Assignment Number: 8

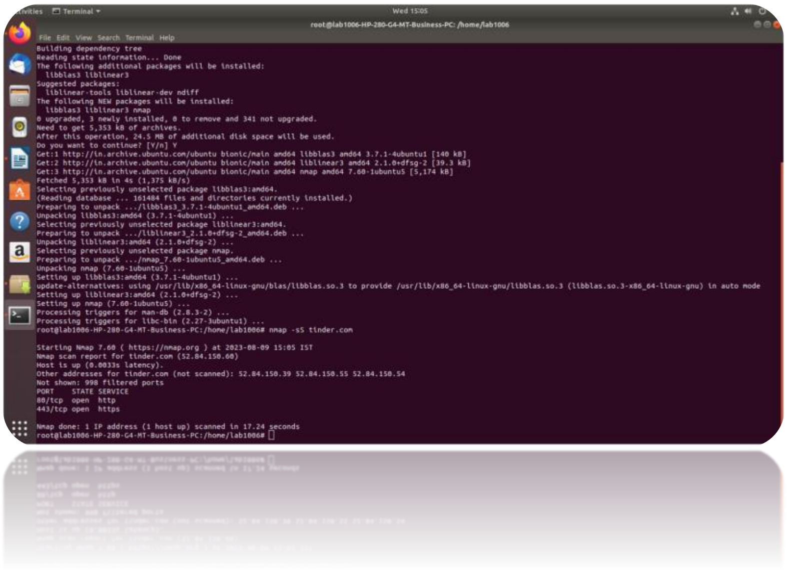
Name: Divya Shah; Branch: I.T (T.E.); Roll Number: 115 24/08/2023

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

LO mapped: LO4

Theory:

