ASSIGNMENT – 8

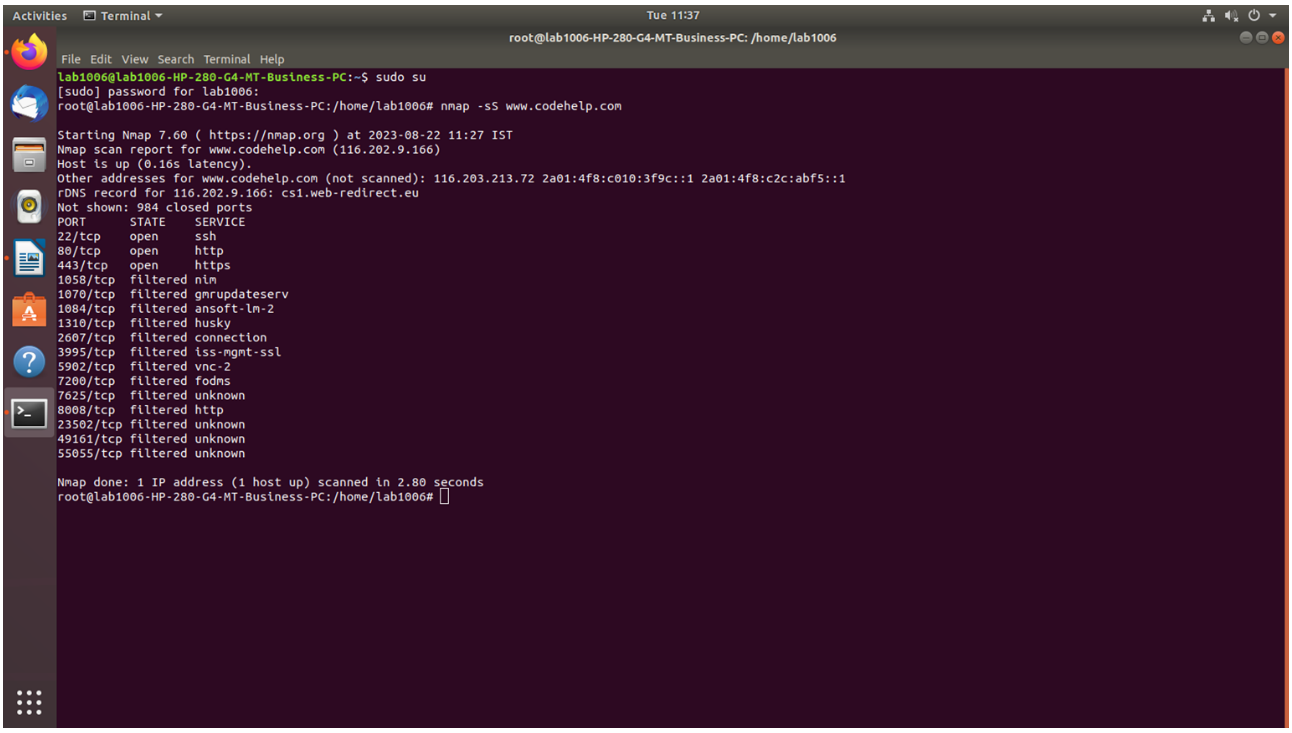
Aim: To perform port scanning using port scanning techniques Tcp Syn, Tcp Connect, Tcp ACK, FIN, NULL XMUS, IP Protocol, OS detection, Ping and UDP .

LO 4 :
Use tools like sniffers, port scanners and other related tools for analyzing packets in network

Command – [-sS (TCP SYN scan)]
- nmap -sS www.codehelp.com

Description -
-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.



