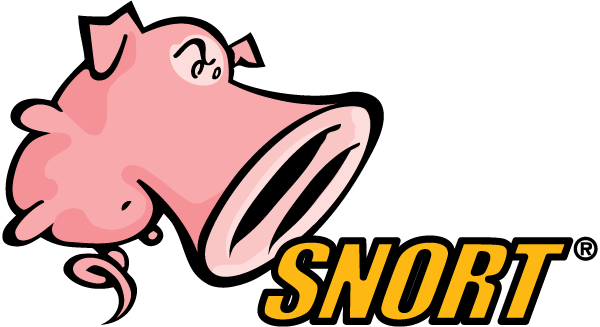
**AYSUN KURT-16030411010- https://github.com/AysunKurt**

**GAMZE YAMAN-17030411034- https://github.com/GamzeYaman**

**GAMZENUR TOKTAY-17030411049- https://github.com/gamzenur12**

****

**MIS311- INFORMATION SECURITY SYSTEMS DESIGN AND APPLICATIONS**

***MIS 311-INFORMATION SECURITY SYSTEMS DESIGN AND APPLICATIONS PROJECT***

**WHAT IS THE SNORT?**

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.

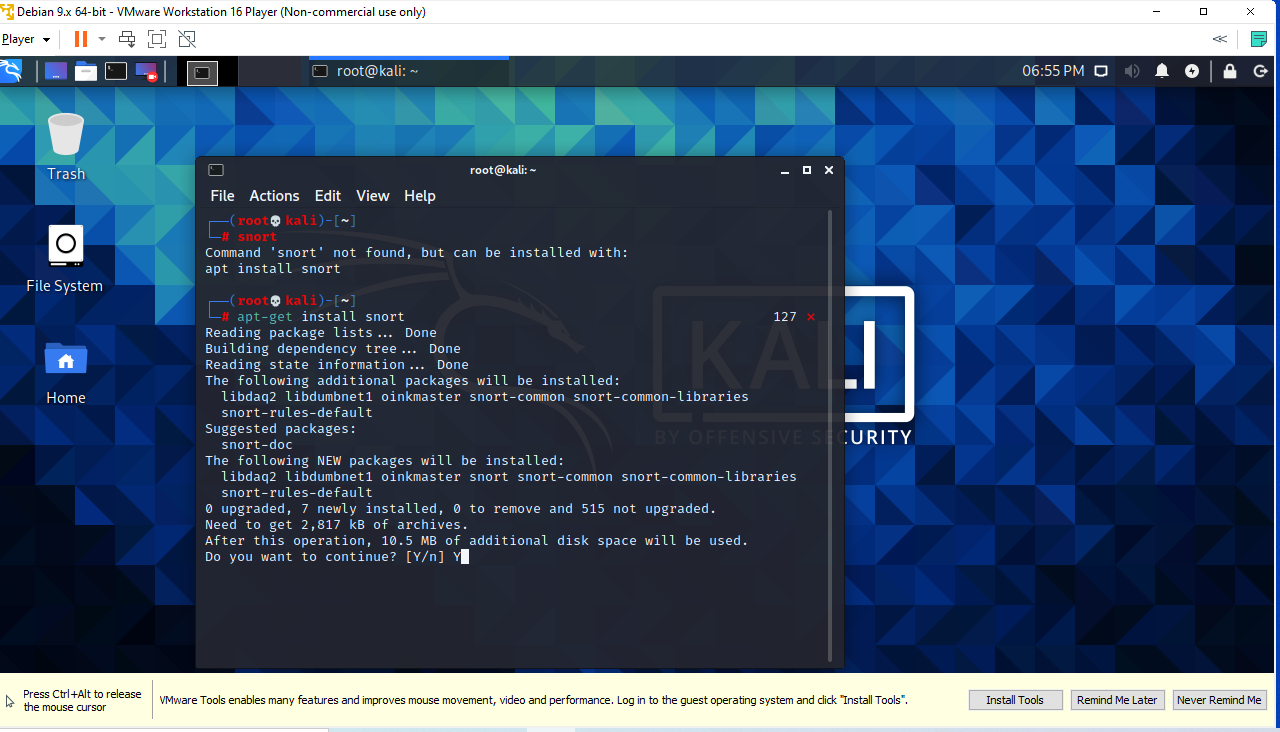
Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system.

