**Intrusion detection using Snort**

· **Detecting nmap scans using snort:**

Configuring details:

sudo apt-get install lamp-server^

sudo apt-get install openssh-server

sudo apt-get install php-pear

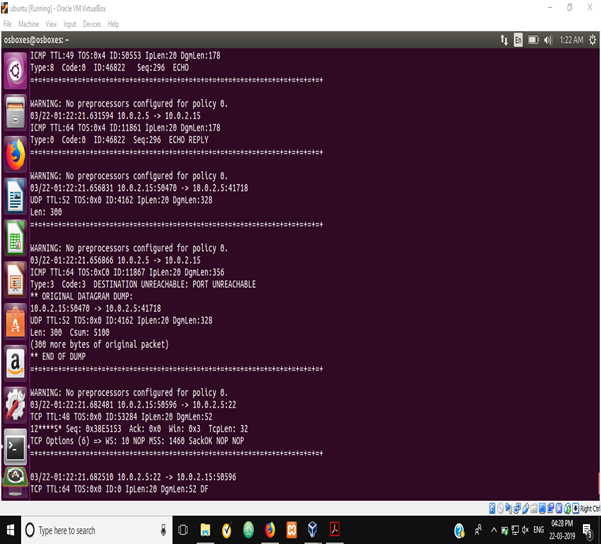
sudo apt-get install snort

sudo dpkg-reconfigure snort (To set the interface type)

sudo snort –v (Starting snort)

We demonstrated this task by using VMs. One as the attacker and one the victim.

When attacker ran nmap command by targeting the victims ip following things were observed:



· **Writing rules to detect DOS attacks:**

In the rules file of snort following rules was added:

**alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)**

The above rule checks if an incoming packet is of type ICMP and outputs the given message.