Activities
Terminal
Tue 11:37
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo su
[sudo] password for lab1006:
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS www.codehelp.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 11:27 IST
Nmap scan report for www.codehelp.com (116.202.9.166)
Host is up (0.16s latency).
Other addresses for www.codehelp.com (not scanned): 116.203.213.72 2a01:4f8:c010:3f9c::1 2a01:4f8:c2c:abf5::1
rDNS record for 116.202.9.166: cs1.web-redirect.eu
Not shown: 984 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
443/tcp   open     https
1058/tcp  filtered nim
1070/tcp  filtered gmrupdateserv
1084/tcp  filtered ansoft-lm-2
1310/tcp  filtered husky
2607/tcp  filtered connection
3995/tcp  filtered iss-mgmt-ssl
5902/tcp  filtered vnc-2
7200/tcp  filtered fodms
7625/tcp  filtered unknown
8008/tcp  filtered http
23502/tcp filtered unknown
49161/tcp filtered unknown
55055/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 
```

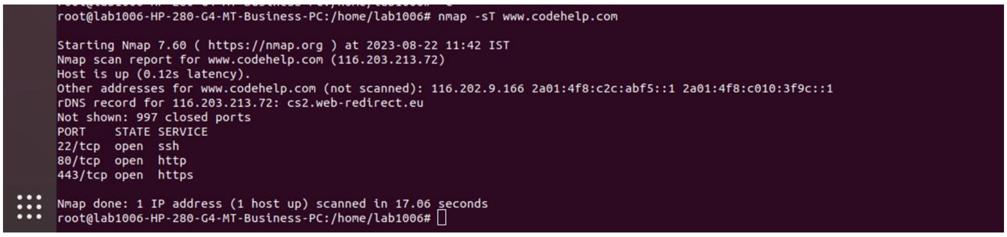
Command - [-sT (TCP connect scan)]

- nmap -sT www.codehelp.com

Description -

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.



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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 11:42 IST
Nmap scan report for www.codehelp.com (116.203.213.72)
Host is up (0.12s latency).
Other addresses for www.codehelp.com (not scanned): 116.202.9.166 2a01:4f8:c2c:abf5::1 2a01:4f8:c010:3f9c::1
rDNS record for 116.203.213.72: cs2.web-redirect.eu
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.06 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 
```

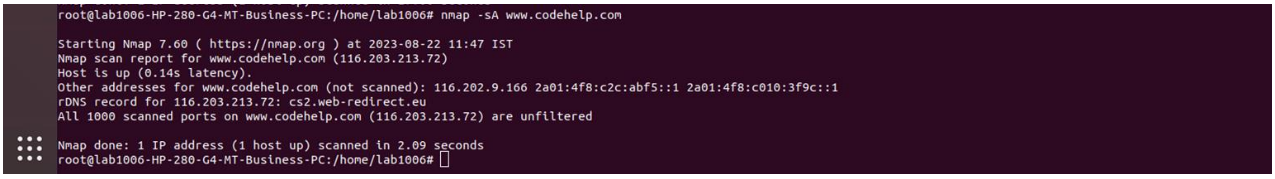
Command - [-sA (TCP ACK scan)]

- nmap -sA www.codehelp.com

Description -

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 --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 (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labeled filtered.



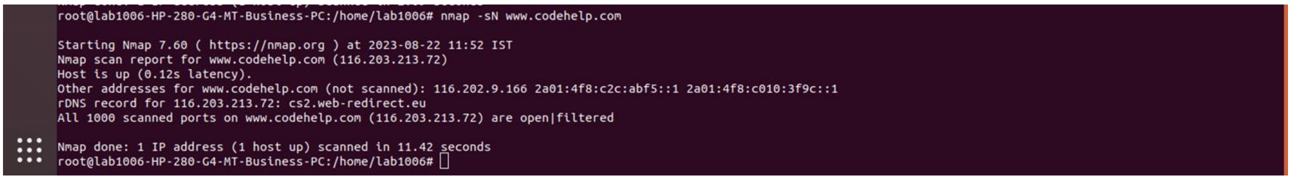
```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sA www.codehelp.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 11:47 IST
Nmap scan report for www.codehelp.com (116.203.213.72)
Host is up (0.14s latency).
Other addresses for www.codehelp.com (not scanned): 116.202.9.166 2a01:4f8:c2c:abf5::1 2a01:4f8:c010:3f9c::1
rDNS record for 116.203.213.72: cs2.web-redirect.eu
All 1000 scanned ports on www.codehelp.com (116.203.213.72) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 
```

Command - [Null scan (-sN)]