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

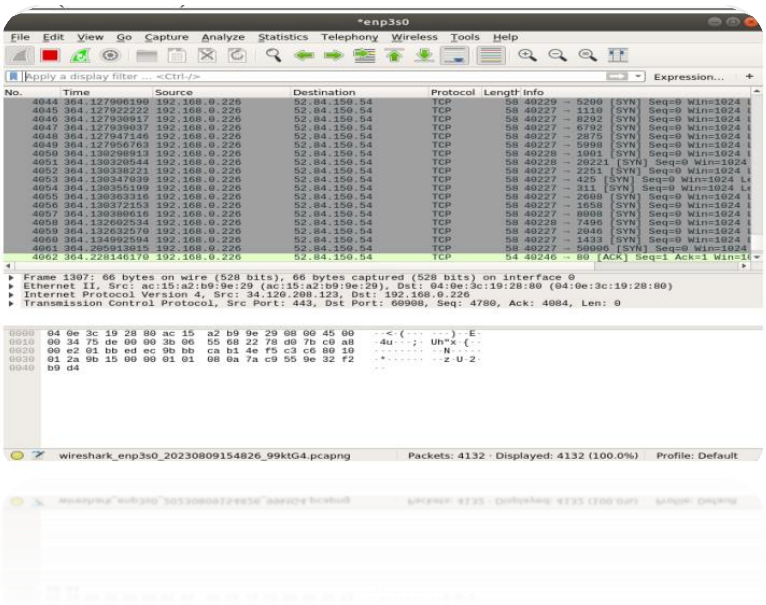


Activities
Terminal
Wed 15:05
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear3
Suggested packages:
  liblinear-tools liblinear-dev ndiff
The following NEW packages will be installed:
  libblas3 liblinear3 nmap
0 upgraded, 3 newly installed, 0 to remove and 341 not upgraded.
Need to get 5,353 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libblas3 amd64 3.7.1-4ubuntu1 [140 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 liblinear3 amd64 2.1.0+dfsg-2 [39.3 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 nmap amd64 7.60-1ubuntu5 [5,174 kB]
Fetched 5,353 kB in 4s (1,375 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 161484 files and directories currently installed.)
Preparing to unpack .../libblas3_3.7.1-4ubuntu1_amd64.deb ...
Unpacking libblas3:amd64 (3.7.1-4ubuntu1) ...
Selecting previously unselected package liblinear3:amd64.
Preparing to unpack .../liblinear3_2.1.0+dfsg-2_amd64.deb ...
Unpacking liblinear3:amd64 (2.1.0+dfsg-2) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.60-1ubuntu5_amd64.deb ...
Unpacking nmap (7.60-1ubuntu5) ...
Setting up libblas3:amd64 (3.7.1-4ubuntu1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux-gnu) in auto mode
Setting up liblinear3:amd64 (2.1.0+dfsg-2) ...
Setting up nmap (7.60-1ubuntu5) ...
Processing triggers for man-db (2.8.3-2) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS 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# 
```

II. -sS (TCP SYN scan)

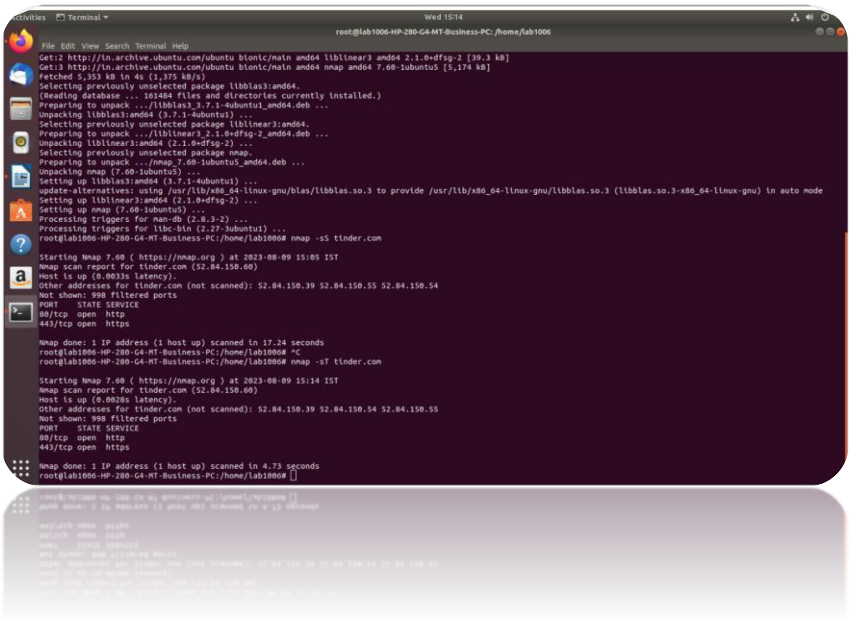
SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. SYN scan works against 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 the open, closed, and filtered states. This technique is often referred to as half-open scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and then wait for a response. A SYN/ACK indicates the port is listening (open), while a RST (reset) is indicative of a non-listener. If no response is received after several retransmissions, the port is marked as filtered. The port is also marked filtered if an ICMP unreachable error (type 3, code 0, 1, 2, 3, 9, 10, or 13) is received. The port is also considered open if a SYN packet (without the ACK flag) is received in response. This can be due to an extremely rare TCP feature known as a simultaneous open or split handshake connection


*enp3s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.    Time           Source          Destination     Protocol Length Info
  4044 364.127906190  192.168.0.226   52.84.150.54    TCP        58 40229 → 5200 [SYN] Seq=0 Win=1024 L
