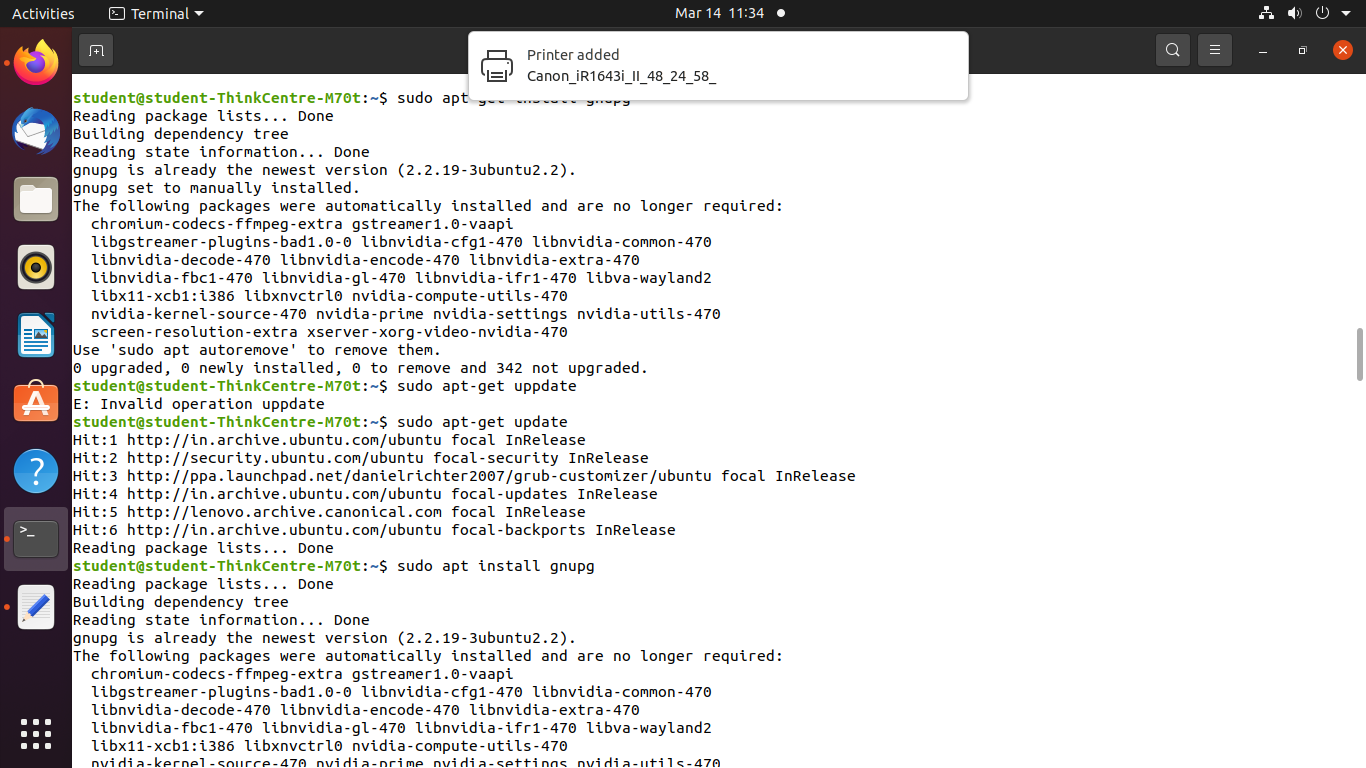
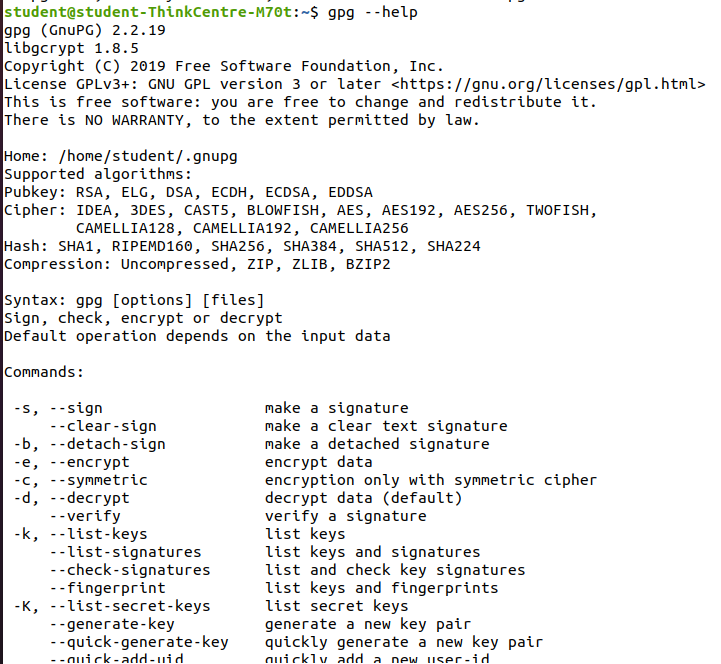