- nmap -sN www.codehelp.com

Description -

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



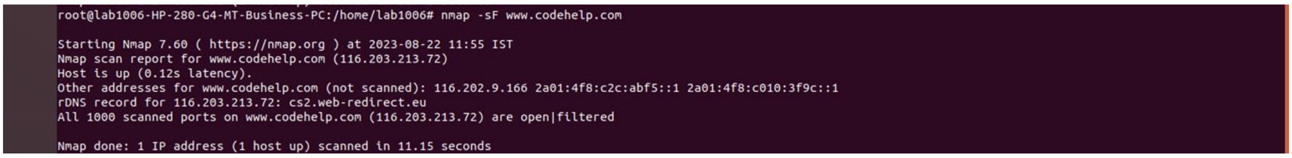
```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sN www.codehelp.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 11:52 IST
Nmap scan report for www.codehelp.com (116.203.213.72)
Host is up (0.12s latency).
Other addresses for www.codehelp.com (not scanned): 116.202.9.166 2a01:4f8:c2c:abf5::1 2a01:4f8:c010:3f9c::1
rDNS record for 116.203.213.72: cs2.web-redirect.eu
All 1000 scanned ports on www.codehelp.com (116.203.213.72) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.42 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 
```

Command – [FIN scan (-sF)]

- nmap -sF www.codehelp.com

Description -

Sets just the TCP FIN bit.



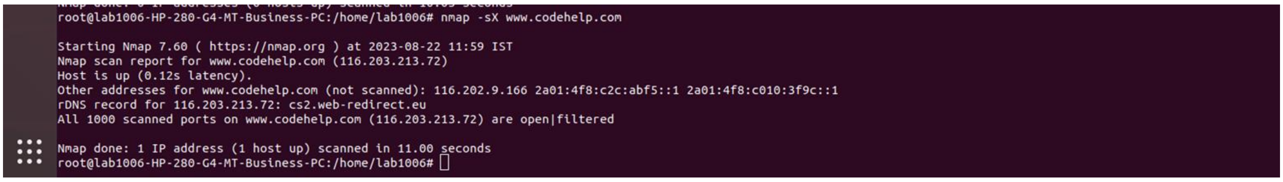
```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sF www.codehelp.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 11:55 IST
Nmap scan report for www.codehelp.com (116.203.213.72)
Host is up (0.12s latency).
Other addresses for www.codehelp.com (not scanned): 116.202.9.166 2a01:4f8:c2c:abf5::1 2a01:4f8:c010:3f9c::1
rDNS record for 116.203.213.72: cs2.web-redirect.eu
All 1000 scanned ports on www.codehelp.com (116.203.213.72) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.15 seconds
```

Command - [Xmas scan (-sX)]

- nmap -sX www.codehelp.com

Description -

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



```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sX www.codehelp.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 11:59 IST
Nmap scan report for www.codehelp.com (116.203.213.72)
Host is up (0.12s latency).
Other addresses for www.codehelp.com (not scanned): 116.202.9.166 2a01:4f8:c2c:abf5::1 2a01:4f8:c010:3f9c::1
rDNS record for 116.203.213.72: cs2.web-redirect.eu
All 1000 scanned ports on www.codehelp.com (116.203.213.72) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.00 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 
```

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

These three scan types are exactly the same in behavior 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.

The key advantage to these scan types is that they can sneak through certain non-stateful firewalls and packet filtering routers. Another advantage is that these scan types are a little more stealthy than even a SYN scan. Don't count on this though—most modern IDS products can be configured to detect them. The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled closed. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400. This scan does work against most Unix-based systems though.

Command - [-sO (IP protocol scan)]

- nmap -sO www.codehelp.com

Description -

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.

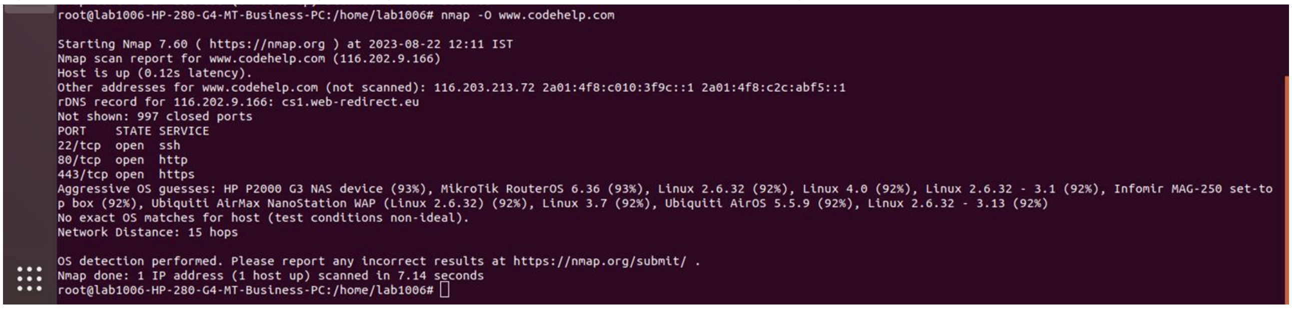
Besides being useful in its own right, protocol scan demonstrates the power of open-source software. While the fundamental idea is pretty simple, I had not thought to add it nor received any requests for such functionality. Then in the summer of 2000, Gerhard Rieger conceived the idea, wrote an excellent 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. Few pieces of commercial software have users enthusiastic enough to design and contribute their own improvements!