  4045 364.127922222  192.168.0.226   52.84.150.54    TCP        58 40227 → 1110 [SYN] Seq=0 Win=1024 L
  4046 364.127930917  192.168.0.226   52.84.150.54    TCP        58 40227 → 8292 [SYN] Seq=0 Win=1024 L
  4047 364.127939037  192.168.0.226   52.84.150.54    TCP        58 40227 → 6792 [SYN] Seq=0 Win=1024 L
  4048 364.127947146  192.168.0.226   52.84.150.54    TCP        58 40227 → 2875 [SYN] Seq=0 Win=1024 L
  4049 364.127956763  192.168.0.226   52.84.150.54    TCP        58 40227 → 5998 [SYN] Seq=0 Win=1024 L
  4050 364.130298913  192.168.0.226   52.84.150.54    TCP        58 40228 → 1001 [SYN] Seq=0 Win=1024 L
  4051 364.130320544  192.168.0.226   52.84.150.54    TCP        58 40228 → 20221 [SYN] Seq=0 Win=1024
  4052 364.130338221  192.168.0.226   52.84.150.54    TCP        58 40227 → 2251 [SYN] Seq=0 Win=1024 L
  4053 364.130347039  192.168.0.226   52.84.150.54    TCP        58 40227 → 425 [SYN] Seq=0 Win=1024 Le
  4054 364.130355199  192.168.0.226   52.84.150.54    TCP        58 40227 → 311 [SYN] Seq=0 Win=1024 Le
  4055 364.130363316  192.168.0.226   52.84.150.54    TCP        58 40227 → 2608 [SYN] Seq=0 Win=1024 L
  4056 364.130372153  192.168.0.226   52.84.150.54    TCP        58 40227 → 1658 [SYN] Seq=0 Win=1024 L
  4057 364.130380616  192.168.0.226   52.84.150.54    TCP        58 40227 → 8008 [SYN] Seq=0 Win=1024 L
  4058 364.132602534  192.168.0.226   52.84.150.54    TCP        58 40228 → 7496 [SYN] Seq=0 Win=1024 L
  4059 364.132632570  192.168.0.226   52.84.150.54    TCP        58 40227 → 2046 [SYN] Seq=0 Win=1024 L
  4060 364.134992594  192.168.0.226   52.84.150.54    TCP        58 40227 → 1433 [SYN] Seq=0 Win=1024 L
  4061 364.205913015  192.168.0.226   52.84.150.54    TCP        58 40227 → 50006 [SYN] Seq=0 Win=1024
  4062 364.228146170  192.168.0.226   52.84.150.54    TCP        54 40246 → 80 [ACK] Seq=1 Ack=1 Win=16

▸ Frame 1307: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: ac:15:a2:b9:9e:29 (ac:15:a2:b9:9e:29), Dst: 04:0e:3c:19:28:80 (04:0e:3c:19:28:80)
▸ Internet Protocol Version 4, Src: 34.120.208.123, Dst: 192.168.0.226
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 60908, Seq: 4780, Ack: 4084, Len: 0

0000  04 0e 3c 19 28 80 ac 15  a2 b9 9e 29 08 00 45 00   ··<·(···  ···)··E·
0010  00 34 75 de 00 00 3b 06  55 68 22 78 d0 7b c0 a8   ·4u···;·  Uh"x·{··
0020  00 e2 01 bb ed ec 9b bb  ca b1 4e f5 c3 c6 80 10   ········  ··N·····
0030  01 2a 9b 15 00 00 01 01  08 0a 7a c9 55 9e 32 f2   ·*······  ··z·U·2·
0040  b9 d4                                              ··

wireshark_enp3s0_20230809154826_99ktG4.pcapng    Packets: 4132 · Displayed: 4132 (100.0%)    Profile: Default
```

