MINI PROJECT REPORT

**On**

**Network Firewall**

**Submitted by**

**Govind Sharma**

**Roll No:171500115**

**Ayush Kumar Singh**

**Roll no:171500074**

Department of Computer Engineering & Applications

**Institute of Engineering & Technology**



**GLA University**

**Mathura- 281406, INDIA**

**2019**

**Department of computer Engineering and Applications**

**GLA University, Mathura**

**17 km. Stone NH#2, Mathura-Delhi Road, P.O. – Chaumuha,**

**Mathura – 281406**



**Declaration**

We hereby declare that the work which is being presented in the Mini project “Network Firewall” in partial fulfillment of the requirements for project viva voice, is an authentic record of my own work carried under the supervision of our mentor Mr. Amir Khan Sir.

Signature of Candidate:

Name of Candidate:

1. Ayush Kumar Singh (171500074)
2. Govind Sharma (171500074)

Course: B.Tech

Year:3rd

Semester:5th

**ACKNOWLEDGEMENT**

It is indeed with a great pleasure and immense sense of gratitude that we acknowledge the help of these individuals. We are highly indebted to our Mentor Mr. Amir Khan for the facilities provided to accomplish this mini project.

We would like to thank our mentor for this constructive criticism throughout our project.We extremely grateful to our Departmental staff members, Lab technicians and Non-teaching staff members for their extreme help throughout our project.

Finally, we express our heartful thanks to all of our professors who is helping us in thi completion of this project.

**ABSTRACT**

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined like any employee from HR department cannot access the data from code server and at the same time other rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies purpose of that packet.

**Introduction to snort**

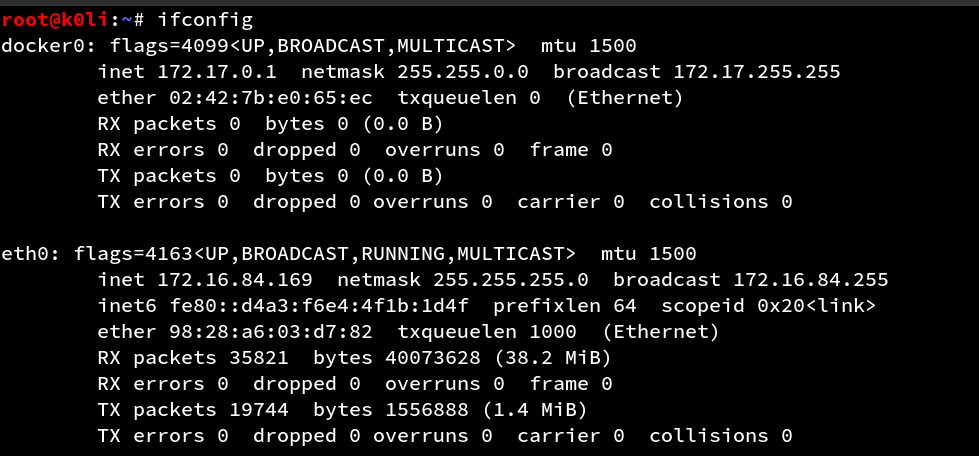
Snort is a Network Intrusion Detection System (NIDS). It’s quite popular and is open source software which helps in monitor network traffic in real-time, hence it can also be considered as a packet sniffer. Basically, it examines each and every data packet in depth to see if there are any malicious payloads. 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