Command -

- nmap -sO www.codehelp.com

Description -

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, and device type (general purpose, router, switch, game console, etc).



```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -O www.codehelp.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 12:11 IST
Nmap scan report for www.codehelp.com (116.202.9.166)
Host is up (0.12s latency).
Other addresses for www.codehelp.com (not scanned): 116.203.213.72 2a01:4f8:c010:3f9c::1 2a01:4f8:c2c:abf5::1
rDNS record for 116.202.9.166: cs1.web-redirect.eu
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
Aggressive OS guesses: HP P2000 G3 NAS device (93%), MikroTik RouterOS 6.36 (93%), Linux 2.6.32 (92%), Linux 4.0 (92%), Linux 2.6.32 - 3.1 (92%), Infomir MAG-250 set-to
p box (92%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (92%), Linux 3.7 (92%), Ubiquiti AirOS 5.5.9 (92%), Linux 2.6.32 - 3.13 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.14 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 
```

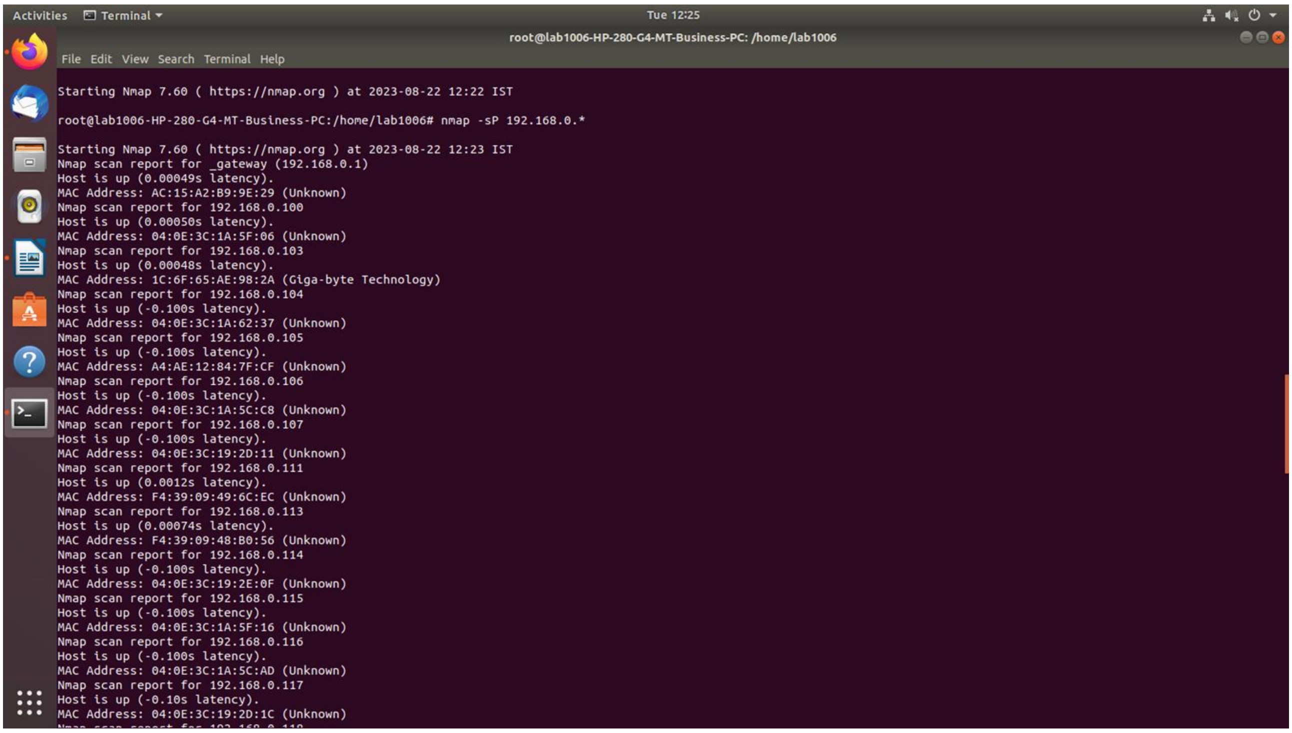
Command - [nmap -sP ip address]