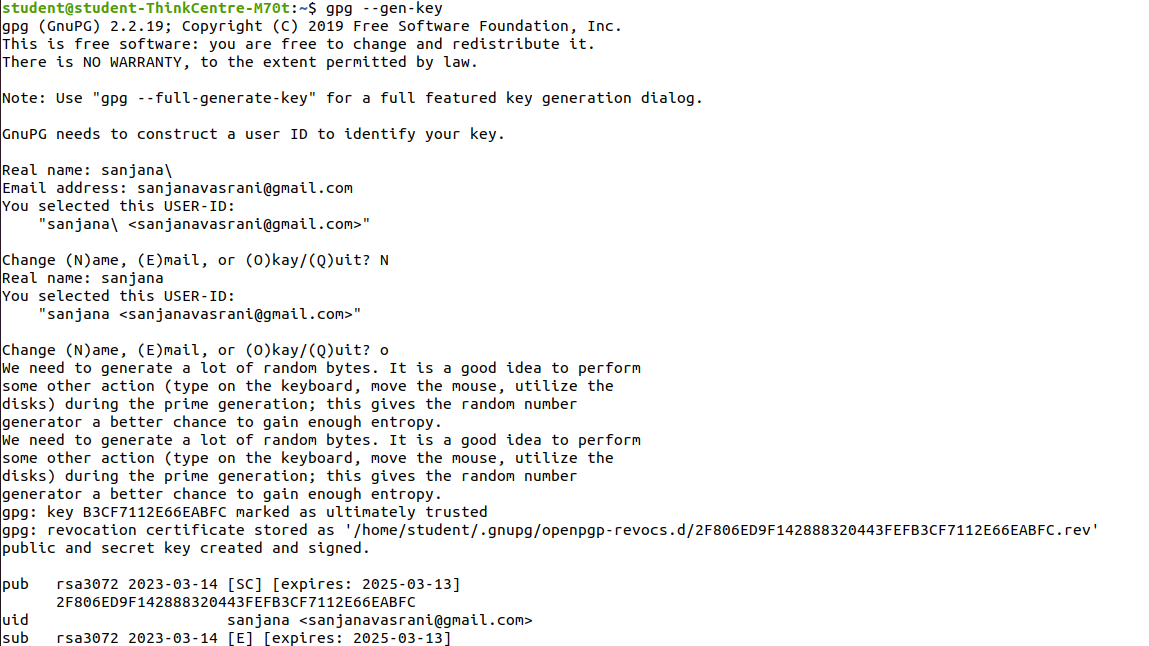
* ***Sudo apt -get install gpg***