**WHY WE USE SNORT?**

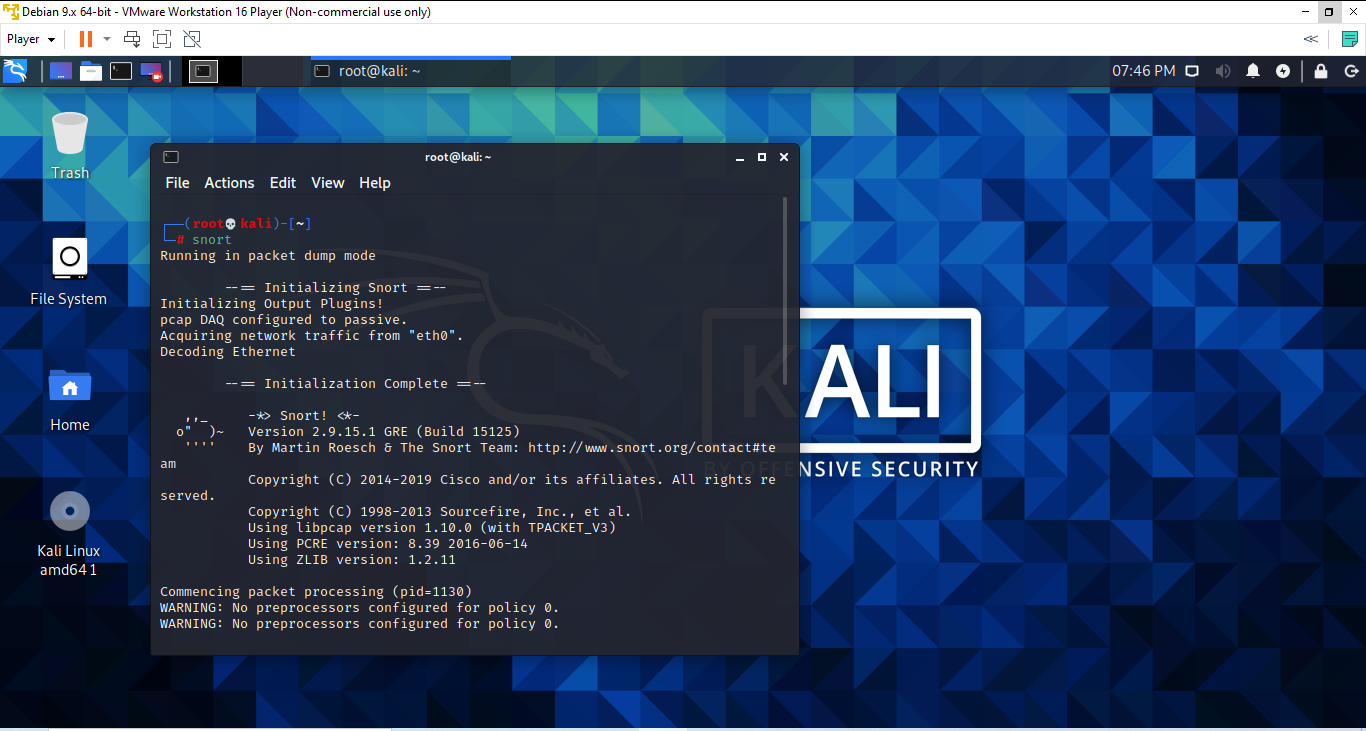
The purpose of our use of snort is to see in detail the attack on a device.The fact that the snort was not complex made the content of our attack more understandable.We set up the hacked device as a virtual machine that we installed on our computer. We protected the security on our original computer. We installed the virtual machine via VMware Workstation.