Description –

Ping Scan(-sP):

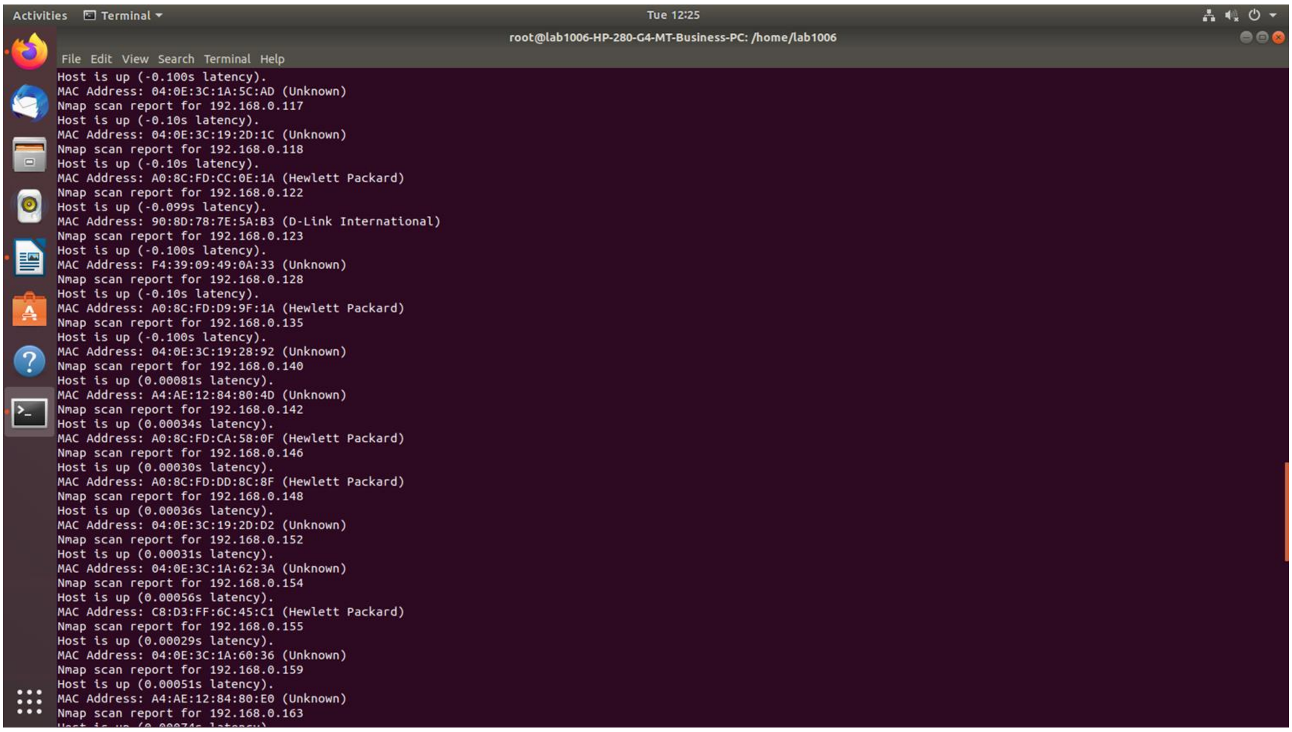
The `-sP` option in Nmap is used to perform a Ping Scan. It's used to discover live hosts on a network by sending ICMP Echo Request (ping) packets to potential target hosts and analyzing their responses.

Ping Scan (`-sP`) is a simple method to identify hosts that are online in a network without performing any port scanning.