III. -sT (TCP connect scan)

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. 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. When SYN scan is available, it is usually a better choice. Nmap has less control over the high level connect call than with raw packets, making it less efficient. The system call completes connections to open target ports rather than performing the half-open reset that SYN scan does. Not only does this take longer and require more packets to obtain the same information, but target machines are more likely to log the connection. A decent IDS will catch either, but most machines have no such alarm system. Many services on your average Unix system will add a note to syslog, and sometimes a cryptic error message, when Nmap connects and then closes the connection without sending data. Truly pathetic services crash when this happens, though that is uncommon. An administrator who sees a bunch of connection attempts in her logs from a single system should know that she has been connect scanned.

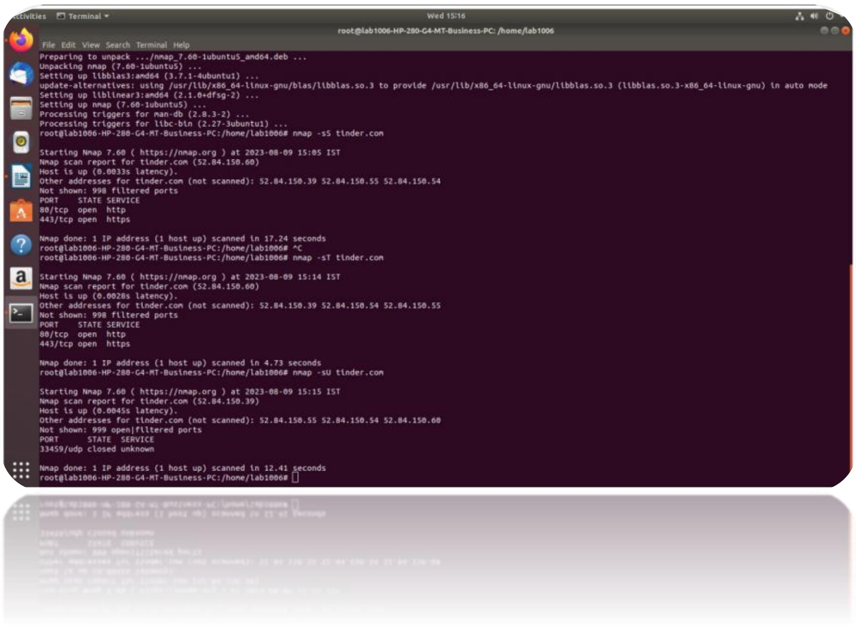


Activities
Terminal
Wed 15:14
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
Get:2 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 liblinear3 amd64 2.1.0+dfsg-2 [39.3 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 nmap amd64 7.60-1ubuntu5 [5,174 kB]
Fetched 5,353 kB in 4s (1,375 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 161484 files and directories currently installed.)
Preparing to unpack .../libblas3_3.7.1-4ubuntu1_amd64.deb ...
Unpacking libblas3:amd64 (3.7.1-4ubuntu1) ...
Selecting previously unselected package liblinear3:amd64.
Preparing to unpack .../liblinear3_2.1.0+dfsg-2_amd64.deb ...
Unpacking liblinear3:amd64 (2.1.0+dfsg-2) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.60-1ubuntu5_amd64.deb ...
Unpacking nmap (7.60-1ubuntu5) ...
Setting up libblas3:amd64 (3.7.1-4ubuntu1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux-gnu) in auto mode
Setting up liblinear3:amd64 (2.1.0+dfsg-2) ...
Setting up nmap (7.60-1ubuntu5) ...
Processing triggers for man-db (2.8.3-2) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS 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# 
```

IV. -sU (UDP scans)

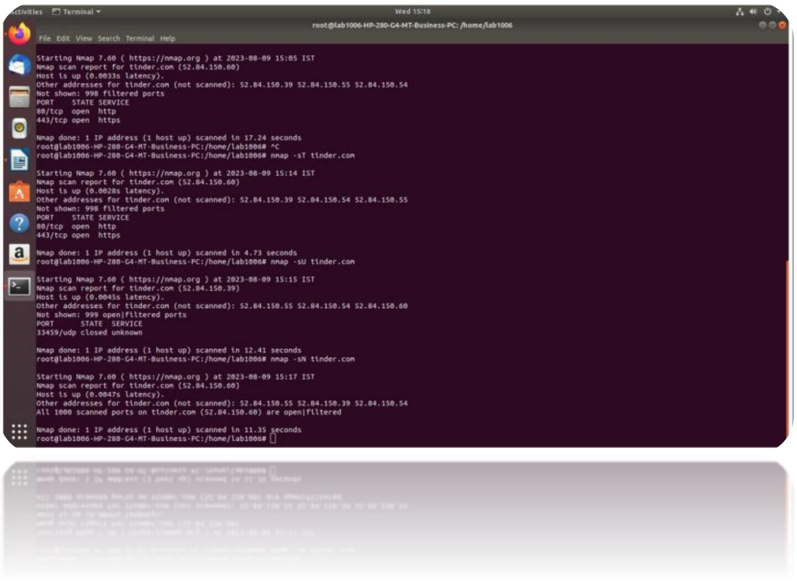
While most popular services on the Internet run over the TCP protocol, UDP services are widely deployed. DNS, SNMP, and DHCP (registered ports 53, 161/162, and 67/68) are three of the most common. Because UDP scanning is generally slower and more difficult than TCP, some security auditors ignore these ports. This is a mistake, as exploitable UDP services are quite common, and attackers certainly don't ignore the whole protocol. Fortunately, Nmap