CST4550

man nmap

a. What do the following switches do?

* -sn This switch disables port scanning. Only host are discovered but their ports are not scanned weather they are open or not
* -PO This switch scans both the host which are up and all the ports of each host which are open along with their Port number, state and service
* -PS The switch is used to discover all the SYN packets on a port transferred through TCP protocol. The default port number is 80. It also shows all the host up and the open port list of each host.
* -PU The switch is used to discover all the UDP packets on a port. It also shows all the host up and the open port list of each host.
* -sO This switch scans for all the services and the ports which the host is using. Also, it scans for all the hosts which are up in the network
* -sV This switch scans all the ports which are open as well as the specific version a service is using. It also scans for all the hosts which are up in the network
* -O

4. Specifically enter the following scans:

a. nmap -n –sn {Network}

root@testpc1-VirtualBox:~# nmap -n -sn 102.116.119.196

Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-26 22:16 +04

Nmap scan report for 102.116.119.196

Host is up (0.00077s latency).

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds

ii. Why is the -n option used?

The -n option disables DNS resolution

* iii. What happens if you rerun this command without the -n option? (Try it)

root@testpc1-VirtualBox:~# nmap -sn 102.116.119.196

Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-26 22:17 +04

Nmap scan report for 102.116.119.196

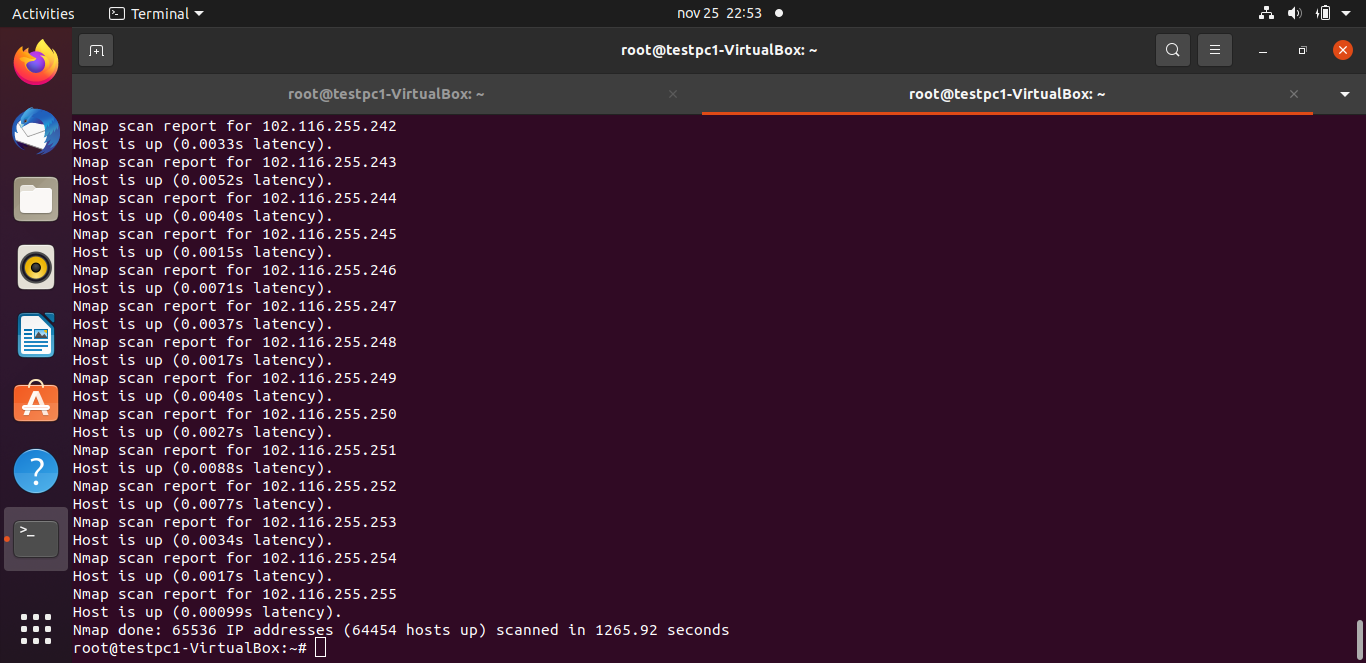
Host is up (0.00078s latency).

