**Project Name :- Network Firewall**

**We are implementing this network firewall by using SNORT (open source application)**

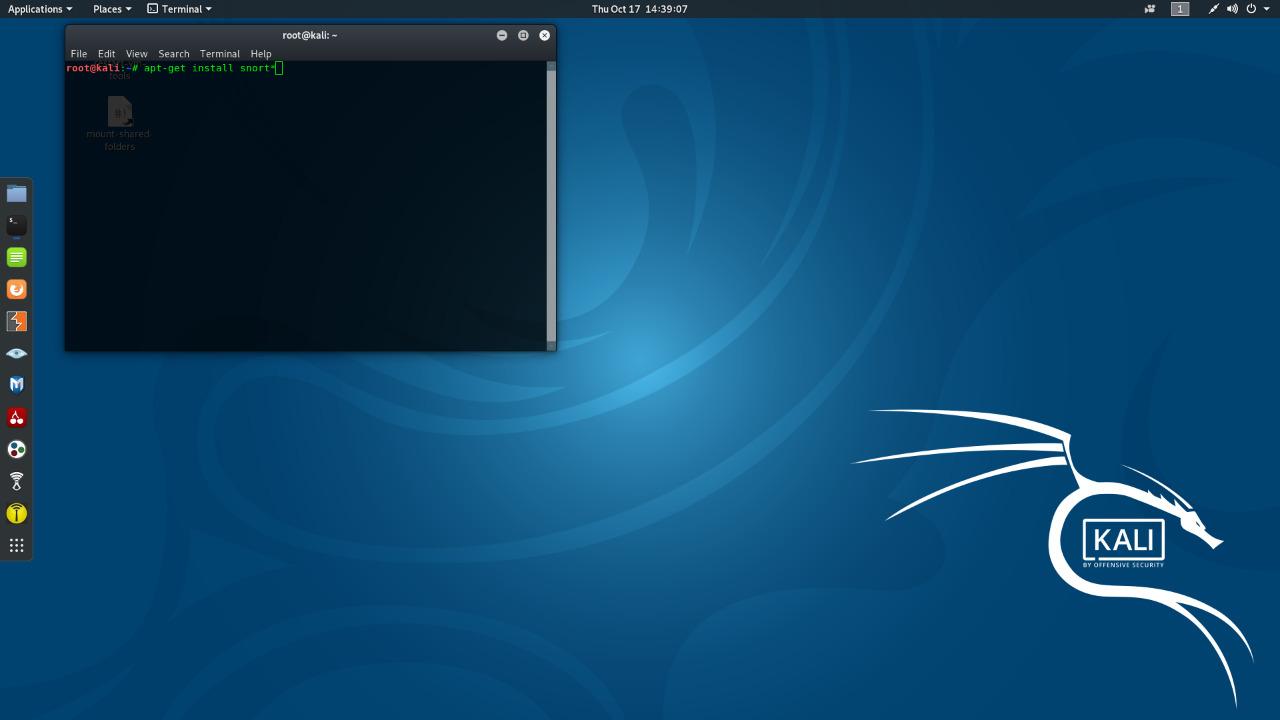
**Introduction to snort**

Snort is a Network Intrusion Detection System (NIDS). It’s quite popular and is open source software which helps in monitor network traffic in real-time, hence it can also be considered as a packet sniffer. Basically, it examines each and every data packet in depth to see if there are any malicious payloads. it can also be used for protocol analysis and content searching. It is capable of detecting various attacks like port scans, buffer overflow, etc. It’s available for all platforms i.e. Windows, Linux, etc. It doesn’t require any recompilation with the system or hardware to added to your distribution; root privileges are required though. It inspects all the network traffic against the provided set of rules and then alerts the administration about any suspicious activity. it’s divided into multiple components and all the components work together to detect an intrusion. Following are the major components of snort :

