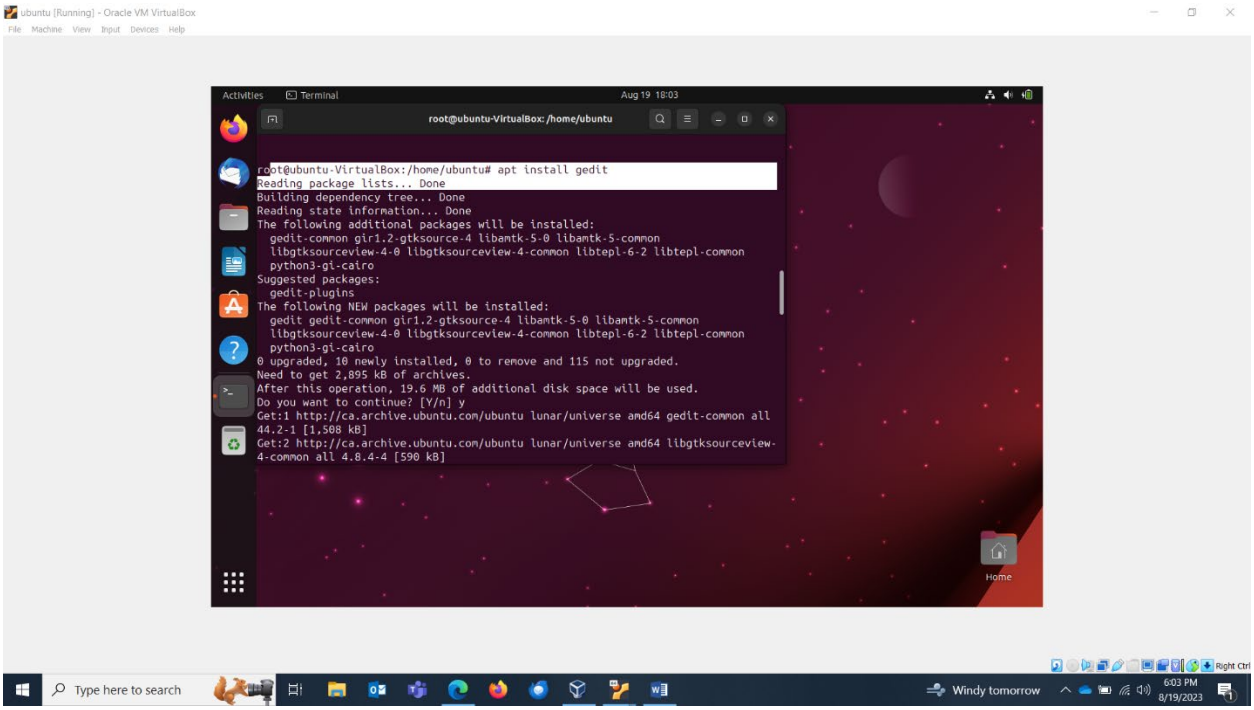
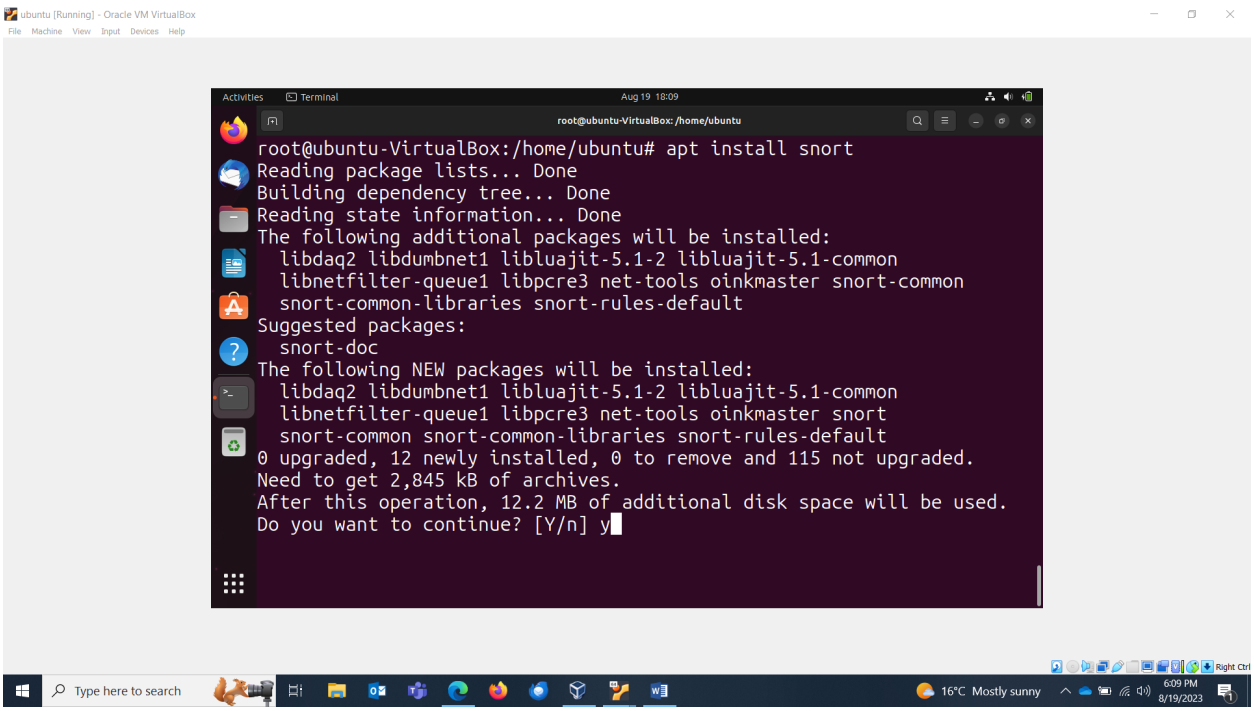
# SNORT IN UBUNTU