* **Gpg –help**

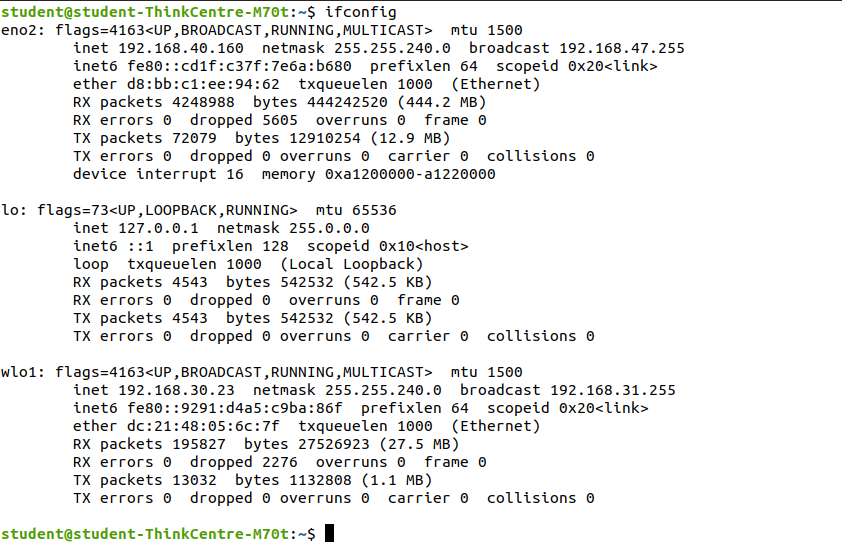
****

* **Gpg –gen-key**

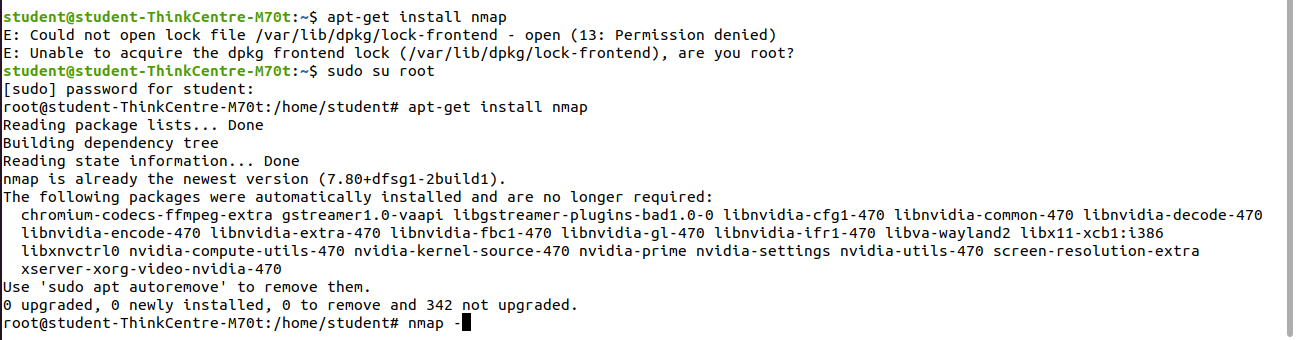
****

***01\_D12B\_SANJANA ASRANIN\_CSS\_NMAP***

* **ifconfig**

****

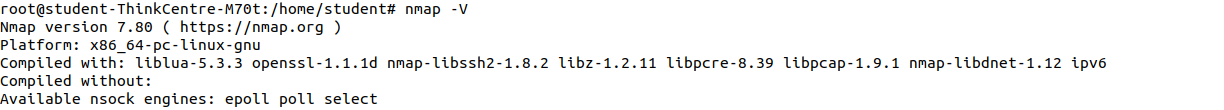
* **Sudo su root** to get root access
* **Apt-get install nmap**



* **nmap -V**

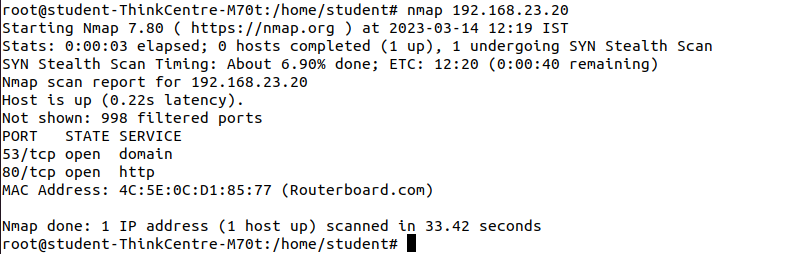
# nmap -V

It gives the version of Nmap



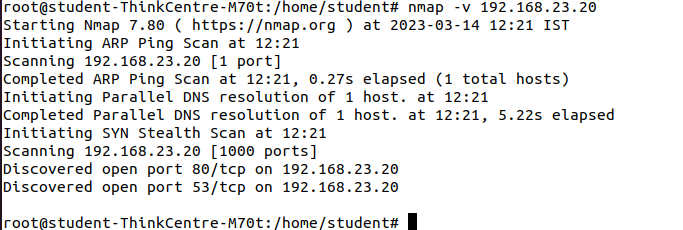
* **Nmap 192.168.23.20**

It gives information about a single host. It gives the output in column form where first column is the PORT, second column is the STATE and third column is the SERVICE