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds.

It takes a longer time to scan without the -n option.

b.Use the same nmap command to start a ping scan on the entire /16 network

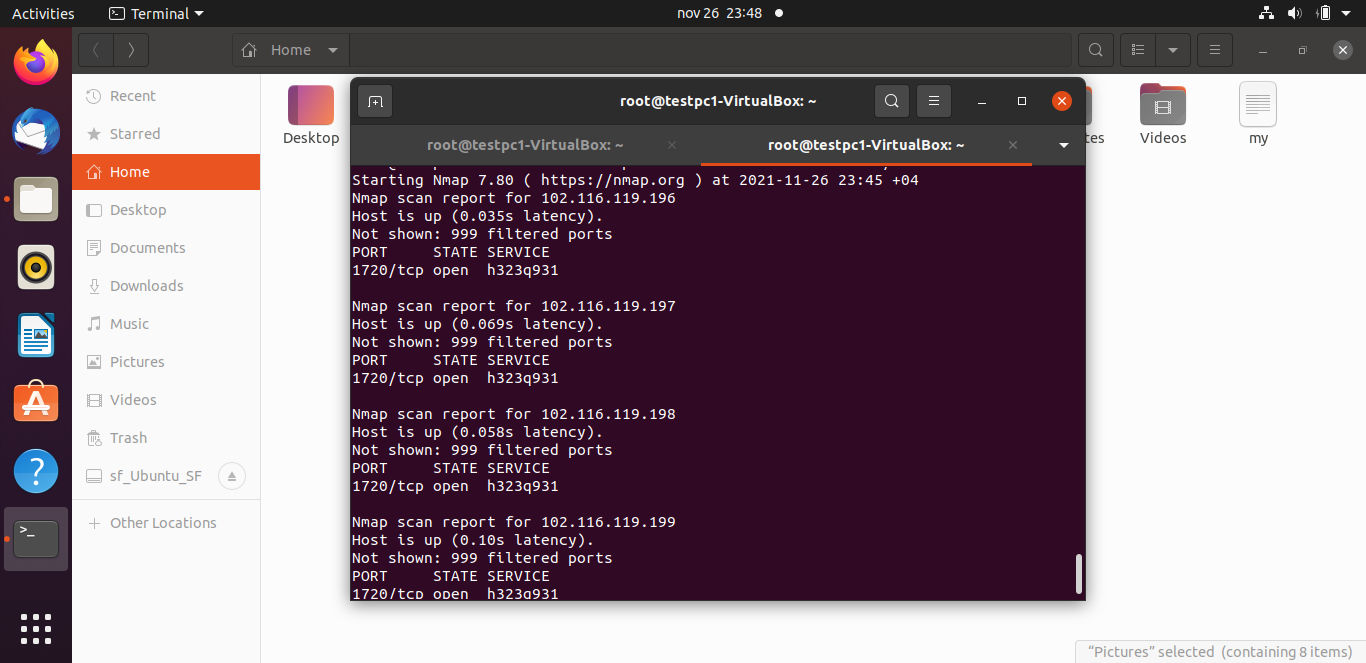
i. How many hosts would this scan look for? Justify your answer



Number of hosts scanned is 65,536. This is because the scan range is from 102.116.0.0 -102.116.255.255.

