* Install Snort

Text

Description automatically generated

* After installing verify snort

Text

Description automatically generated

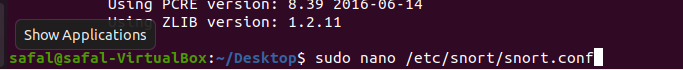
* Create required files and directory if needed

# mkdir /etc/snort

# mkdir /etc/snort/rules

# mkdir /var/log/snort

* Create snort conf rule



Text

Description automatically generated

* Create icmp rule



Text

Description automatically generated

* Execute snort, AS we have not used eth0 port and ensp03



* Start attack from kali linux

A screenshot of a computer

Description automatically generated

* Configure in wireshark if the packets are sent

Graphical user interface, table

Description automatically generated

* Verify the IDS

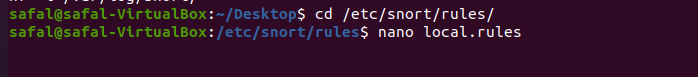
Text

Description automatically generated with medium confidence

We can see that detection can be seen.

**For SynAttack**

In your defending machine i.e, Ubuntu



Text

Description automatically generated

* To validate the configuration

A screenshot of a computer

Description automatically generated with medium confidence

Add your IP address

Then

Text

Description automatically generated

Now in attacking machine

Text

Description automatically generated

Monitoring in Defending machine

A picture containing text

Description automatically generated

In this class I had learned about SNORT and how it is used in the real life. The key learnings were to monitor the traffic in Wireshark. There was two virtual machines and we attacked one virtual machine using SNORT and we monitored the traffic using Wireshark. Both of the machines were on a same router so, it was not that easy. The main challenge was to configure the snort and preview how it worked as we had never used SNORT before. We did sync flood attack that time. So, the challenge was to find out if there was any attack happening on the defending machine and to check it as it was a bit hard to setup this thing and get the hold of this scenarios.