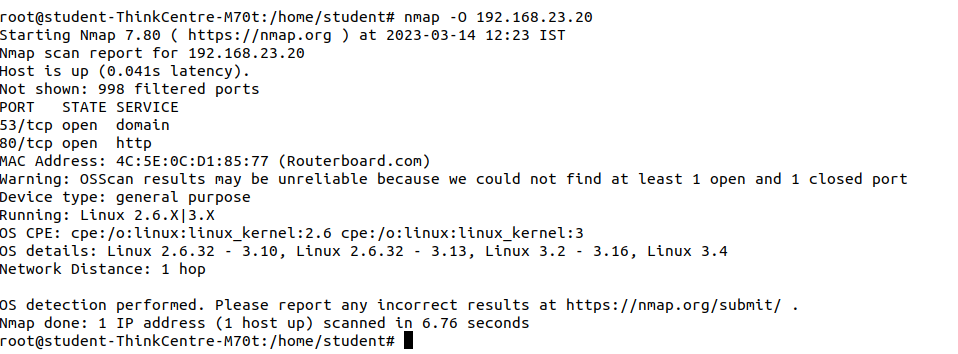
* **Nmap -v 192.168.23.20**

It gives detailed information about remote host.

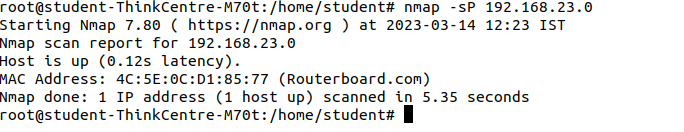


* **Nmap -O 192.168.23.20**

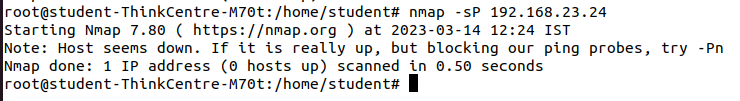
It finds the remote host operating system and version (OS detection)