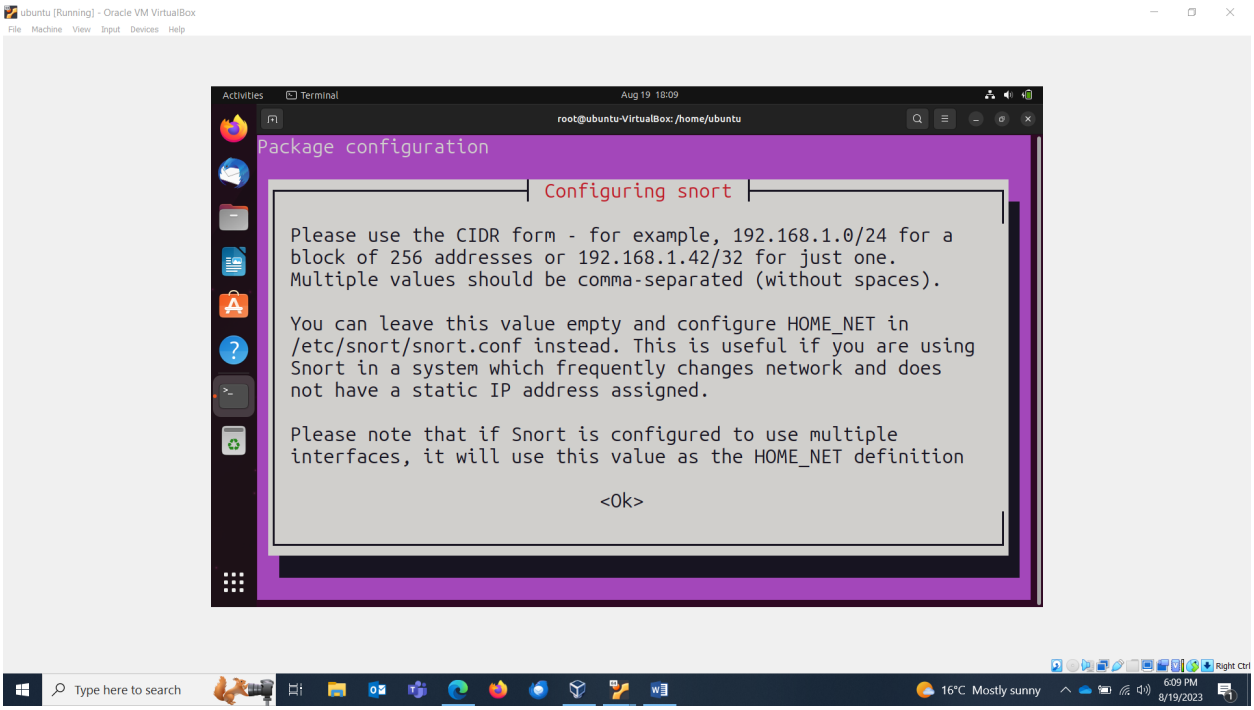
I have installed ubuntu will full installation feature.