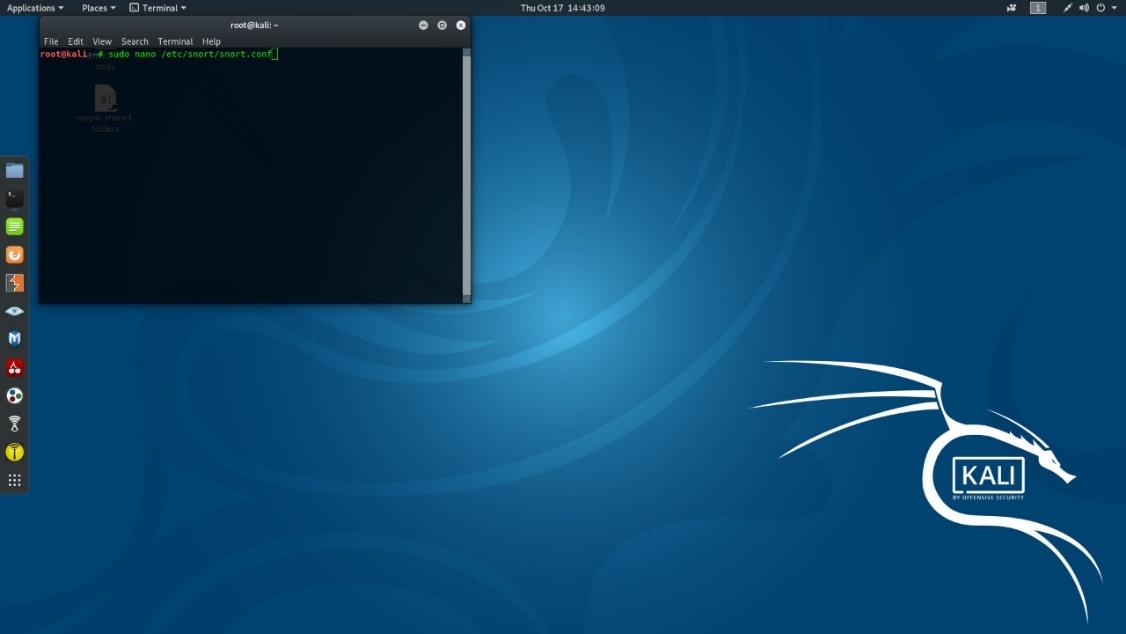
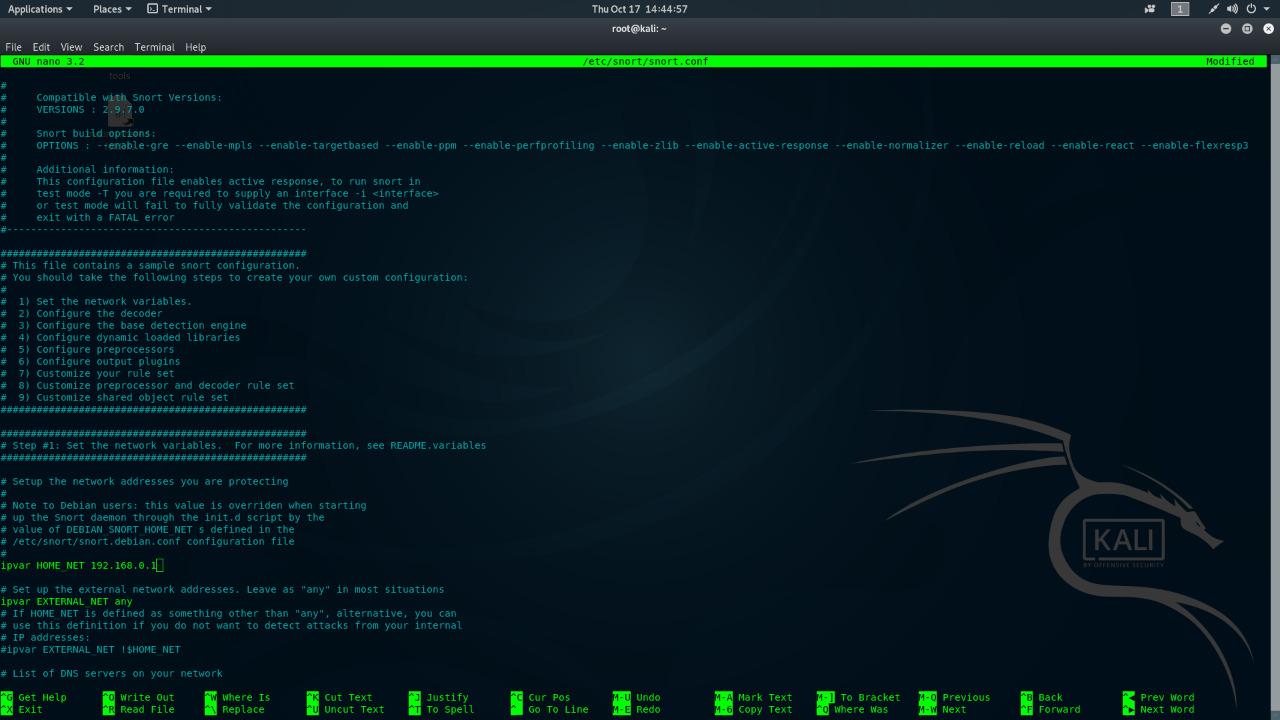
* Packet Decoder
* Pre-processors
* Detection Engine
* Logging and Alerting System
* Output Modules

**Following steps are shown to configure snort :-**

* First, use the ifconfig command in your Ubuntu to check the interface. As you can see the image below the interface is eth0.
* Now we will install SNORT :-



As the snort is installed, open the configuration file using nano or any text editor to make some changes inside. Use the following command to do so :

* sudo nano /etc/snort/snort.conf
* ipvar HOME\_NET 192.168.1.21
* sudo snort -A console -i eth0 -c /etc/snort/snort.conf