can help inventory UDP ports. UDP scan is activated with the -sU option. It can be combined with a TCP scan type such as SYN scan (-sS) to check both protocols during the same run. UDP scan works by sending a UDP packet to every targeted port. For some common ports such as 53 and 161, a protocol-specific payload is sent to increase response rate, but for most ports the packet is empty unless the --data, --data-string, or --data-length options are specified. If an ICMP port unreachable error (type 3, code 3) is returned, the port is closed. Other ICMP unreachable errors (type 3, codes 0, 1, 2, 9, 10, or 13) mark the port as filtered. Occasionally, a service will respond with a UDP packet, proving that it is open. 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 communication. Version detection (-sV) can be used to help differentiate the truly open ports from the filtered ones. A big challenge with UDP scanning is doing it quickly. Open and filtered ports rarely send any response, leaving Nmap to time out and then conduct retransmissions just in case the probe or response were lost. Closed ports are often an even bigger problem. They usually send back an ICMP port unreachable error. But unlike the RST packets sent by closed TCP ports in response to a SYN or connect scan, many hosts rate limit ICMP port unreachable messages by default. Linux and Solaris are particularly strict about this. For example, the Linux 2.4.20 kernel limits destination unreachable messages to one per second


Activities
Terminal
Wed 15:16
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

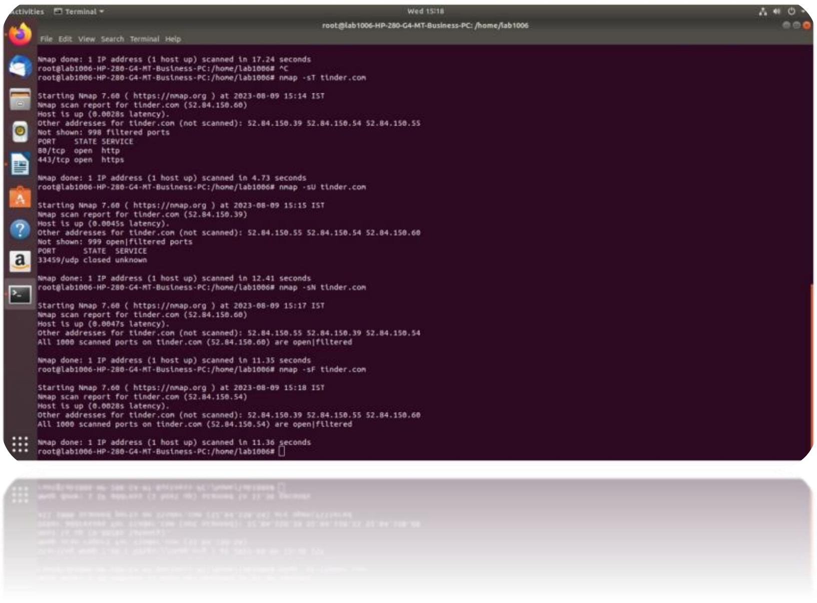
```
Preparing to unpack .../nmap_7.60-1ubuntu5_amd64.deb ...
Unpacking nmap (7.60-1ubuntu5) ...
Setting up libblas3:amd64 (3.7.1-4ubuntu1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux-gnu) in auto mode
Setting up liblinear3:amd64 (2.1.0+dfsg-2) ...
Setting up nmap (7.60-1ubuntu5) ...
Processing triggers for man-db (2.8.3-2) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS 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# 
```

V. -sN; -sF; -sX (TCP NULL, FIN, and Xmas scans)

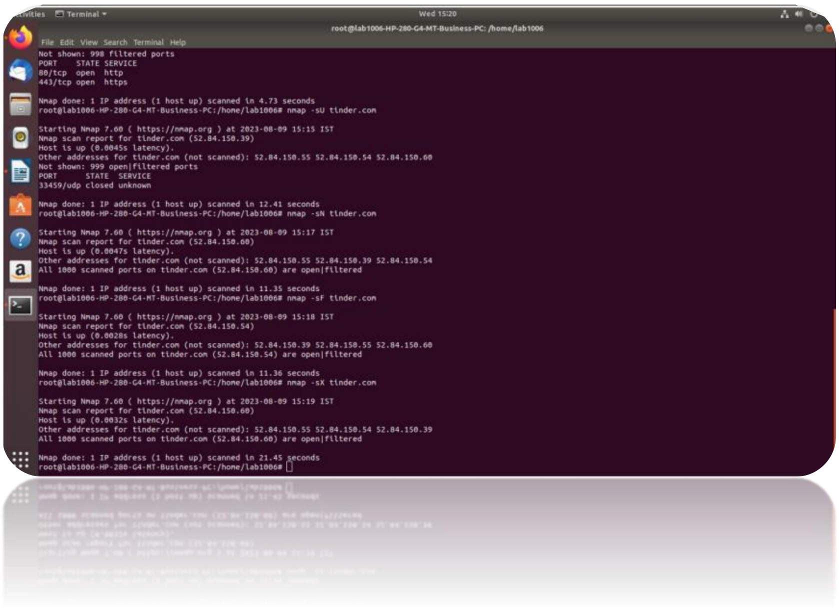
These three scan types (even more are possible with the --scanflags option described in the next section) exploit a subtle loophole in the TCP RFC to differentiate between open and closed ports. Page 65 of RFC 793 says that "if the [destination] port state is CLOSED .... an incoming segment not containing 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:


Activities
Terminal
Wed 15:18
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
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
File Edit View Search Terminal Help