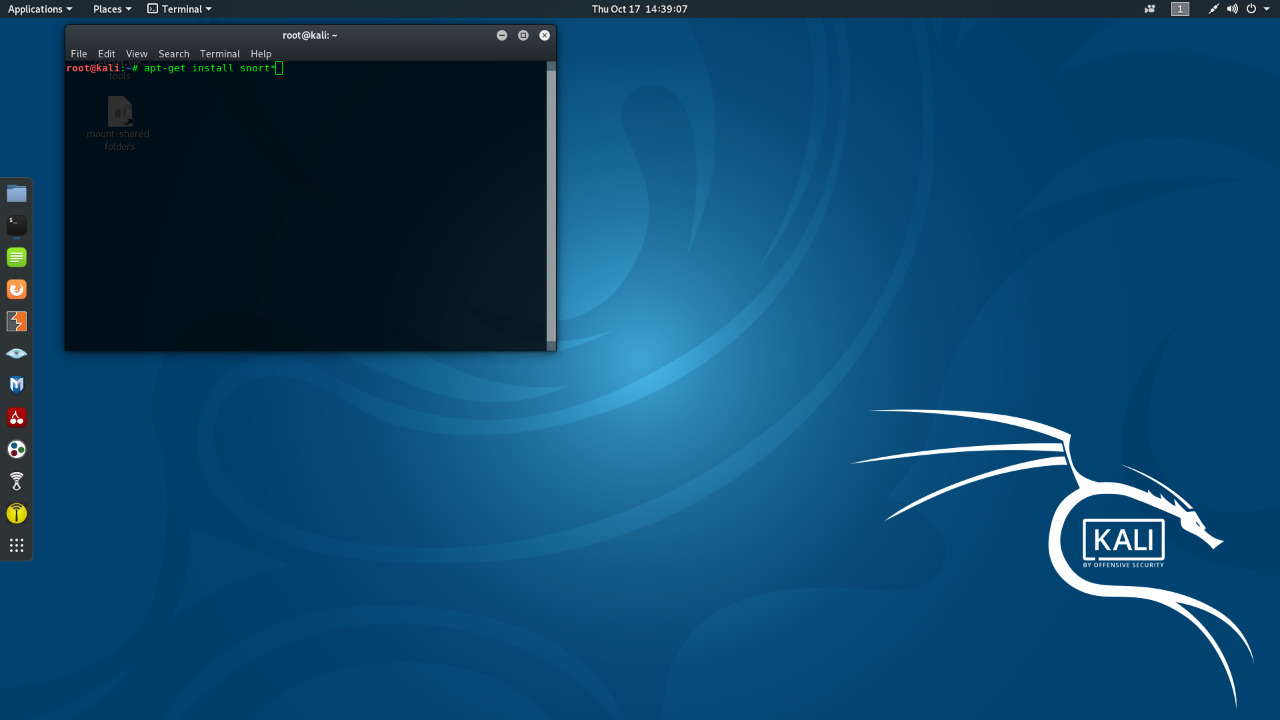
**Following steps are shown to configure snort :-**

* First, use the ifconfig command in your machine to check the interface. As you can see the image below the interface is eth0.

**ifconfig**



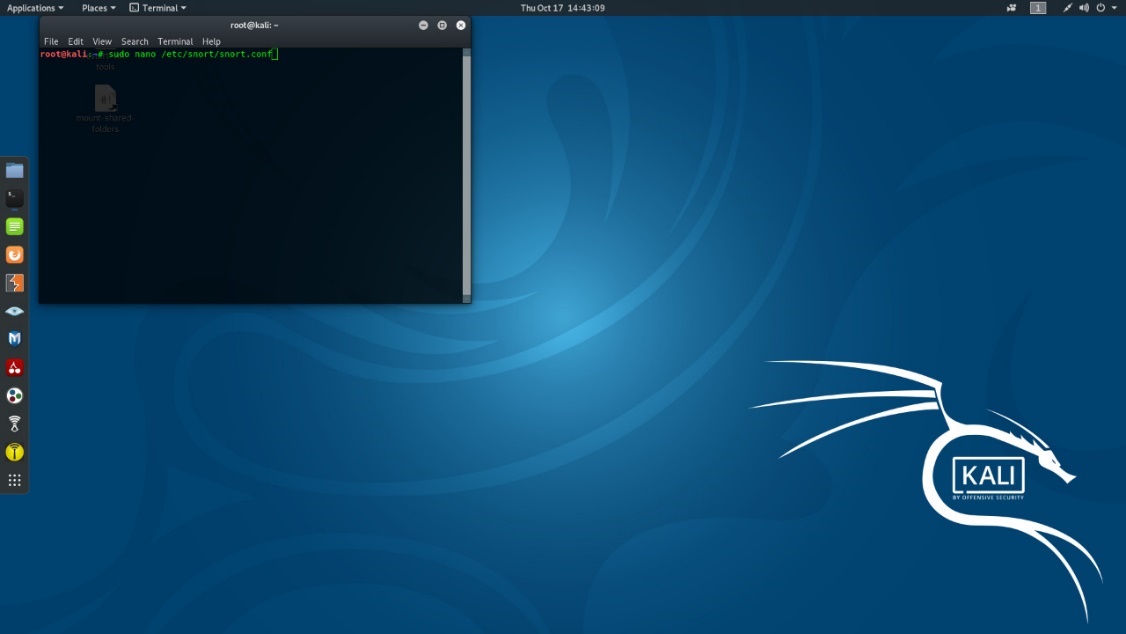
Now we will install SNORT :-



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 :