* **Nmap -sP 192.168.23.20**

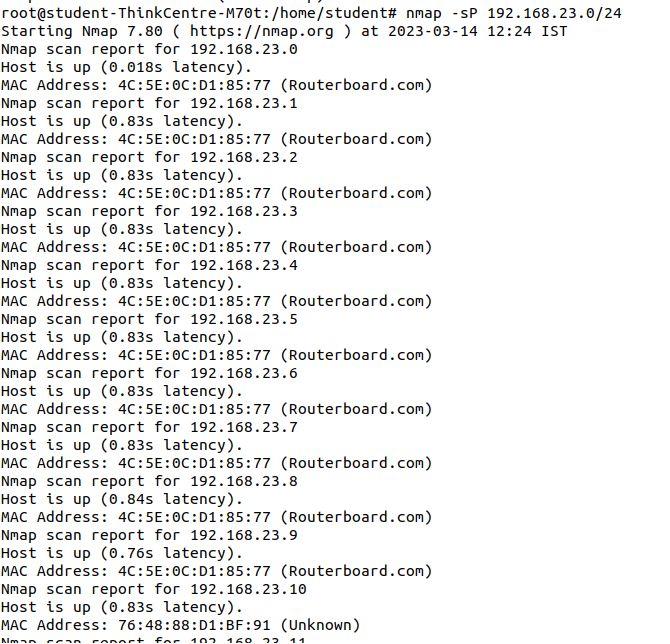


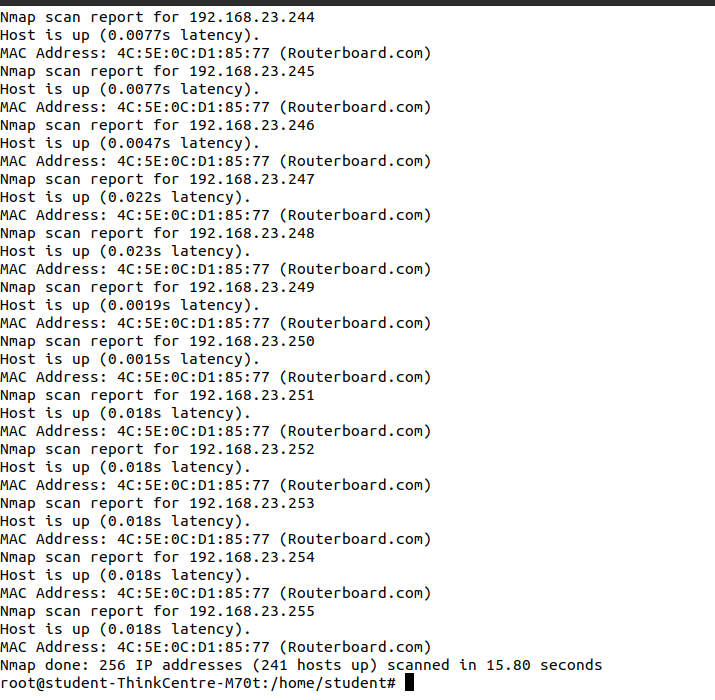
* **Nmap sP 192.168.23.24**

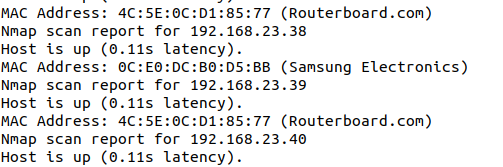


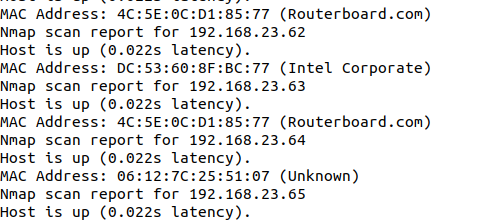
* **Nmap -sP 192.168.23.0/24**

It scans a network and discover which servers and devices are up and running(ping scan)



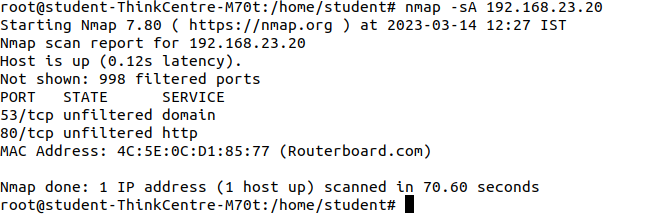






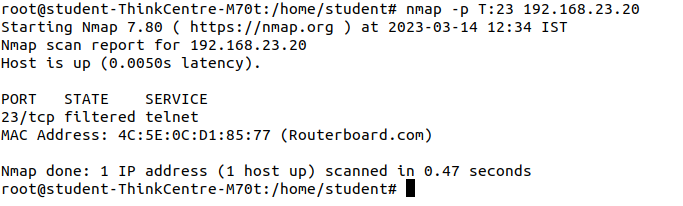
* **Nmap -sA 192.168.23.20**

To discover if a host/network is protected by a firewall. The output has the word FILTERED which shows the presence of a firewall. UNFILTEREDmeans no firewall.



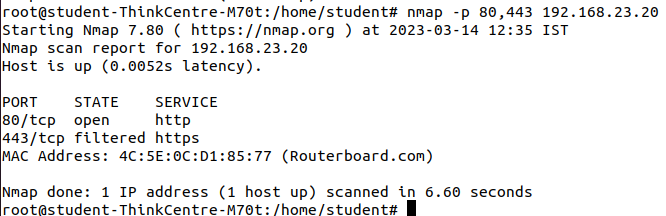
* **Nmap -p T:23 192.168.23.20**

It scans TCP port 23



* **Nmap -p 80,443 192.168.23.20**

It scans multiple ports at one time



* **Nmap -sS 192.168.23.20**

It performs SYN scan or Stealth scan.

Open wireshark.

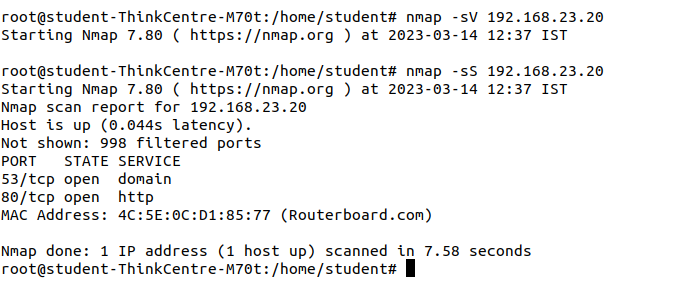
Set the Filter to TCP.