**HOW WE SET UP SNORT?**

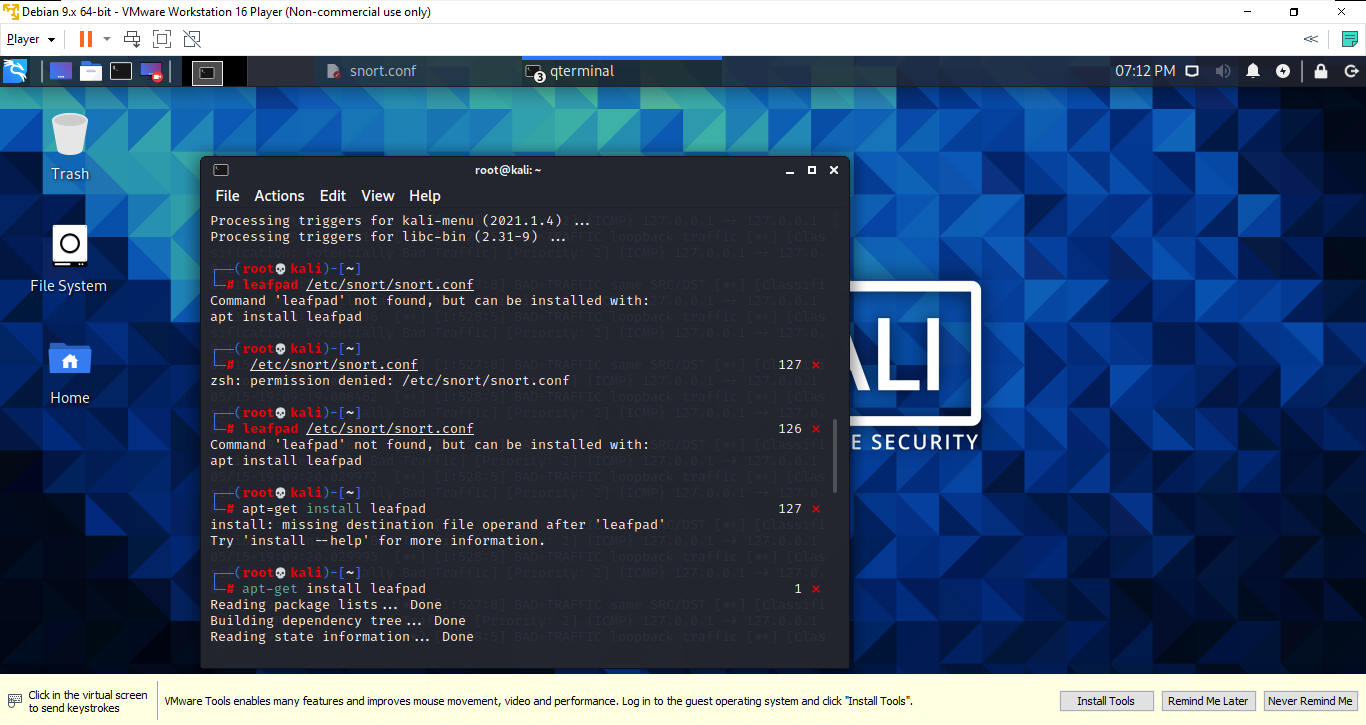
We have used to root user.



