**CNS Exp 8**

**Shashwat Tripathi  
D15A 64**

**Batch C**

**AIM:** Study of Network security : Set up Snort and study the logs

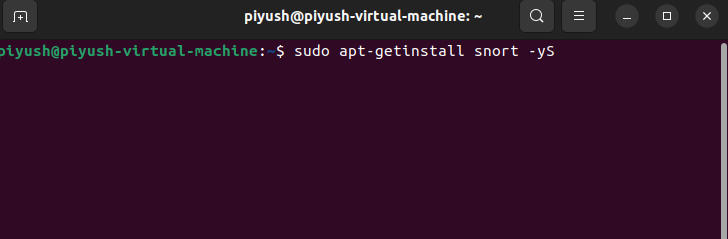
**Theory:**

Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

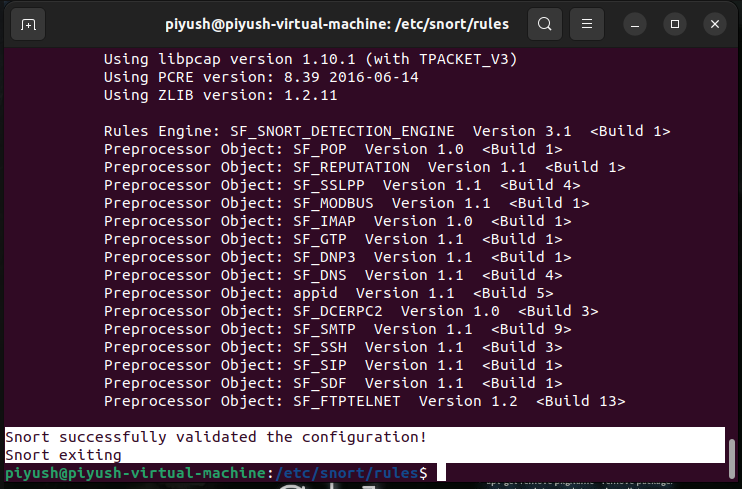
Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

Snort itself uses something called Data Acquisition library (DAQ) to make abstract calls to packet capture libraries. Download the latest DAQ source package from the Snort website with the wget command underneath. Replace the version number in the command if a newer source available.