The adapter is enp0s3 & IP address is 192.168.1.78

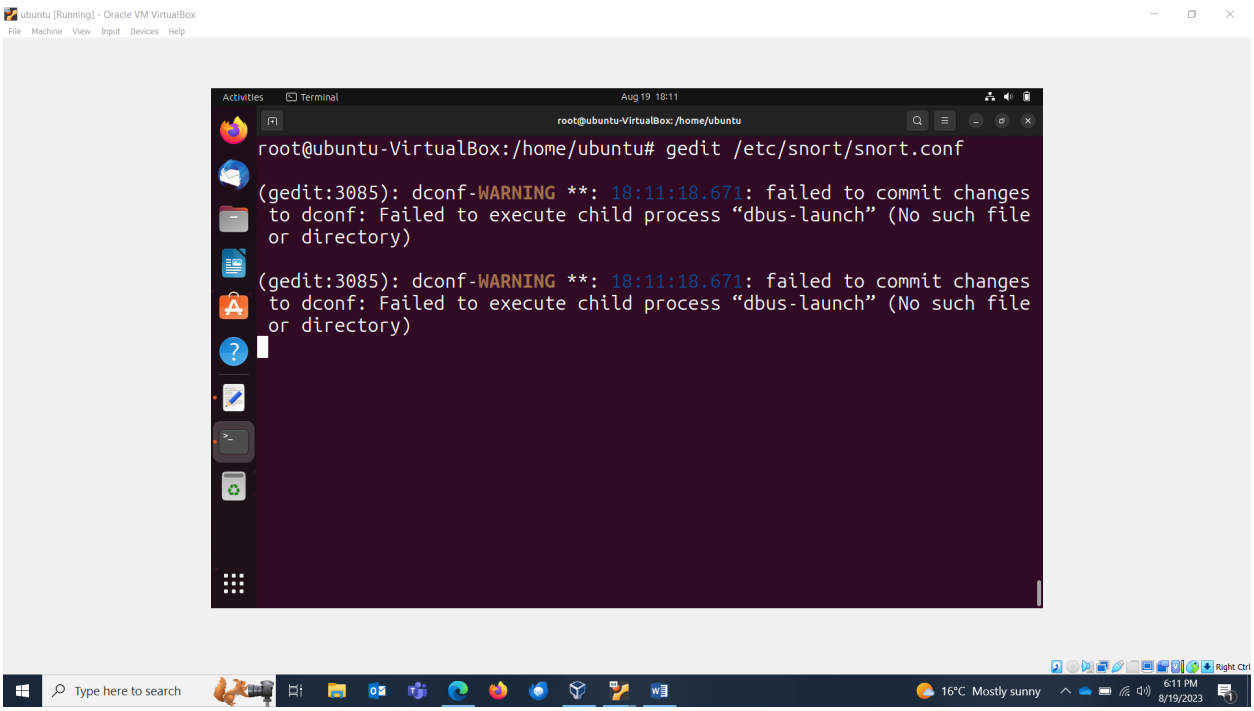


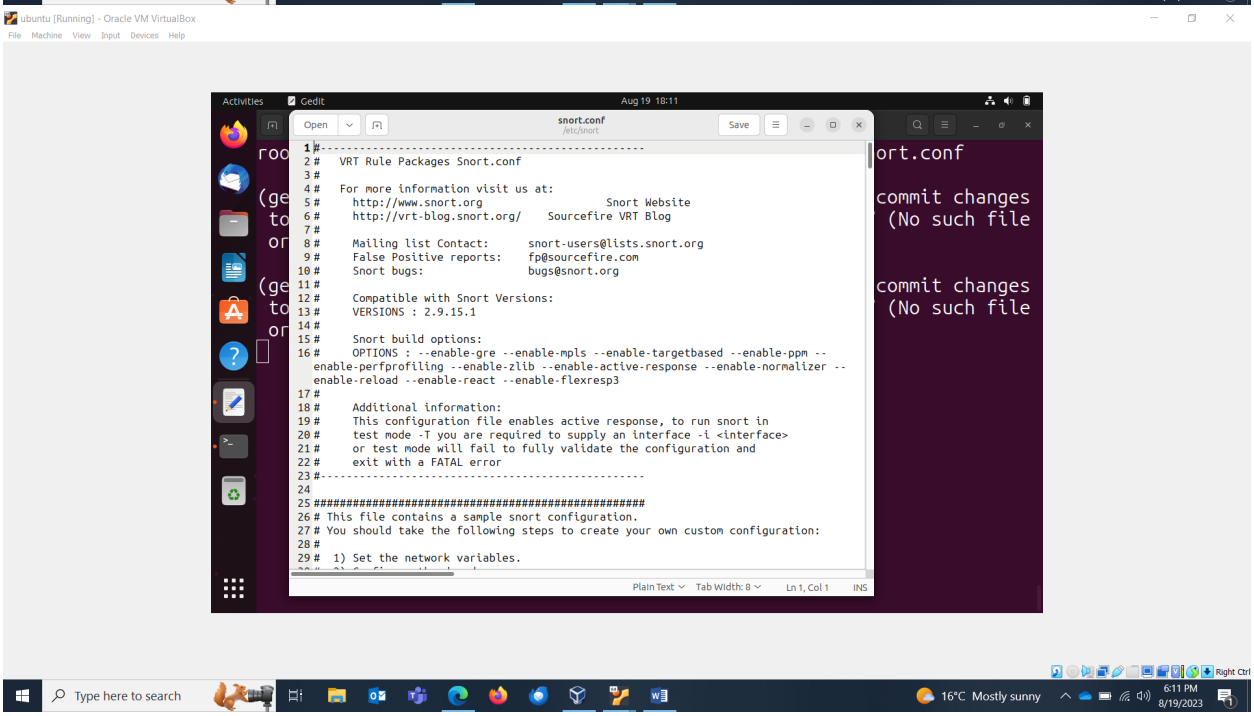

INSTALLING SNORT:



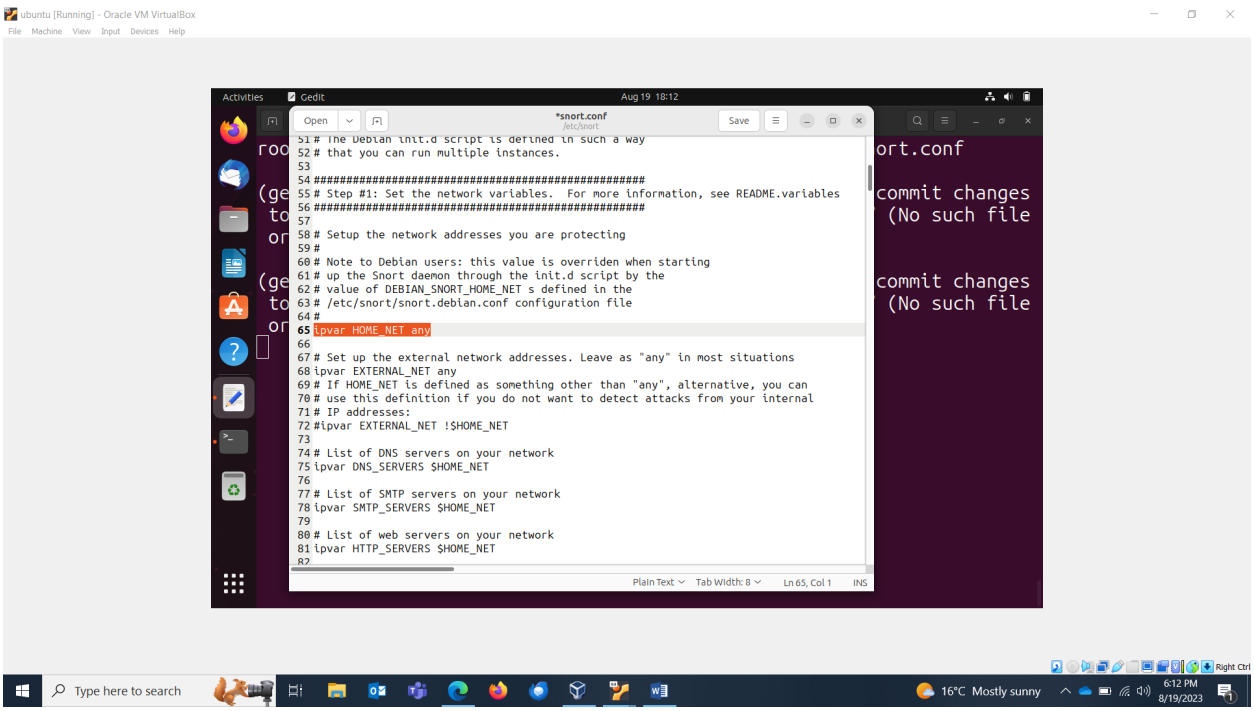




Lets go to the configuration file in snort

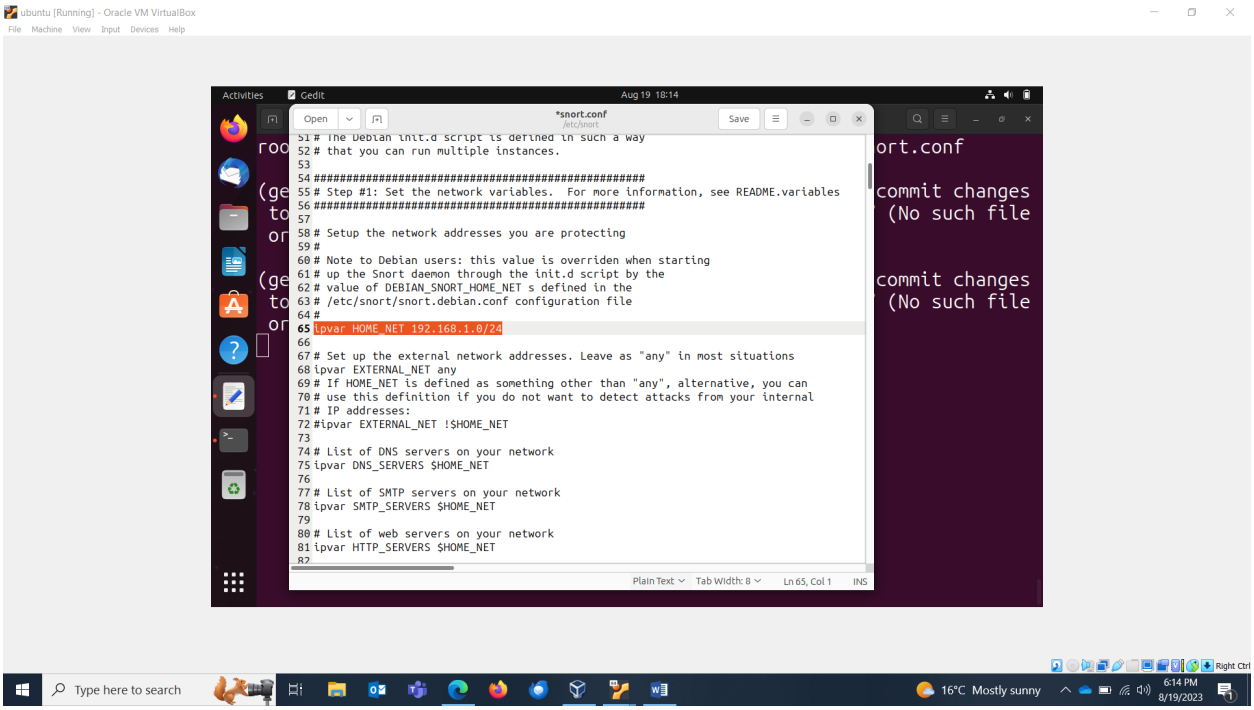


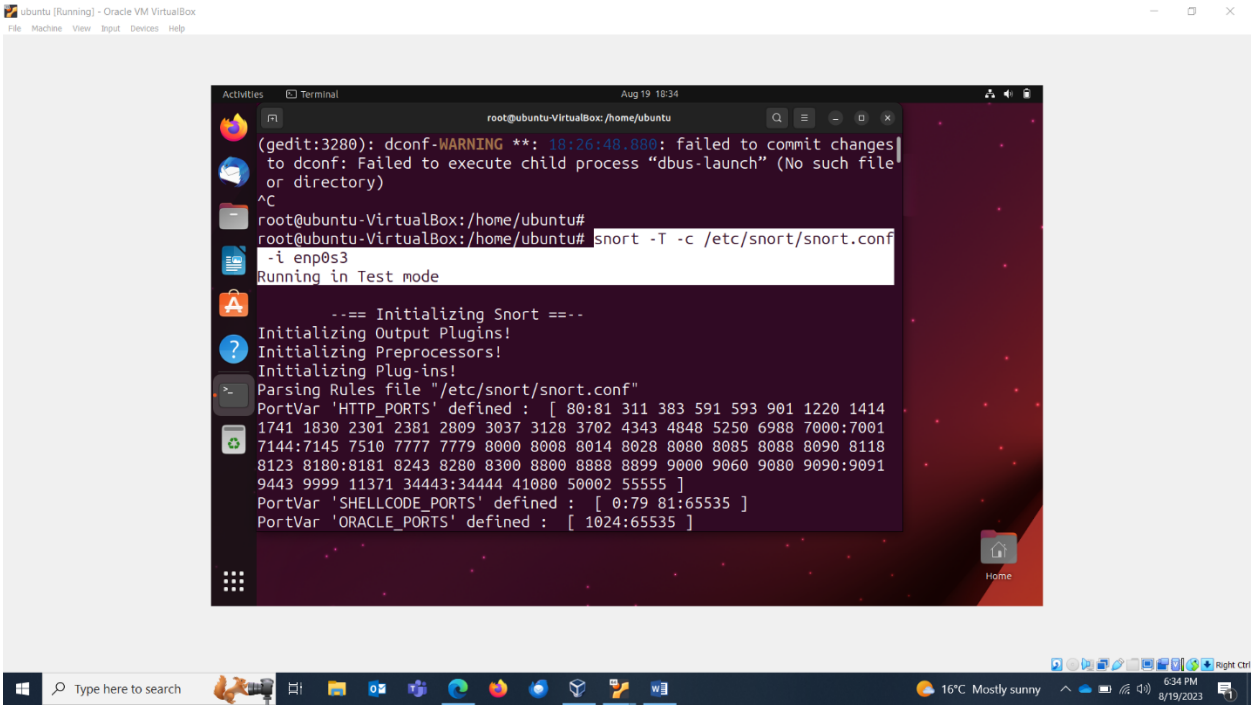