```
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# 
```

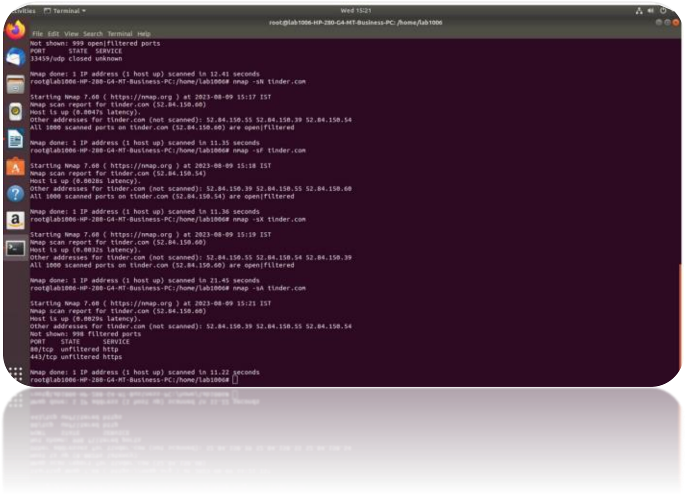

Activities
Terminal
Wed 15:20
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
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# 
```

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree. These three scan types are exactly the same in behaviour except for the TCP flags set in probe packets. If a RST packet is received, the port is considered closed, while no response means it is open filtered. The port is marked filtered if an ICMP unreachable error (type 3, code 0, 1, 2, 3, 9, 10, or 13) is received.

VI. -sA (TCP ACK scan)

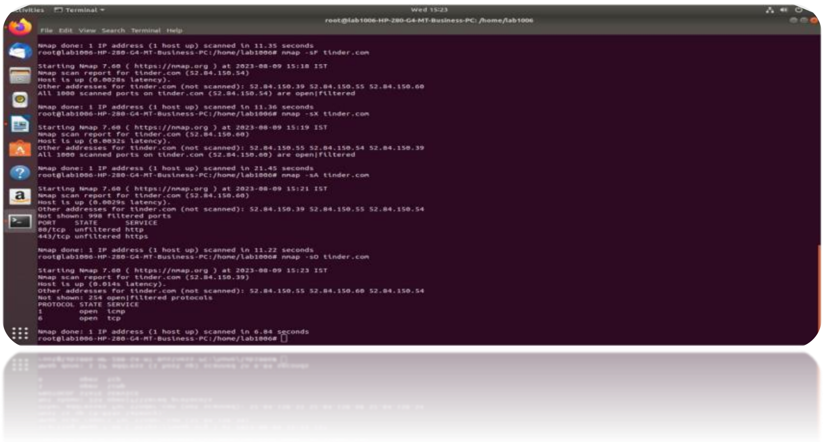
This scan is different than the others discussed so far in that it never determines open (or even open (filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered. The ACK scan probe packet has only the ACK flag set (unless you use –scan flags). 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 (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labelled filtered