See the gray and red color packets

Double click any gray color TCP packet where destination address is the neighbor’s address

See the Flag field of TCP: SYN bit should be set to 1

See the Flag field of TCP: No flag bits should be set



* **Nmap -sN 192.168.23.20**

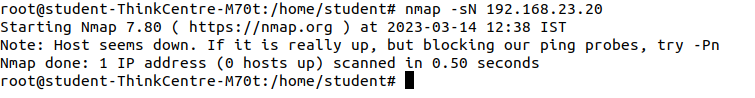
It performs TCP Null Scan. It does not set any bits (TCP flag header is 0)

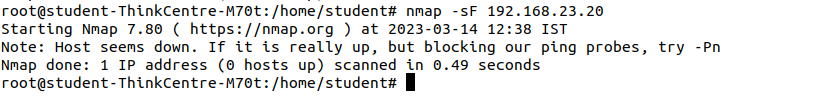
Open wireshark.

Set the Filter to TCP.

Double click any gray color TCP packet where destination address is the neighbor’s

address





* **Nmap -sX 192.168.23.20**

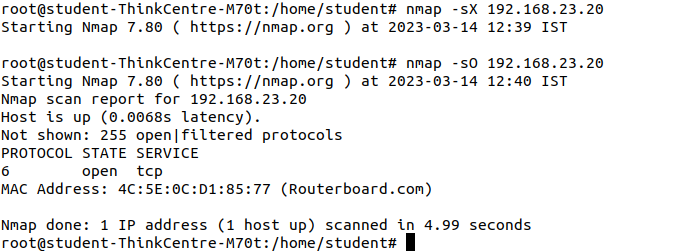
It performs TCP Xmas. It sets the FIN, PSH, and URG flags.

Open wireshark.

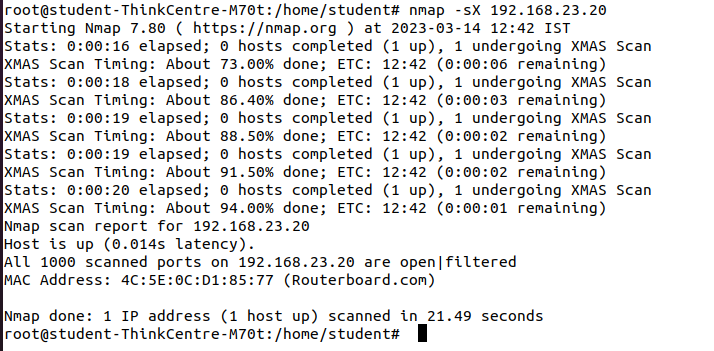
Set the Filter to TCP.

Double click any gray color TCP packet where destination address is the neighbor’s address

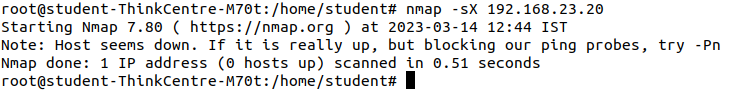
See the Flag field of TCP: FIN, PSH, and URG flags should be set to 1



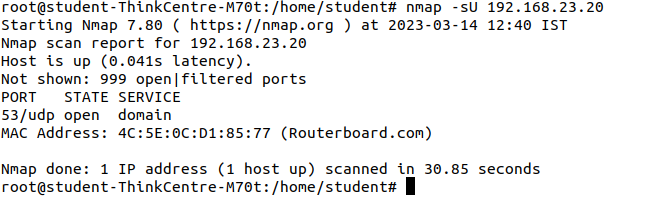
* **Nmap -sX 192.168.23.20**

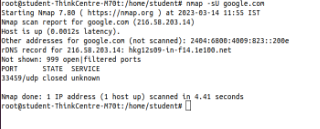


* **Nmap -sX 192.168.23.20**



* **Nmap -sU 192.168.23.20 :** It performs UDP port scan.