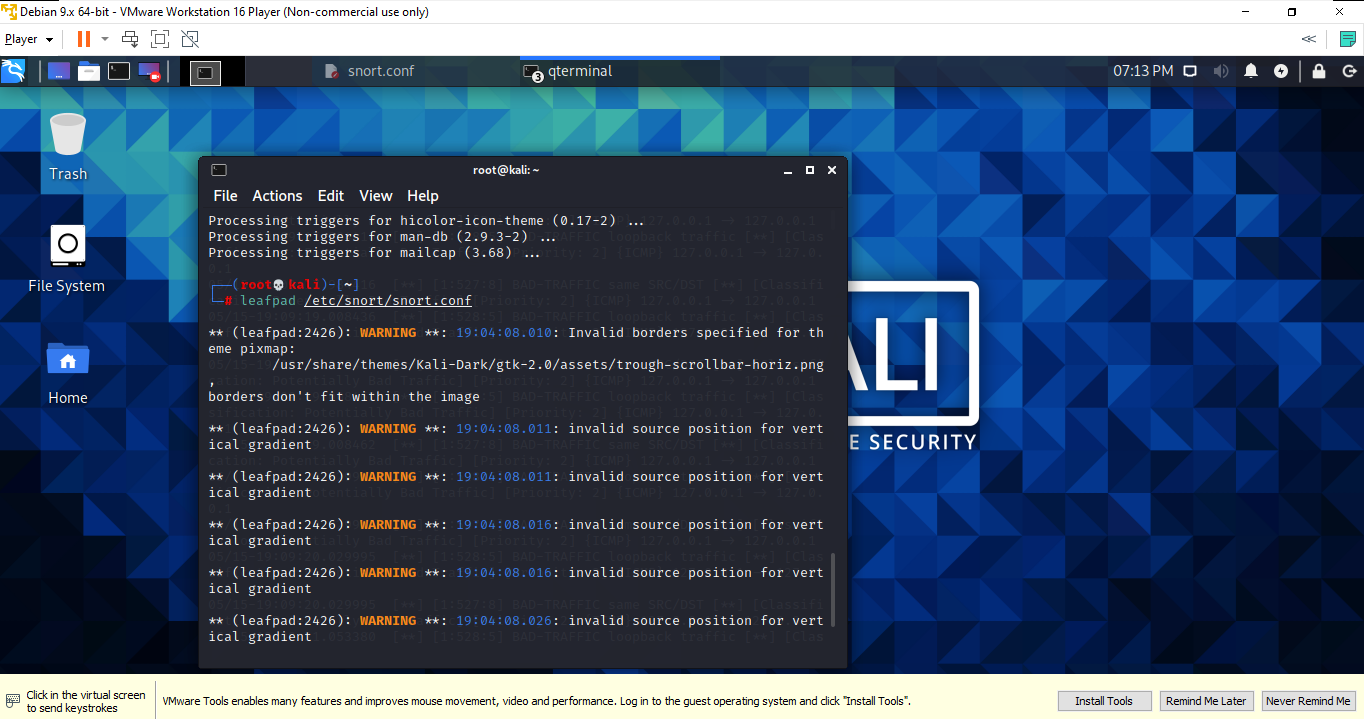
* First, we opened the kali linux operating system on the virtual machine.From the terminal area, we wrote the necessary code to load the snort into the system.



* To check if snort is installed, we wrote the following code to the terminal : ***SNORT.***