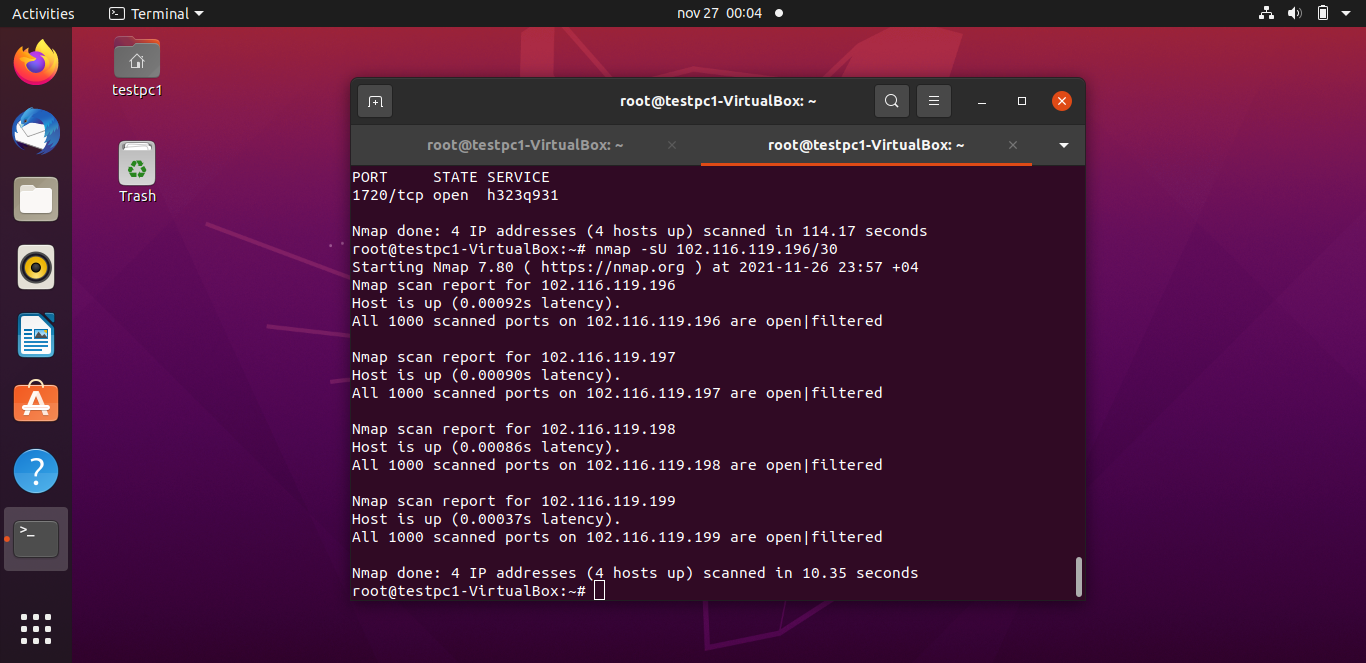
c. Conduct an IP protocol ping (switch -PO / -PS / -PU) on the Common Network hosts. Note that for this scan "nmap needs to read raw responses off the wire"; you must use sudo to have sufficient privilege.

i. How many TCP ports are open on each?