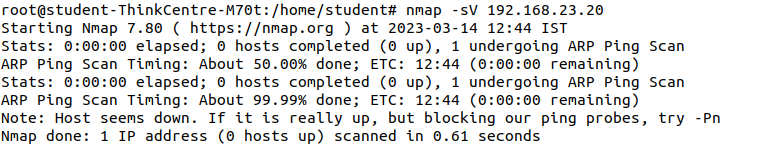






* **Nmap -sV 192.168.23.20**

It detects remote services (server / daemon) version numbers. Version numbers are displayed only if the Port is open



* **Sudo nmap -sF google.com**

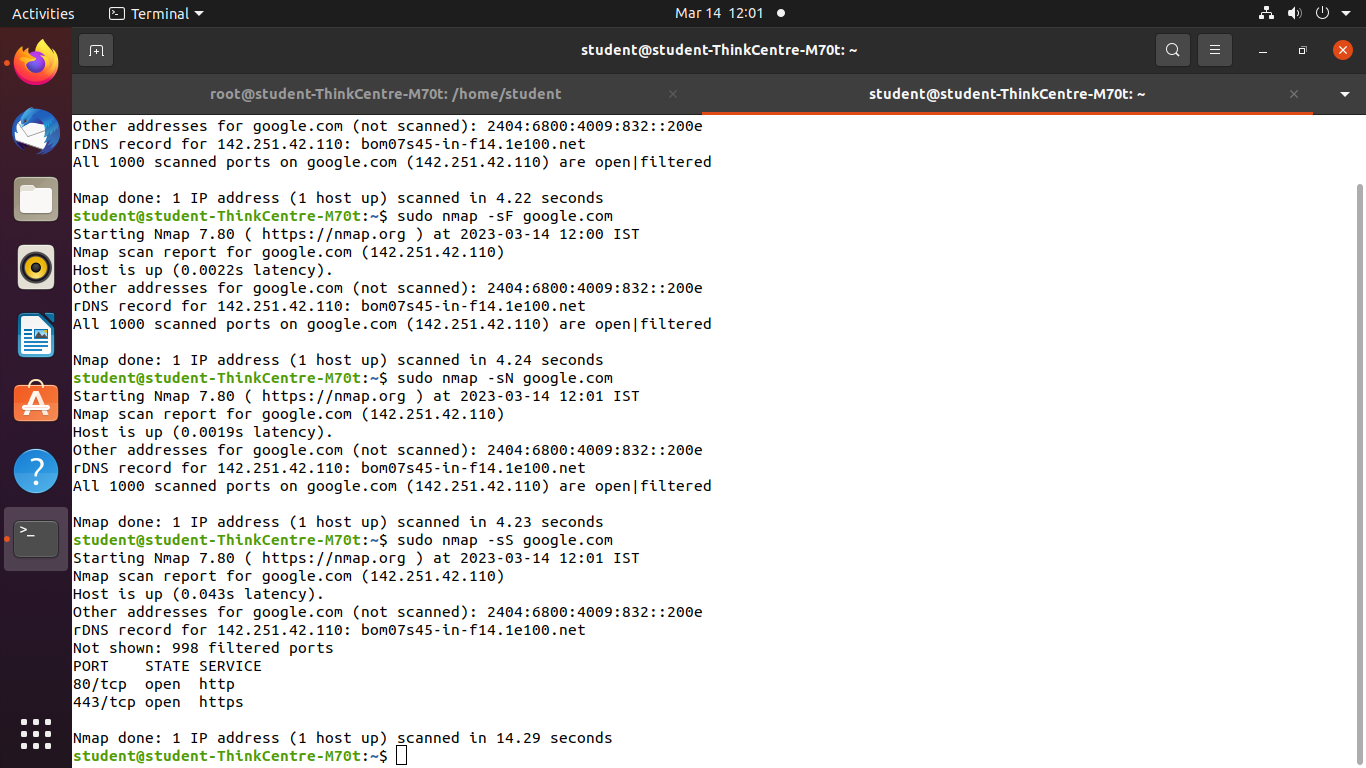
It performs FIN scan. It sets just the TCP FIN bit.

Open wireshark.

Set the Filter to TCP.

Double click any gray color TCP packet where destination address is the neighbor’s address

See the Flag field of TCP: FIN flag should be set to 1



# nmap –sO192.168.23.20: It performs IP protocol scan and allows us to determine which IP protocols) are supported by target machines.