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).
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# 
```

VII. -sO (IP protocol scan)

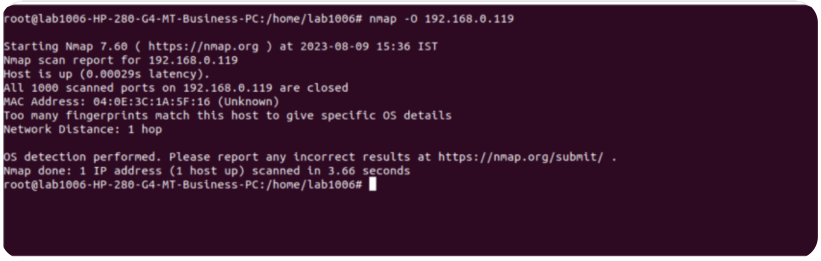
IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers. Yet it still uses the -p option to select scanned protocol numbers, 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 announce mailing list (then called Nmap-hackers). I incorporated that patch into the Nmap tree and released a new version the next day.


Activities
Terminal
Wed 15:23
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
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# 
```

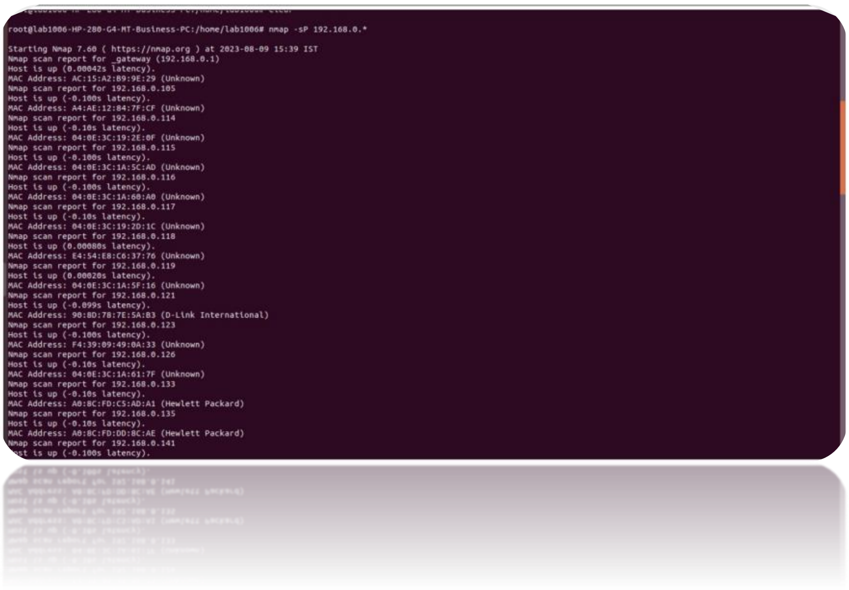
VIII. -O (Enable OS detection)

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's 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. If Nmap is unable to guess the OS of a machine, and conditions are good (e.g. at least one open port and one closed port were found), Nmap will provide a URL you can use to submit the fingerprint if you know (for sure) the OS running on the machine. By doing this you contribute to the pool of operating systems known to Nmap and thus it will be more accurate for everyone. OS detection enables some other tests which make use of information that is gathered during the process anyway. One of these is TCP Sequence Predictability Classification. This measures approximately how hard it is to establish a forged TCP connection against the remote host. It is useful for exploiting source-IP based trust relationships (rlogin, firewall filters, etc) or for hiding the source of an attack. This sort of spoofing is rarely performed any more, but many machines are still vulnerable to it. The actual difficulty number is based on statistical sampling and may fluctuate. It is generally better to use the English classification such as “worthy challenge” or “trivial joke”. This is only reported in normal output in verbose (-v) mode. When verbose mode is enabled along with -O, IP ID sequence generation is also reported. Most machines are in the “incremental” class, which means that they increment the ID field in the IP header for each packet they send. This makes them vulnerable to several advanced information gathering and spoofing attacks



```
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# 
```

IX. 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:A2:B9:9E: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:AD (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:C5:AD:A1 (Hewlett Packard)
Nmap scan report for 192.168.0.135
Host is up (-0.10s latency).
MAC Address: A0:8C:FD:DD:8C:AE (Hewlett Packard)
Nmap scan report for 192.168.0.141
ost is up (-0.100s latency).
```

Conclusion: We implemented Installation of NMAP and using it with different options to scan open ports, perform OS fingerprinting, ping scan, TCP port scan, UDP port scan, etc.