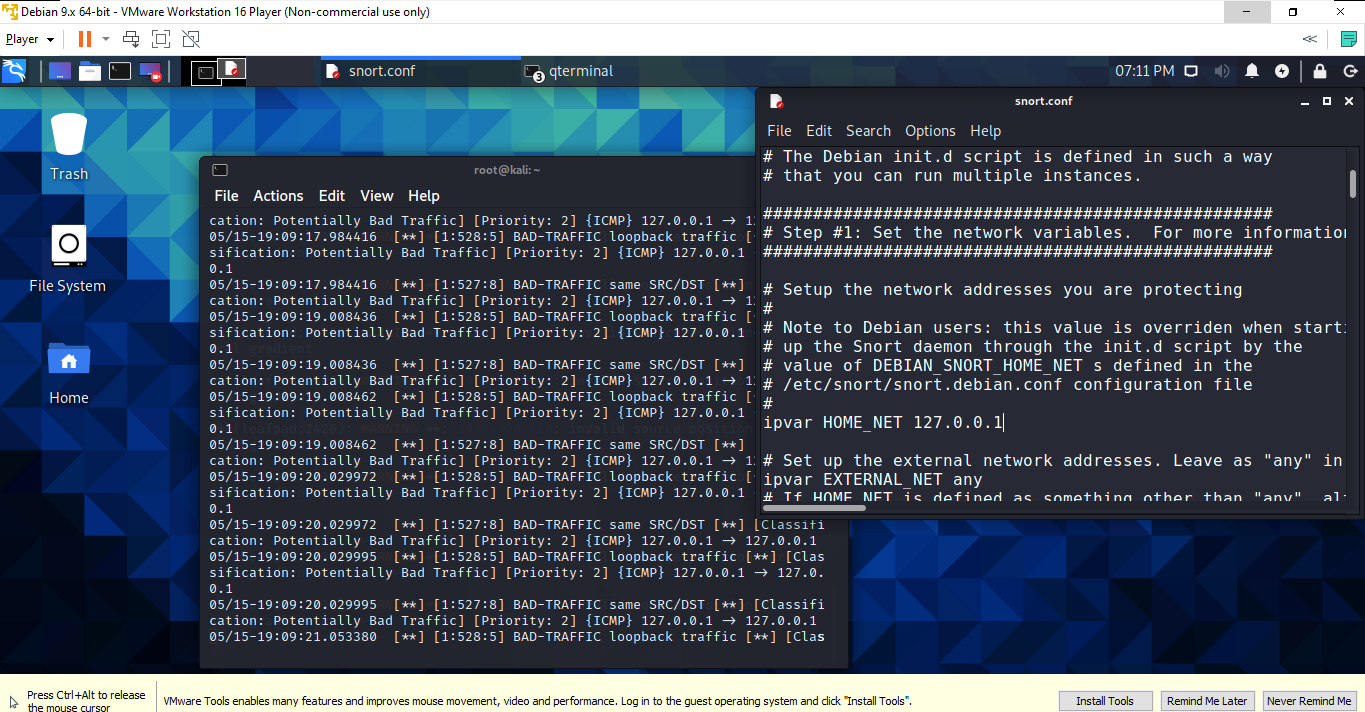


* We have installed the leafpad command, which is not installed on the virtual machine. (You can also see the codes written in screenshot.)