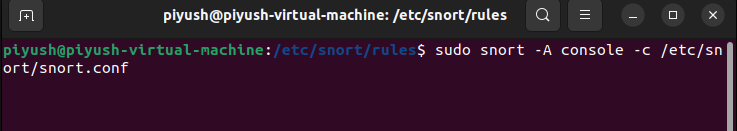
Installing snort on the victim machine



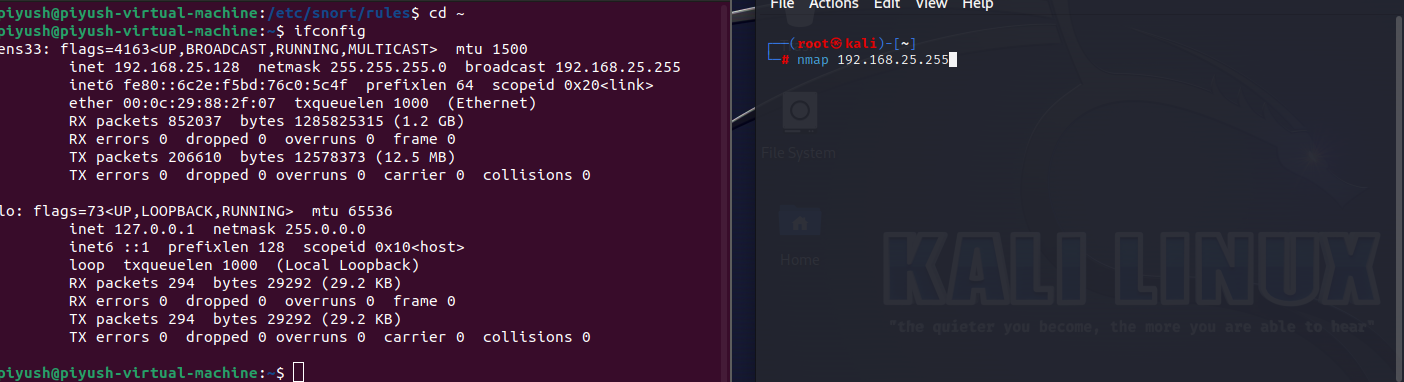
Checking snort configuration



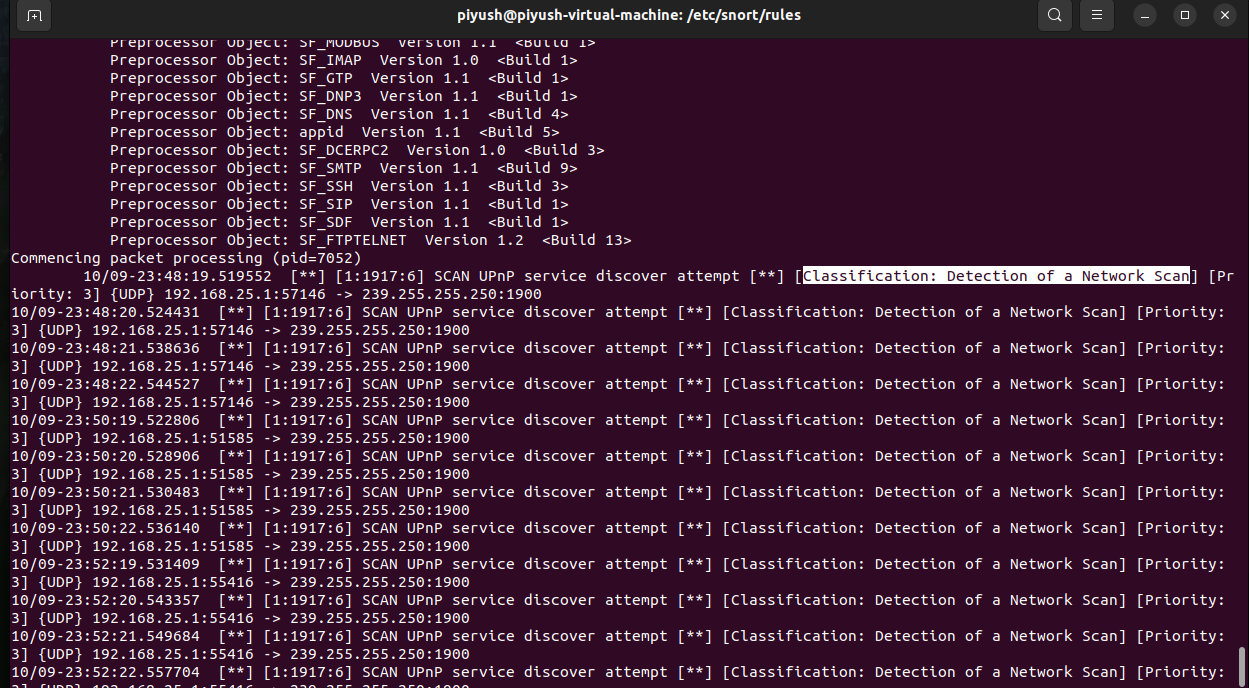
Initialising snort



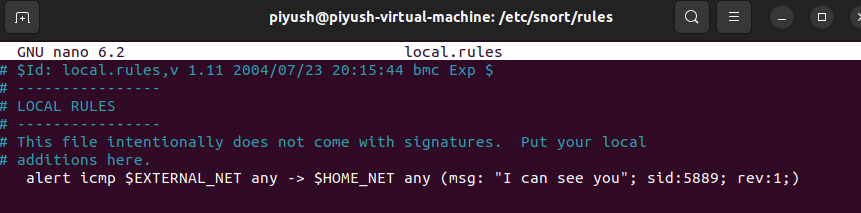
Trying to connect to victim machine that has snort initialized, with kali machine



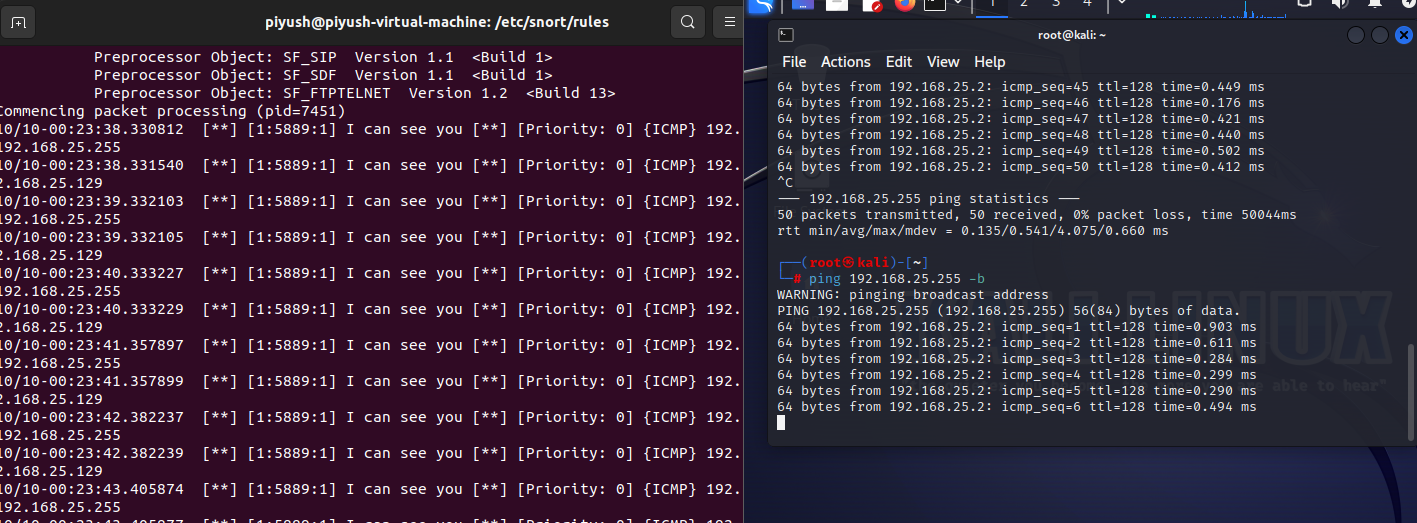
Connection request is logged in the terminal



Adding custom rules to local.rules file



Testing for the logs of custom message



Conclusion: Therefore, we have set up Snort and studied the logs and understood how we can attempts of attacks on our system with the help of snort