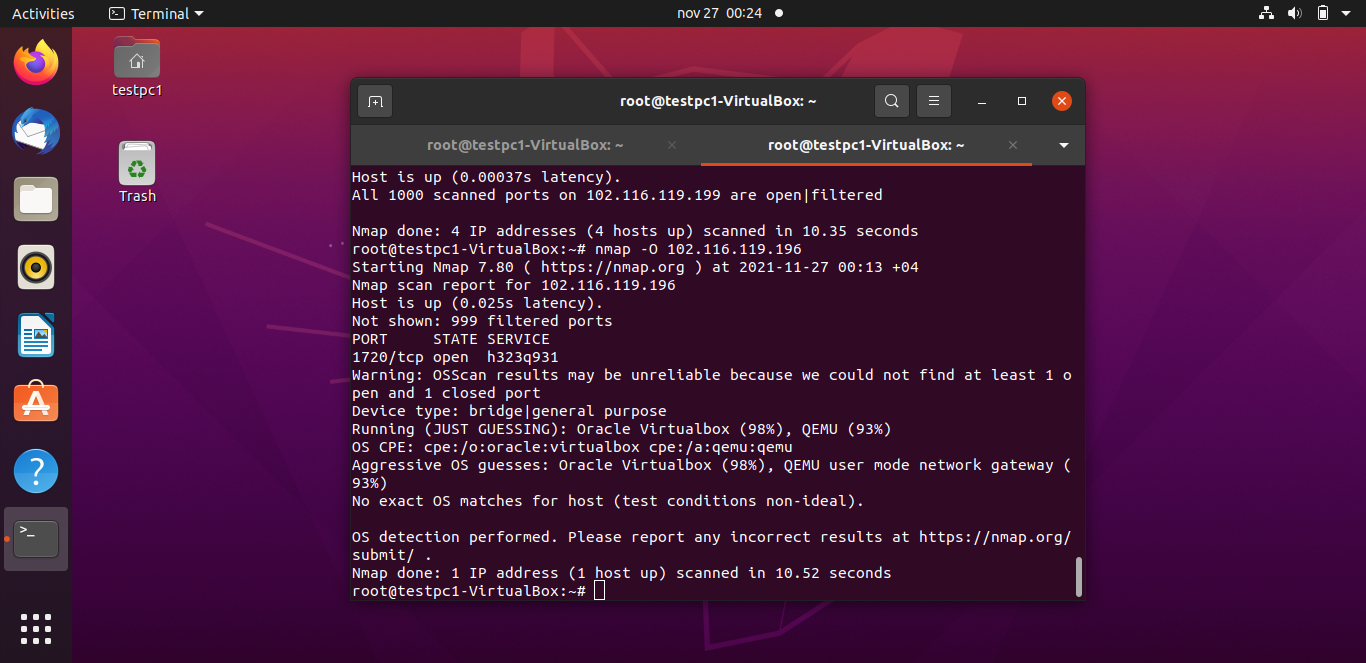


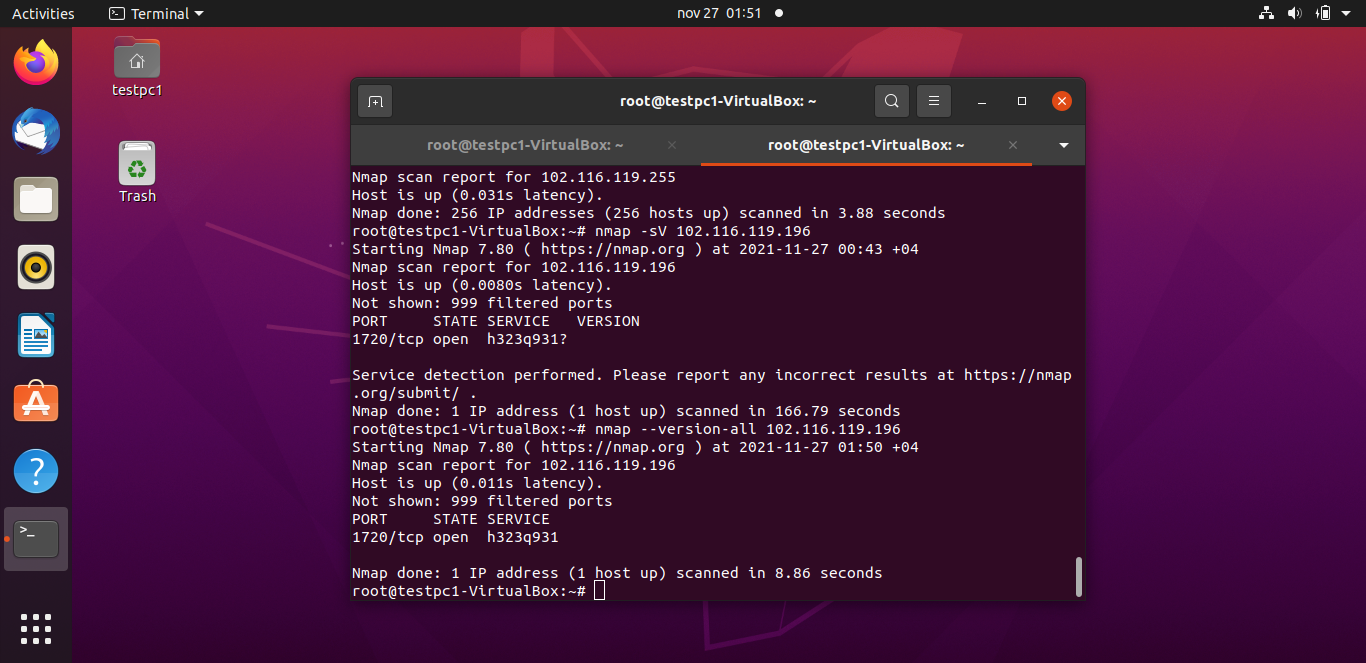
Only 1 tcp port is open on each host

ii. Are there any UDP ports open on any machine?



Nmap was unable to determine if ports were open or filtered





Task3.

1. From the Nmap manual, identify the different types of TCP port Scan

Syn scan, Connect port scan, Ack port scan, Fin scan Null scan

sS/sT/sA/ sN/sF/.

1. From the Namp manual, what is the option to be used for UDP port Scan?

# nmap -sU {ip}