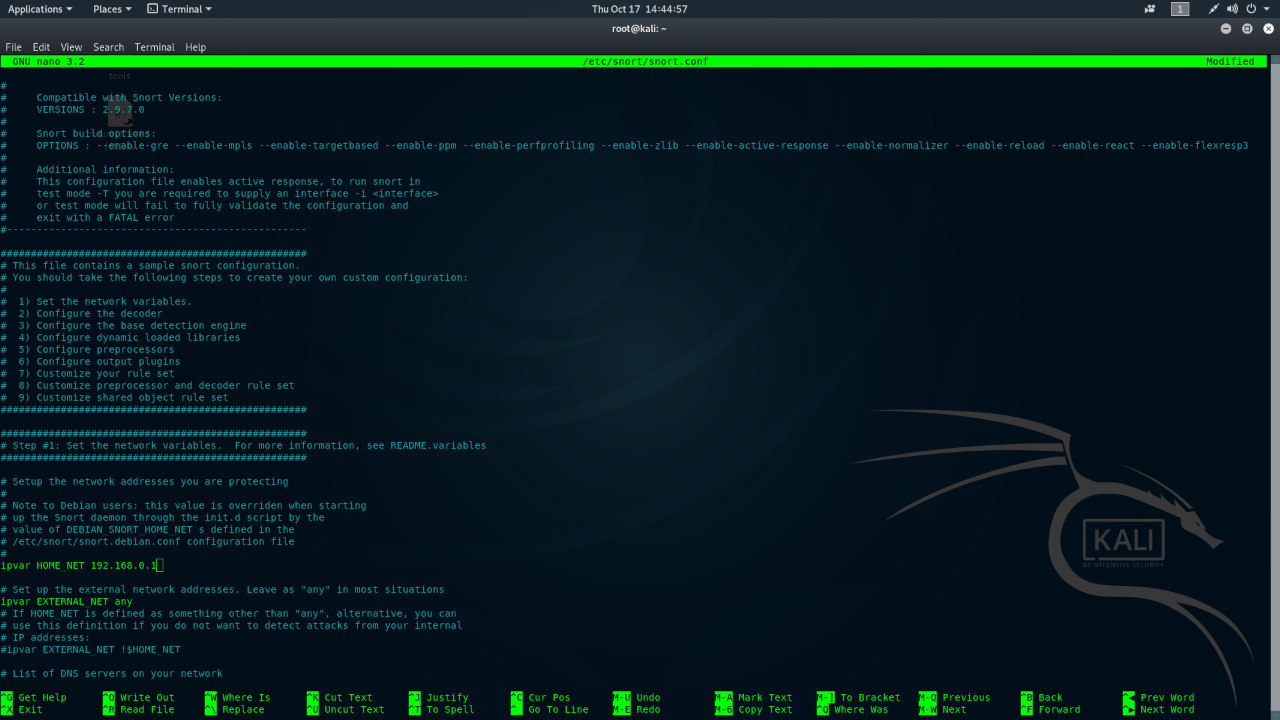
**sudo nano**

**/etc/snort/snort.conf**



**ipvar HOME\_NET**

**192.168.1.21**



sudo snort -A console -i eth0 -c /etc/snort/snort.conf

Once the snort is installed and configured, we can start making changes to its rules as per our own requirement and desire. To the rules on which snort works use the following command :