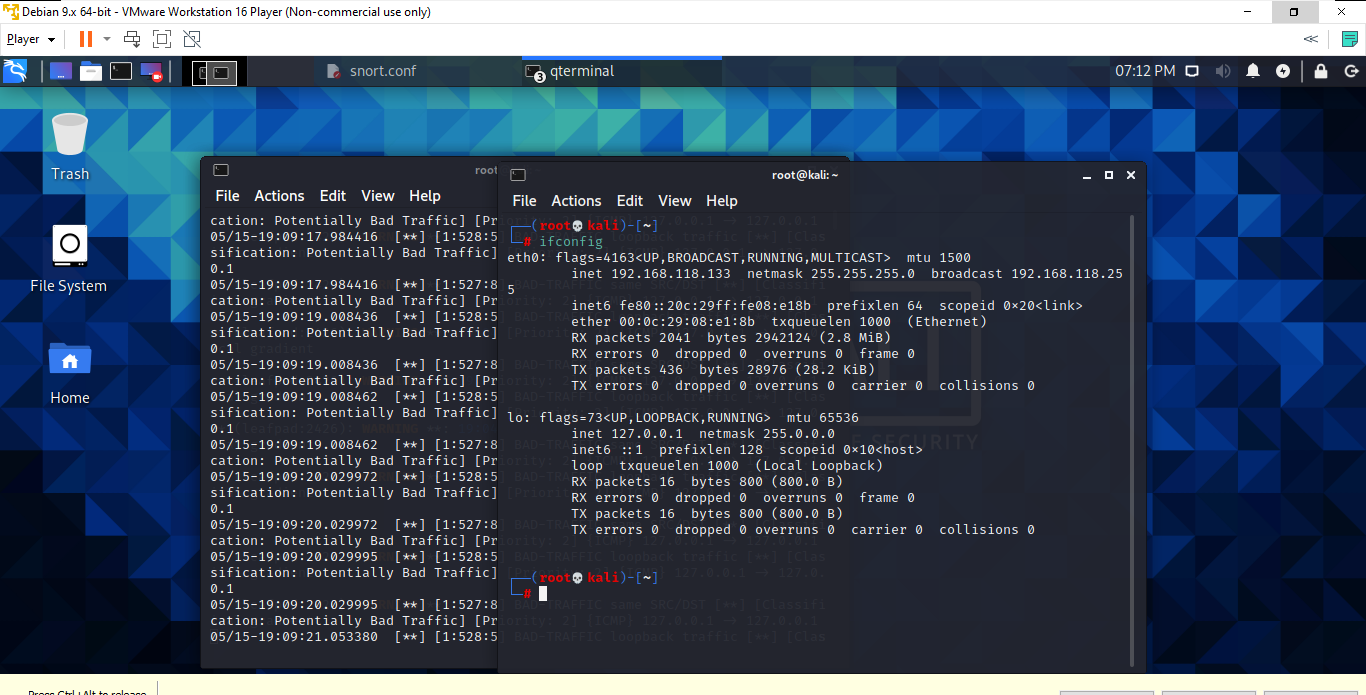


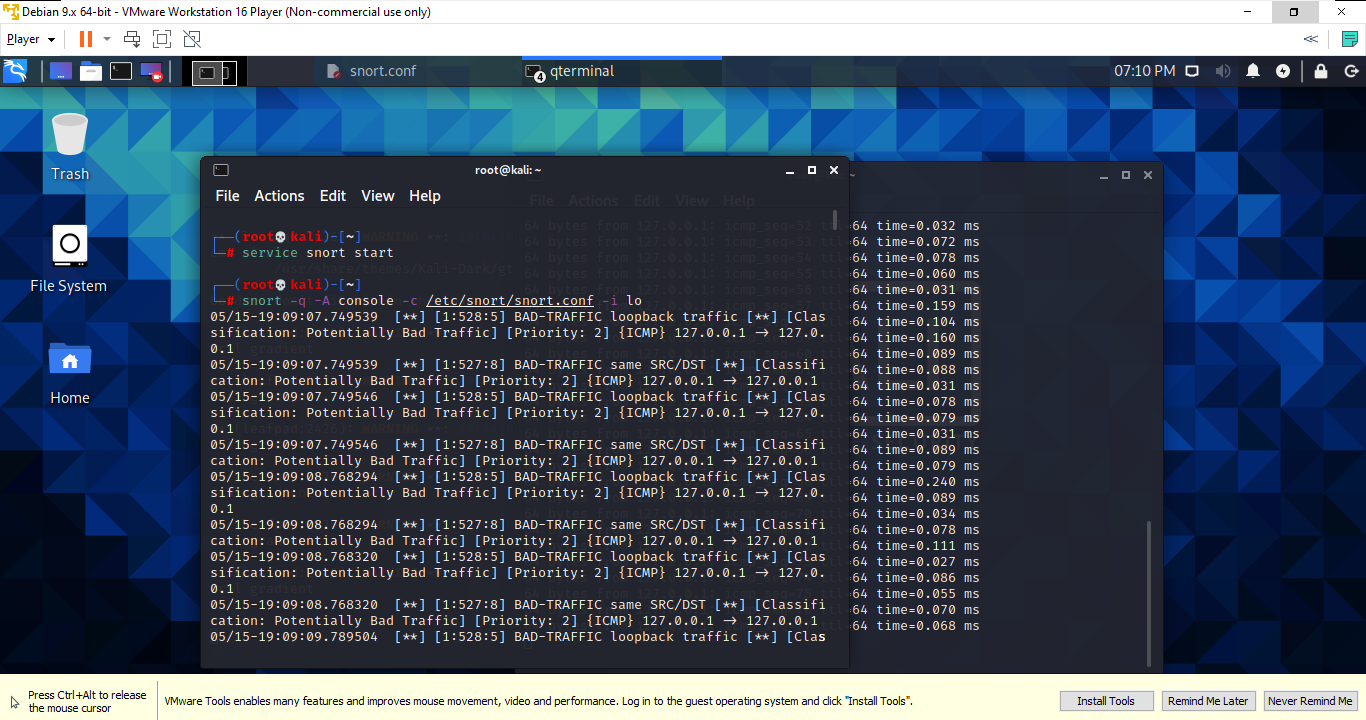
* We used the leafpad command to configure the installed snort.