Lets check the CIDR for home net.

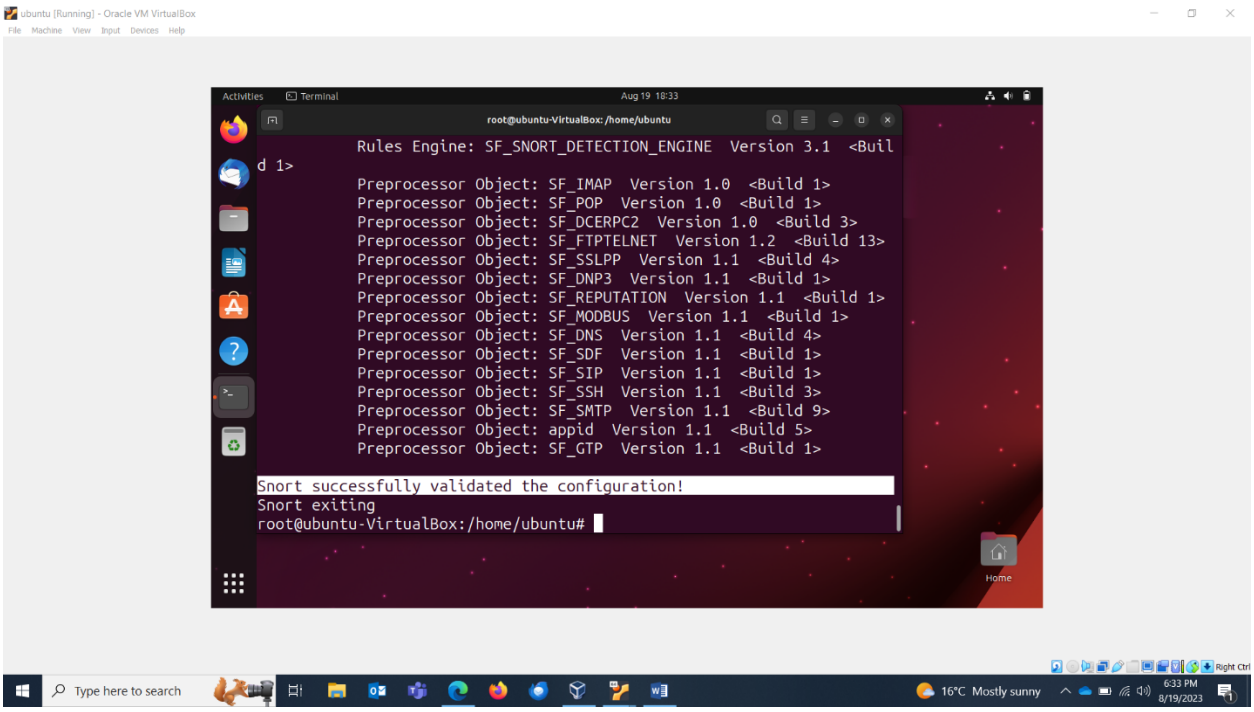



We'll now change it to 192.168.1.0/24



Rules verification exposure:




Lets start monitoring:

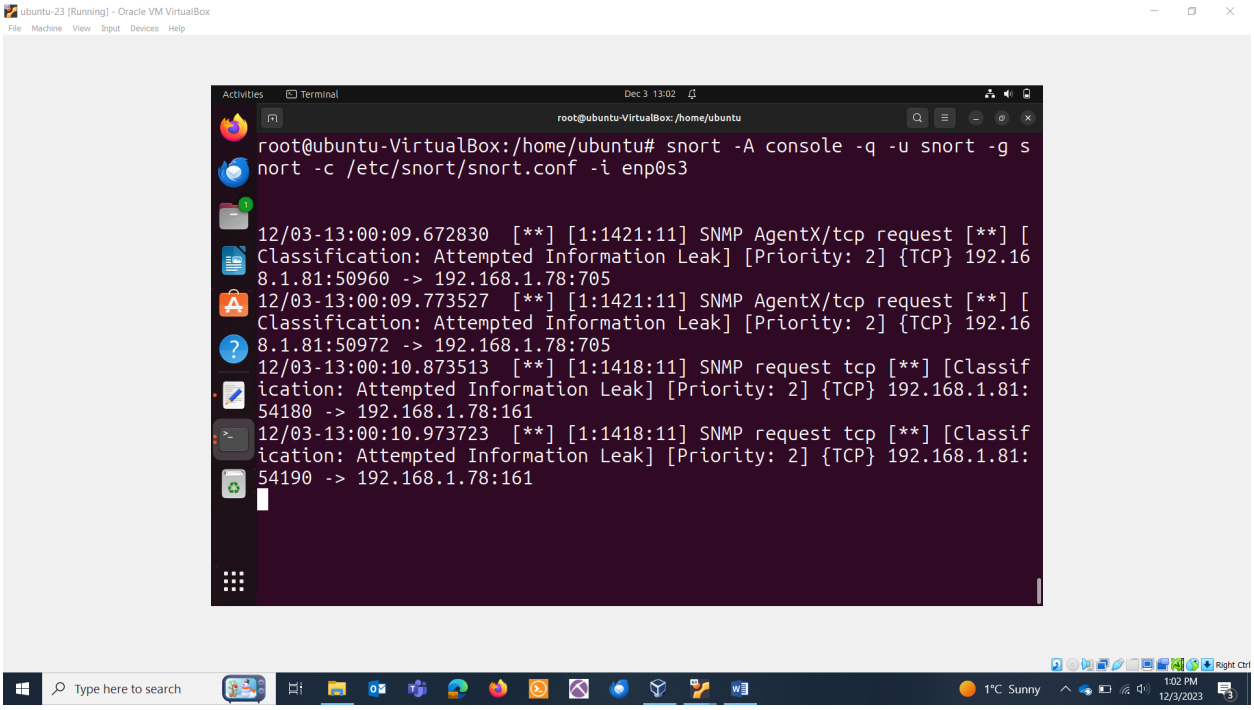
Fire up your kali/parrot machine & run nmap on the ubuntu machine.

My ip address of ubuntu is : 192.168.1.78 and parrot is 192.168.1.81

ATTACK 1: nmap scan:

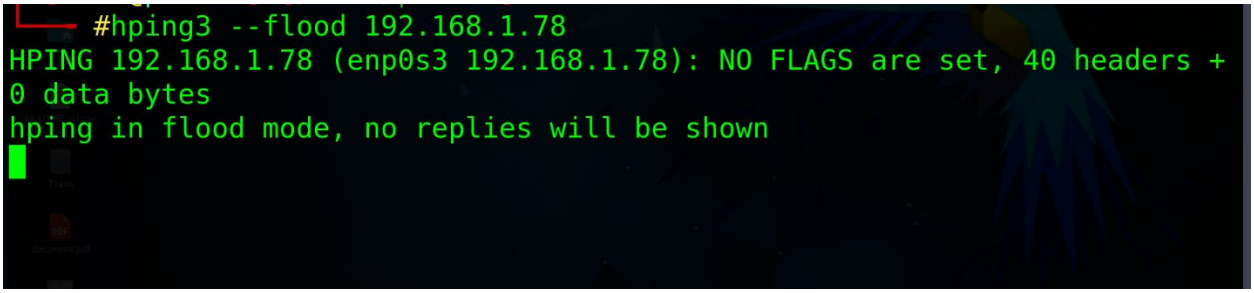
```
┌──[parrot@parrot]─[~]
└──╼ $nmap 192.168.1.78 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-03 15:00 EST
Nmap scan report for 192.168.1.78
Host is up (0.0017s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  closed ftp
22/tcp  open   ssh
445/tcp closed microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
```

Here is the trigger of Information leak which was attacked from 192.168.1.81:



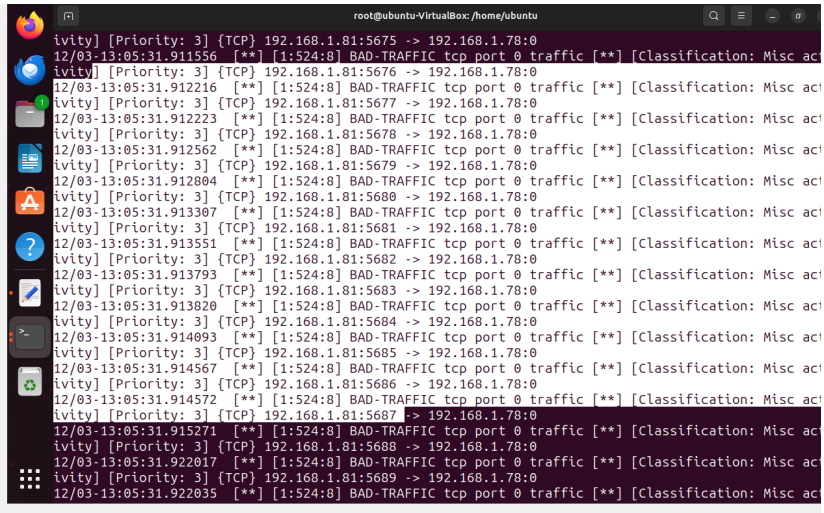
ATTACK 2: DOS through hping3

Lets perform a dos attack from kali linux



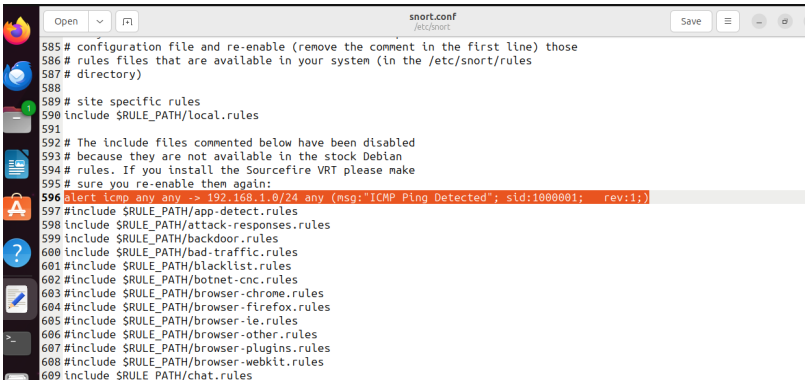

DIY: Analyze with wireshark.

Alerts in Snort console:

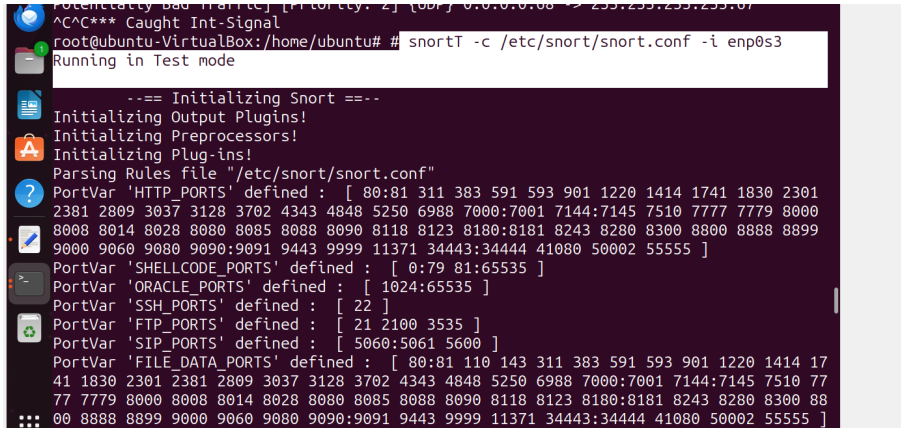


ATTACK 3: Rule for ping

Creating a rule:

