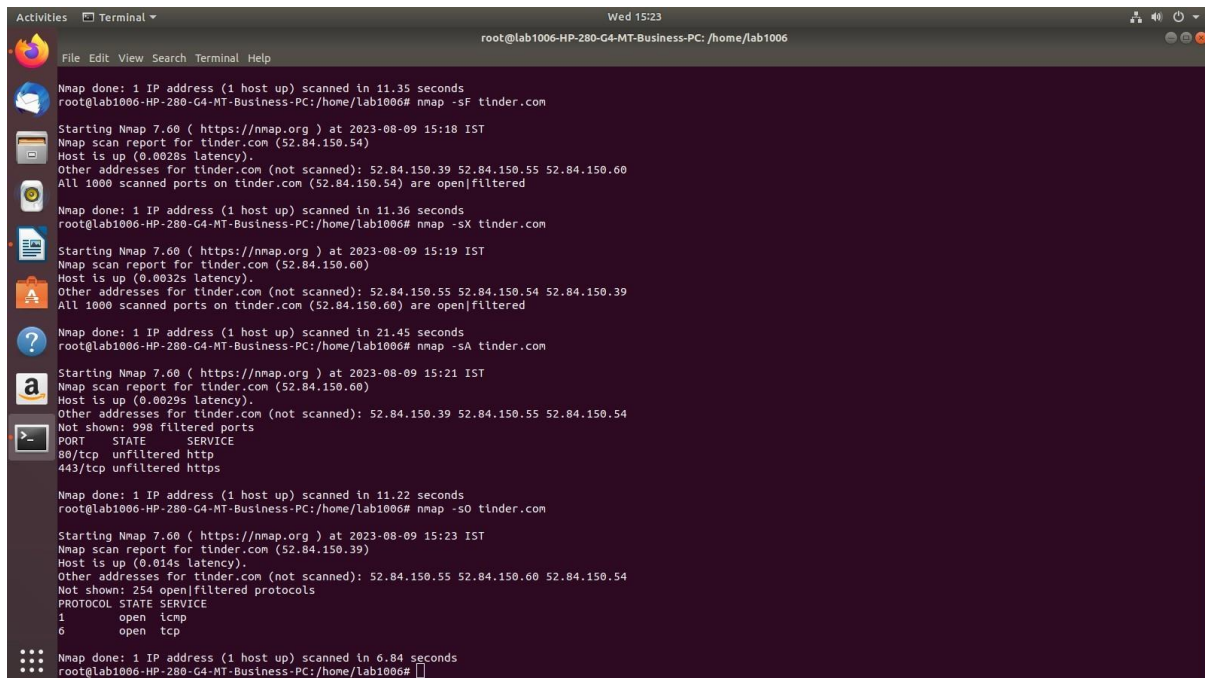
This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

ACK scan is enabled by specifying the `-sA` option. Its probe packet has only the ACK flag set (unless you use `--scanflags`). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is



undetermined. Ports that don't respond, or send certain ICMP error messages back, are labeled filtered. [Table 5.5](#) provides the full details.