“leafpad /etc/snort/snort.conf”

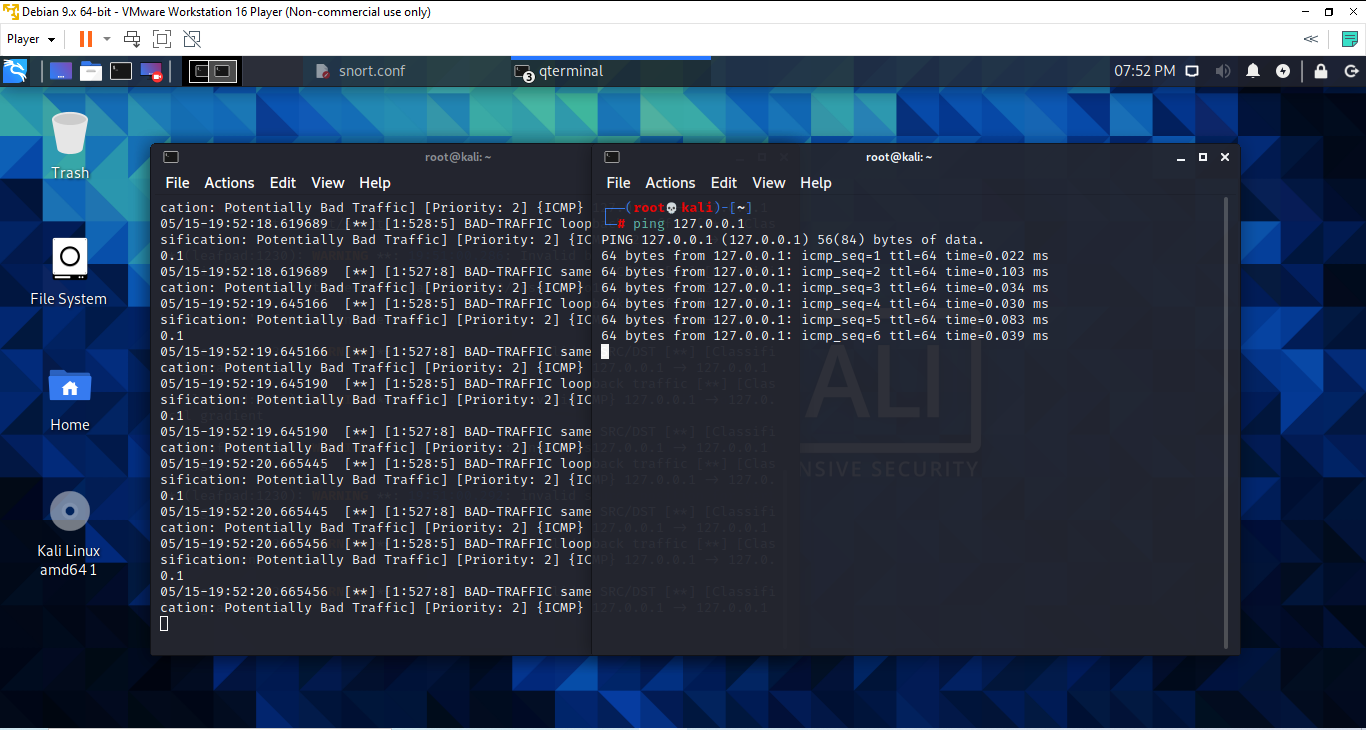


* When we run this code: “leafpad /etc/snort/snort.conf” a text file named snort.conf is opened.
* Using the ifconfig command, we learned the ip address of the computer.(You can review it in the next screenshot.)
* We've placed the IP address we learned in the space here.