Activities
Terminal
Tue 12:25
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 12:22 IST

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 12:23 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.00049s latency).
MAC Address: AC:15:A2:B9:9E:29 (Unknown)
Nmap scan report for 192.168.0.100
Host is up (0.00050s latency).
MAC Address: 04:0E:3C:1A:5F:06 (Unknown)
Nmap scan report for 192.168.0.103
Host is up (0.00048s latency).
MAC Address: 1C:6F:65:AE:98:2A (Giga-byte Technology)
Nmap scan report for 192.168.0.104
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:1A:62:37 (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 192.168.0.106
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:1A:5C:C8 (Unknown)
Nmap scan report for 192.168.0.107
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:19:2D:11 (Unknown)
Nmap scan report for 192.168.0.111
Host is up (0.0012s latency).
MAC Address: F4:39:09:49:6C:EC (Unknown)
Nmap scan report for 192.168.0.113
Host is up (0.00074s latency).
MAC Address: F4:39:09:48:B0:56 (Unknown)
Nmap scan report for 192.168.0.114
Host is up (-0.100s 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:5F:16 (Unknown)
Nmap scan report for 192.168.0.116
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:1A:5C:AD (Unknown)
Nmap scan report for 192.168.0.117
Host is up (-0.10s latency).
MAC Address: 04:0E:3C:19:2D:1C (Unknown)
```

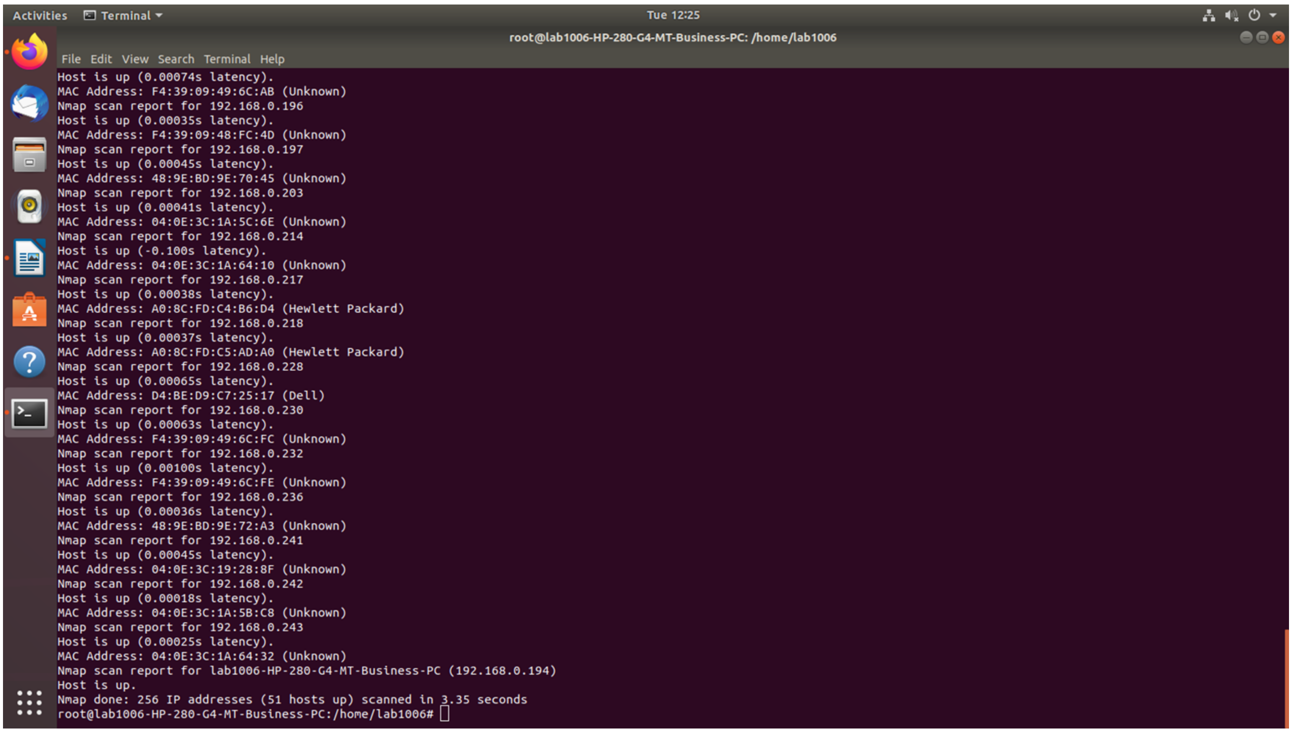


Activities
Terminal
Tue 12:25
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:1A:5C:AD (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 (-0.10s latency).
MAC Address: A0:8C:FD:CC:0E:1A (Hewlett Packard)
Nmap scan report for 192.168.0.122
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 192.168.0.128
Host is up (-0.10s latency).
MAC Address: A0:8C:FD:D9:9F:1A (Hewlett Packard)
Nmap scan report for 192.168.0.135
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:19:28:92 (Unknown)
Nmap scan report for 192.168.0.140
Host is up (0.00081s latency).
MAC Address: A4:AE:12:84:80:4D (Unknown)
Nmap scan report for 192.168.0.142
Host is up (0.00034s latency).
MAC Address: A0:8C:FD:CA:58:0F (Hewlett Packard)
Nmap scan report for 192.168.0.146
Host is up (0.00030s latency).
MAC Address: A0:8C:FD:DD:8C:8F (Hewlett Packard)
Nmap scan report for 192.168.0.148
Host is up (0.00036s latency).
MAC Address: 04:0E:3C:19:2D:D2 (Unknown)
Nmap scan report for 192.168.0.152
Host is up (0.00031s latency).
MAC Address: 04:0E:3C:1A:62:3A (Unknown)
Nmap scan report for 192.168.0.154
Host is up (0.00056s latency).
MAC Address: C8:D3:FF:6C:45:C1 (Hewlett Packard)
Nmap scan report for 192.168.0.155
Host is up (0.00029s latency).
MAC Address: 04:0E:3C:1A:60:36 (Unknown)
Nmap scan report for 192.168.0.159
Host is up (0.00051s latency).
MAC Address: A4:AE:12:84:80:E0 (Unknown)
Nmap scan report for 192.168.0.163
```