## 5. -sO (IP protocol scan)



```
Activities Terminal
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006

Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sF tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:18 IST
Nmap scan report for tinder.com (52.84.150.54)
Host is up (0.0028s latency).
Other addresses for tinder.com (not scanned): 52.84.150.39 52.84.150.55 52.84.150.60
All 1000 scanned ports on tinder.com (52.84.150.54) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sX tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:19 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0032s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.54 52.84.150.39
All 1000 scanned ports on tinder.com (52.84.150.60) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 21.45 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sA tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:21 IST
Nmap scan report for tinder.com (52.84.150.60)
Host is up (0.0029s latency).
Other addresses for tinder.com (not scanned): 52.84.150.39 52.84.150.55 52.84.150.54
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    unfiltered http
443/tcp   unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 11.22 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sO tinder.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:23 IST
Nmap scan report for tinder.com (52.84.150.39)
Host is up (0.014s latency).
Other addresses for tinder.com (not scanned): 52.84.150.55 52.84.150.60 52.84.150.54
Not shown: 254 open|filtered protocols
PROTOCOL STATE SERVICE
1         open  icmp
6         open  tcp

Nmap done: 1 IP address (1 host up) scanned in 6.84 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers. Yet it still uses the -p option to select scanned protocol numbers, reports its results within the normal port table format, and even uses the same underlying scan engine as the true port scanning methods. So it is close enough to a port scan that it belongs here.

Besides being useful in its own right, protocol scan demonstrates the power of open-source software. While the fundamental idea is pretty simple, I had not thought to add it nor received any requests for such functionality. Then in the summer of 2000, Gerhard Rieger conceived the idea, wrote an excellent patch implementing it, and sent it to the *nmap-hackers* mailing list. I incorporated that patch into the Nmap tree and released a new version the next day. Few pieces of commercial software have users enthusiastic enough to design and contribute their own improvements!

## 6 -O (Enable OS detection)

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -O 192.168.0.119

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:36 IST
Nmap scan report for 192.168.0.119
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.0.119 are closed
MAC Address: 04:0E:3C:1A:5F:16 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.66 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

One of Nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting.

Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares the results to its nmap-os-db database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match. Each fingerprint includes a freeform textual description of the OS, and a classification which provides the vendor name (e.g. Sun), underlying OS (e.g. Solaris), OS generation (e.g. 10), and device type (general purpose, router, switch, game console, etc). Most fingerprints also have a Common Platform Enumeration (CPE) representation, like `cpe:/o:linux:linux_kernel:2.6`.

## 7 nmap -sP 192.168.0.\*

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sP 192.168.0.*

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:39 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.00042s latency).
MAC Address: AC:15:82:89:9E:29 (Unknown)
Nmap scan report for 192.168.0.105
Host is up (-0.100s latency).
MAC Address: A4:AE:12:84:7F:CF (Unknown)
Nmap scan report for 192.168.0.114
Host is up (-0.10s latency).
MAC Address: 04:0E:3C:19:2E:0F (Unknown)
Nmap scan report for 192.168.0.115
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:1A:5C:A0 (Unknown)
Nmap scan report for 192.168.0.116
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:1A:60:A0 (Unknown)
Nmap scan report for 192.168.0.117
Host is up (-0.10s latency).
MAC Address: 04:0E:3C:19:2D:1C (Unknown)
Nmap scan report for 192.168.0.118
Host is up (0.00080s latency).
MAC Address: E4:54:E8:C6:37:76 (Unknown)
Nmap scan report for 192.168.0.119
Host is up (0.00020s latency).
MAC Address: 04:0E:3C:1A:5F:16 (Unknown)
Nmap scan report for 192.168.0.121
Host is up (-0.099s latency).
MAC Address: 90:8D:78:7E:5A:B3 (D-Link International)
Nmap scan report for 192.168.0.123
Host is up (-0.100s latency).
MAC Address: F4:39:09:49:0A:33 (Unknown)
Nmap scan report for 192.168.0.126
Host is up (-0.10s latency).
MAC Address: 04:0E:3C:1A:61:7F (Unknown)
Nmap scan report for 192.168.0.133
Host is up (-0.10s latency).
MAC Address: A0:8C:FD:05:AD:A1 (Hewlett Packard)
Nmap scan report for 192.168.0.135
Host is up (-0.10s latency).
MAC Address: A0:8C:FD:0D:8C:AE (Hewlett Packard)
Nmap scan report for 192.168.0.141
Host is up (-0.100s latency).
```

A ping sweep (also known as an ICMP sweep) is a basic [network scanning](#) technique used to determine which of a range of [IP addresses](#) map to live [hosts](#) (computers).

Whereas a single [ping](#) will tell whether one specified host computer exists on the network, a ping sweep consists of [ICMP](#) (Internet Control Message Protocol) *echo requests* sent to multiple hosts. To do this, the ping requires an address to send the echo request to, which can be an IP address or a web server domain name.

If a given address is live, it will return an ICMP *echo reply*. To disable ping sweeps on a network, administrators can block ICMP *echo requests* from outside sources. However, ICMP *timestamp* and *Address Mask requests* can be used in a similar manner.

**CONCLUSION :-** By this assignment we implemented various different nmap network scanning commands and used Wireshark.