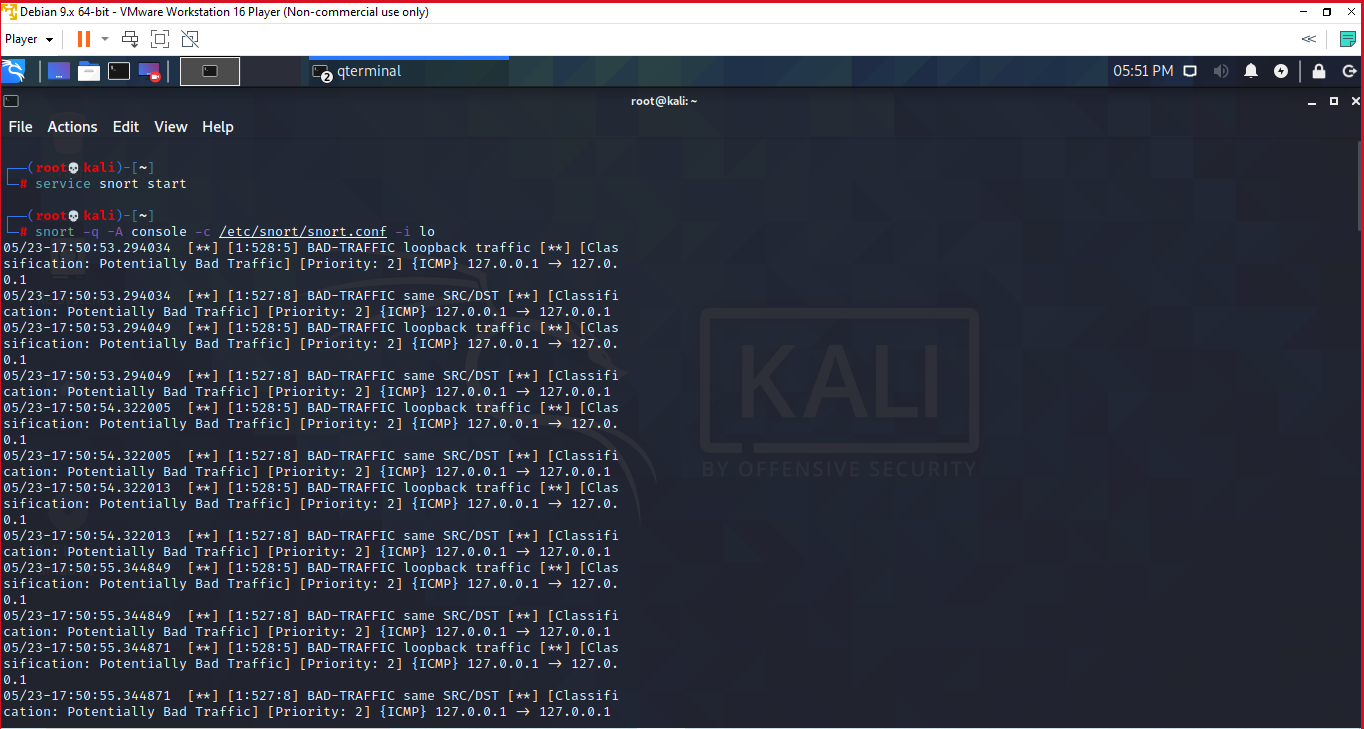




* We used the service command to run snort and detect incoming attacks.



* By opening another terminal, we entered the ip address required by the ping command and launched the attack.
* After the attack began, details of the attack began to appear in the terminal.



05/23-17:50:55.344871 = Indicates when and on what date the ping was thrown.

BAD-TRAFFIC =

127.0.0.1 = Indicates which rope address the attack was made from.

127.0.0.1 = Indicates which ip address the attack was made to.