Command - [ ]

Description -

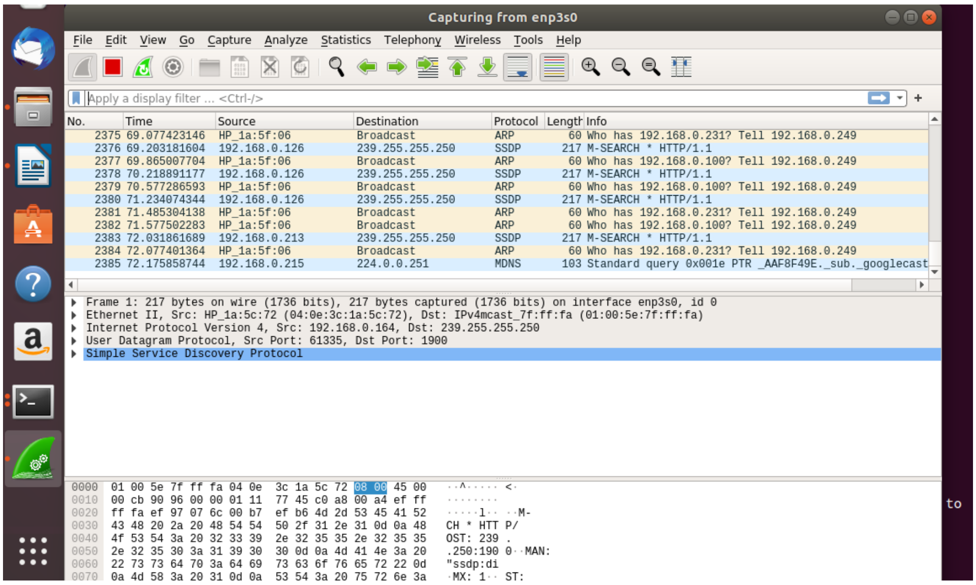

Activities
Terminal
Tue 12:25
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
Host is up (0.00074s latency).
MAC Address: F4:39:09:49:6C:AB (Unknown)
Nmap scan report for 192.168.0.196
Host is up (0.00035s latency).
MAC Address: F4:39:09:48:FC:4D (Unknown)
Nmap scan report for 192.168.0.197
Host is up (0.00045s latency).
MAC Address: 48:9E:BD:9E:70:45 (Unknown)
Nmap scan report for 192.168.0.203
Host is up (0.00041s latency).
MAC Address: 04:0E:3C:1A:5C:6E (Unknown)
Nmap scan report for 192.168.0.214
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:1A:64:10 (Unknown)
Nmap scan report for 192.168.0.217
Host is up (0.00038s latency).
MAC Address: A0:8C:FD:C4:B6:D4 (Hewlett Packard)
Nmap scan report for 192.168.0.218
Host is up (0.00037s latency).
MAC Address: A0:8C:FD:C5:AD:A0 (Hewlett Packard)
Nmap scan report for 192.168.0.228
Host is up (0.00065s latency).
MAC Address: D4:BE:D9:C7:25:17 (Dell)
Nmap scan report for 192.168.0.230
Host is up (0.00063s latency).
MAC Address: F4:39:09:49:6C:FC (Unknown)
Nmap scan report for 192.168.0.232
Host is up (0.00100s latency).
MAC Address: F4:39:09:49:6C:FE (Unknown)
Nmap scan report for 192.168.0.236
Host is up (0.00036s latency).
MAC Address: 48:9E:BD:9E:72:A3 (Unknown)
Nmap scan report for 192.168.0.241
Host is up (0.00045s latency).
MAC Address: 04:0E:3C:19:28:8F (Unknown)
Nmap scan report for 192.168.0.242
Host is up (0.00018s latency).
MAC Address: 04:0E:3C:1A:5B:C8 (Unknown)
Nmap scan report for 192.168.0.243
Host is up (0.00025s latency).
MAC Address: 04:0E:3C:1A:64:32 (Unknown)
Nmap scan report for lab1006-HP-280-G4-MT-Business-PC (192.168.0.194)
Host is up.
Nmap done: 256 IP addresses (51 hosts up) scanned in 3.35 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 
```

UDP Scan (-sU):

UDP unlike TCP, doesn’t perform a handshake to establish a connection before sending data packets to the target port but rather sends the packets hoping that the packets would be received by the target port. That is why UDP connections are often called “stateless”. This type of connection is more efficient when speed dwarfs quality, like in video sharing. As there will be no acknowledgment from the target port whether it has received the packet, UDP scans become more difficult and very much slower.

WIRESHARK