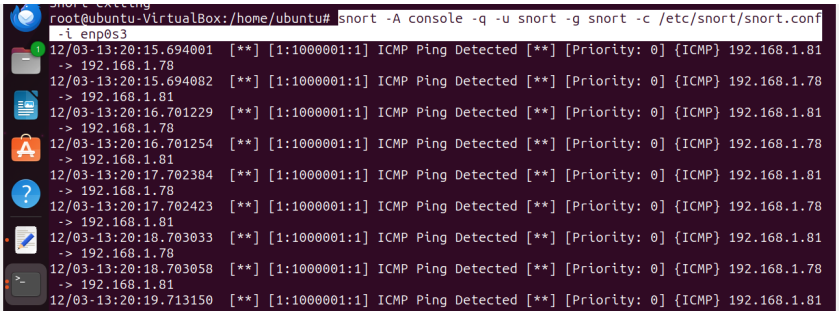



Verify the configurations



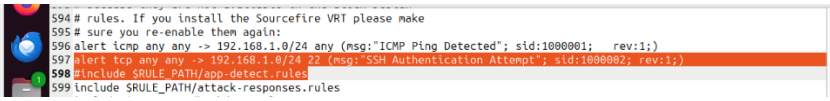

Ping from the other machine

Fire up snort console

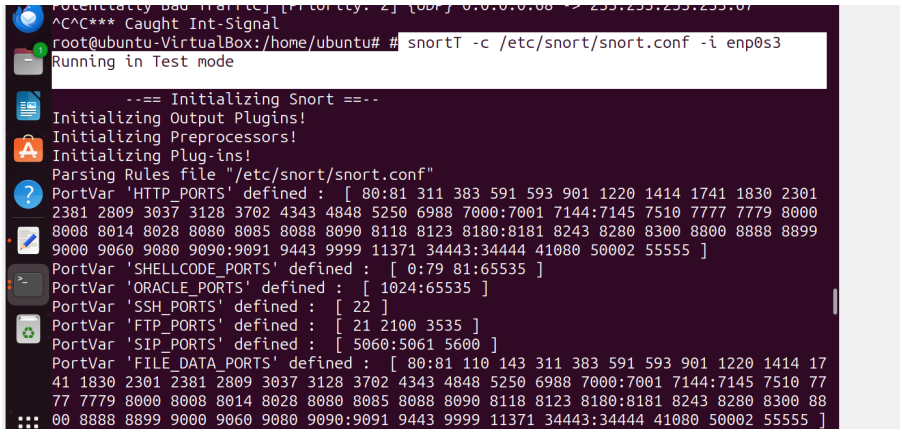


ATTACK 4: ssh

SSH rule

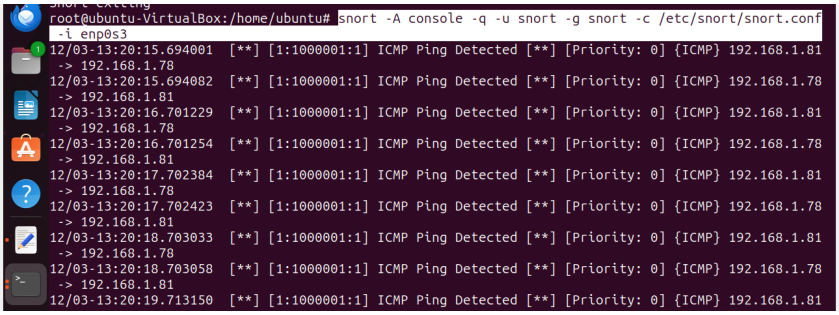


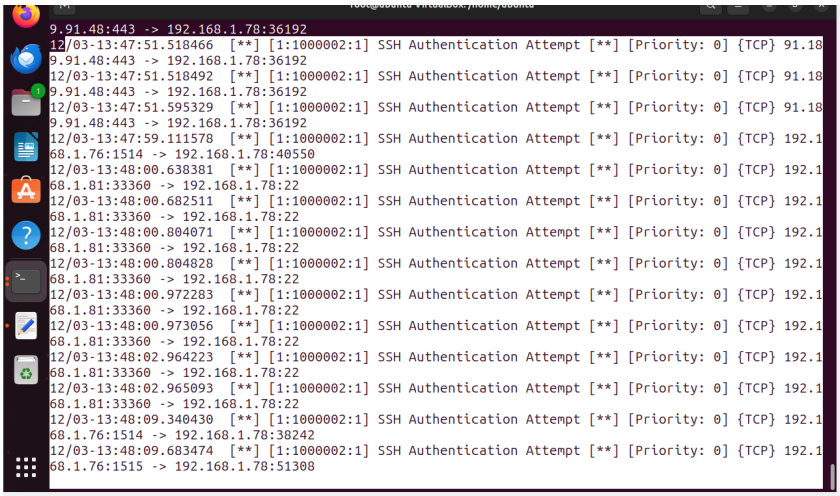

Verify conf.




Try ssh

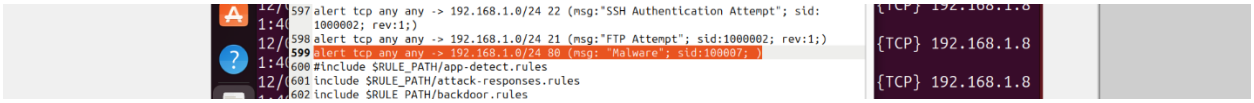

Look in console




9.91.48:443 -> 192.168.1.78:36192
12/03-13:47:51.518466 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 91.18
9.91.48:443 -> 192.168.1.78:36192
12/03-13:47:51.518492 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 91.18
9.91.48:443 -> 192.168.1.78:36192
12/03-13:47:51.595329 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 91.18
9.91.48:443 -> 192.168.1.78:36192
12/03-13:47:59.111578 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.76:1514 -> 192.168.1.78:40550
12/03-13:48:00.638381 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03-13:48:00.682511 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03-13:48:00.804071 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03-13:48:00.804828 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03-13:48:00.972283 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03-13:48:00.973056 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03-13:48:02.964223 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03-13:48:02.965093 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03-13:48:09.340430 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.76:1514 -> 192.168.1.78:38242
12/03-13:48:09.683474 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.76:1515 -> 192.168.1.78:51308

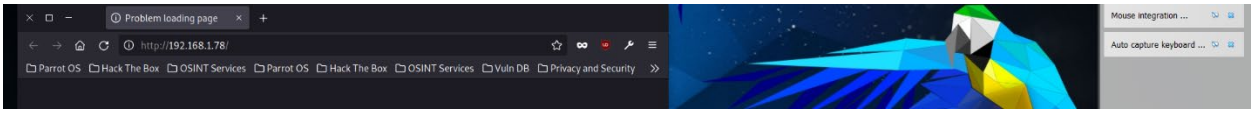
ANALYZE WEB SERVER

Adding rule:




Refresh your configurations: DIY

Access 192.168.1.78's webserver.




Capturing in console