**cd /etc/snort/rules**

**ls -la**

**Snort Rule Format**



**Let’s start writing snort rule:**

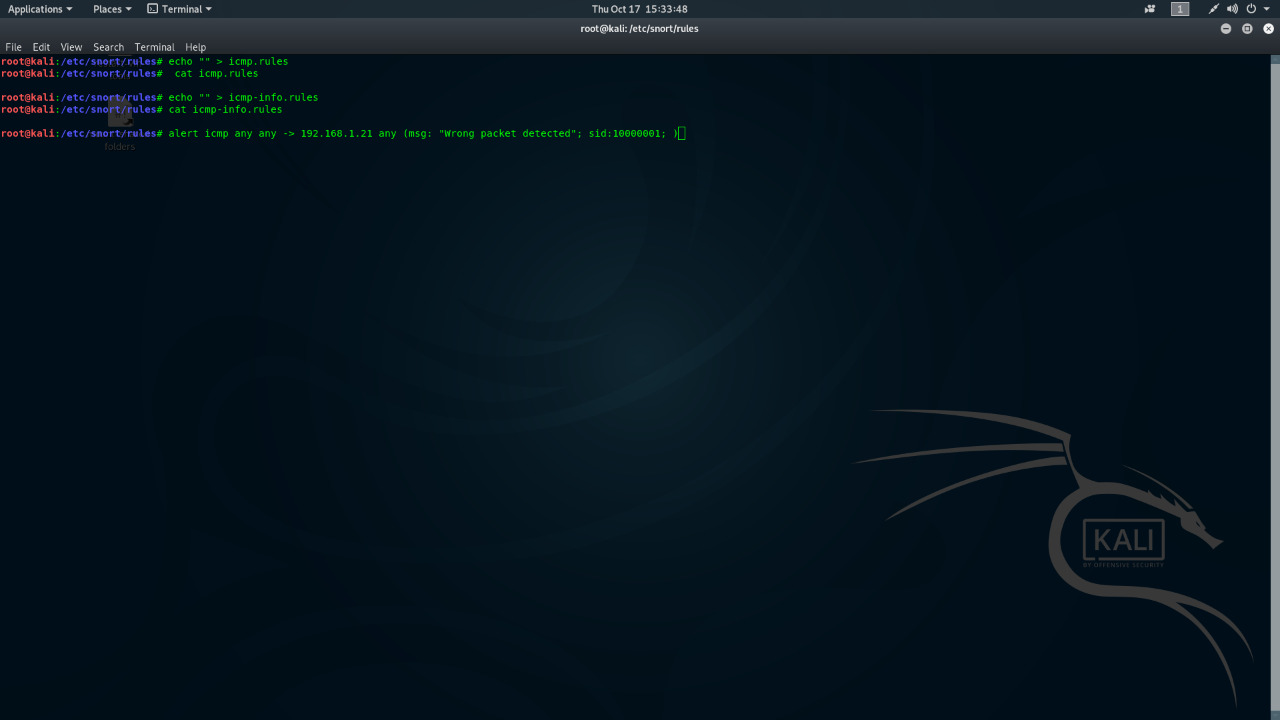
**echo "" > icmp.rules**

**cat icmp.rules**

**echo "" > icmp-info.rules**

**cat icmp-info.rules**

**alert icmp any any -> 192.168.1.21 any (msg: "ICMP Packet found"; sid:10000001; )**



The IP (192.168.47.1) we will attack from is shown in the image shown below :

**ping 192.168.129.141**

Use the following command to activate snort in order to catch the malicious packets :

* sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0
* Here,
* **-A** Set alert mode: fast, full, console, test or none
* **-q** stands for Quiet, Don’t show banner and status report.
* –**u**Run snort uid as <uname> user
* **-g** Run snort gid as <gname> group (or gid)
* **-c** <rules> Use Rules File
* **-i** listen on interface

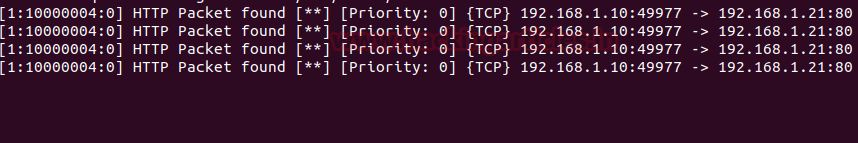
Now we will apply rules on port 21, 22 and 80. This way, whenever a suspicious packet is sent to these ports, we will be notified. Following are the rules to apply to achieve the said :

**alert tcp any any -> any 21 (msg: "FTP Packet found"; sid:10000002; )**

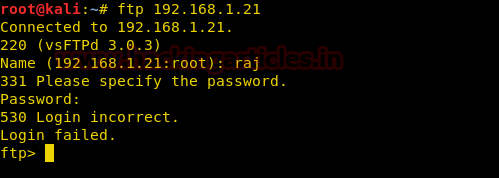
**alert tcp any any -> any 22 (msg: "SSH Packet found"; sid:10000003; )**

**alert tcp any any -> any 80 (msg: "HTTP Packet found"; sid:10000004;)**

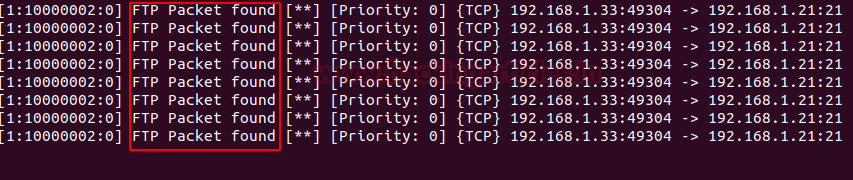
Snort will issue an alert of HTTP packet as its shown in the image below :



Similarly, when a data packet sent to ftp as given in the following image :



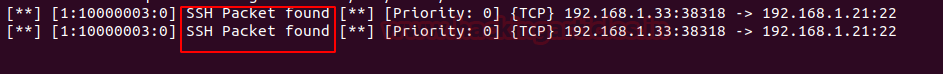
The FTP packets will be detected and one will be notified.



Again, in a similar manner, when one tries to send packets to SSH as shown in the image below :



Snort will notify the administration as shown below :



This way, using snort or any other Firewall(IDS) one can be protected from network attacks by being notified of them in time.