Capturing from enp3s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
to

```
No.    Time           Source           Destination      Protocol Length Info
  2375 69.077423146   HP_1a:5f:06      Broadcast        ARP       60 Who has 192.168.0.231? Tell 192.168.0.249
  2376 69.203181604   192.168.0.126    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  2377 69.865007704   HP_1a:5f:06      Broadcast        ARP       60 Who has 192.168.0.100? Tell 192.168.0.249
  2378 70.218891177   192.168.0.126    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  2379 70.577286593   HP_1a:5f:06      Broadcast        ARP       60 Who has 192.168.0.100? Tell 192.168.0.249
  2380 71.234074344   192.168.0.126    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  2381 71.485304138   HP_1a:5f:06      Broadcast        ARP       60 Who has 192.168.0.231? Tell 192.168.0.249
  2382 71.577502283   HP_1a:5f:06      Broadcast        ARP       60 Who has 192.168.0.100? Tell 192.168.0.249
  2383 72.031861689   192.168.0.213    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  2384 72.077401364   HP_1a:5f:06      Broadcast        ARP       60 Who has 192.168.0.231? Tell 192.168.0.249
  2385 72.175858744   192.168.0.215    224.0.0.251      MDNS     103 Standard query 0x001e PTR _AAF8F49E._sub._googlecast

▸ Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface enp3s0, id 0
▸ Ethernet II, Src: HP_1a:5c:72 (04:0e:3c:1a:5c:72), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▸ Internet Protocol Version 4, Src: 192.168.0.164, Dst: 239.255.255.250
▸ User Datagram Protocol, Src Port: 61335, Dst Port: 1900
▸ Simple Service Discovery Protocol

0000  01 00 5e 7f ff fa 04 0e  3c 1a 5c 72 08 00 45 00   ··^····· <·
0010  00 cb 90 96 00 00 01 11  77 45 c0 a8 00 a4 ef ff   ········
0020  ff fa ef 97 07 6c 00 b7  ef b6 4d 2d 53 45 41 52   ·····l·· ··M-
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST:
```

Conclusion :-

In this theory, we explored various port scanning techniques and their applications using Nmap. Each technique serves a specific purpose in network security assessment. It's essential to use these techniques responsibly and with proper authorization, as unauthorized port scanning can be considered malicious behavior. Nmap's versatility makes it a valuable tool for network administrators and security professionals to identify potential vulnerabilities and enhance overall network security.