PRACTICAL – 3

Aim: Experiments with open-source firewall/proxy packages like iptables, squid etc.

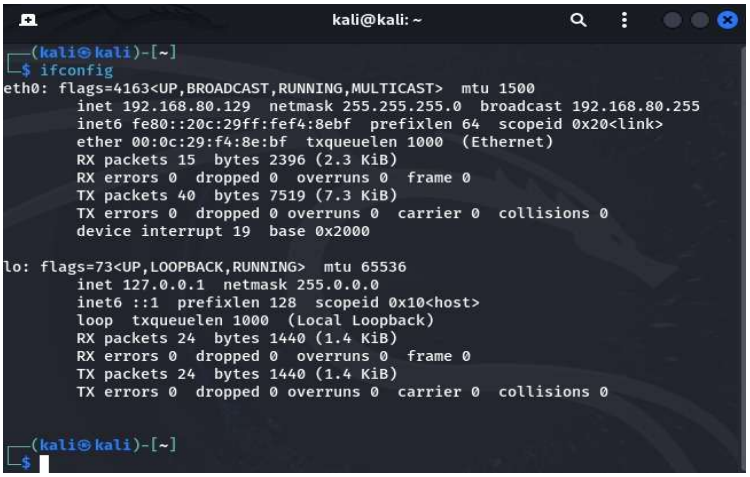
Theory: -

•**Firewall: -** A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

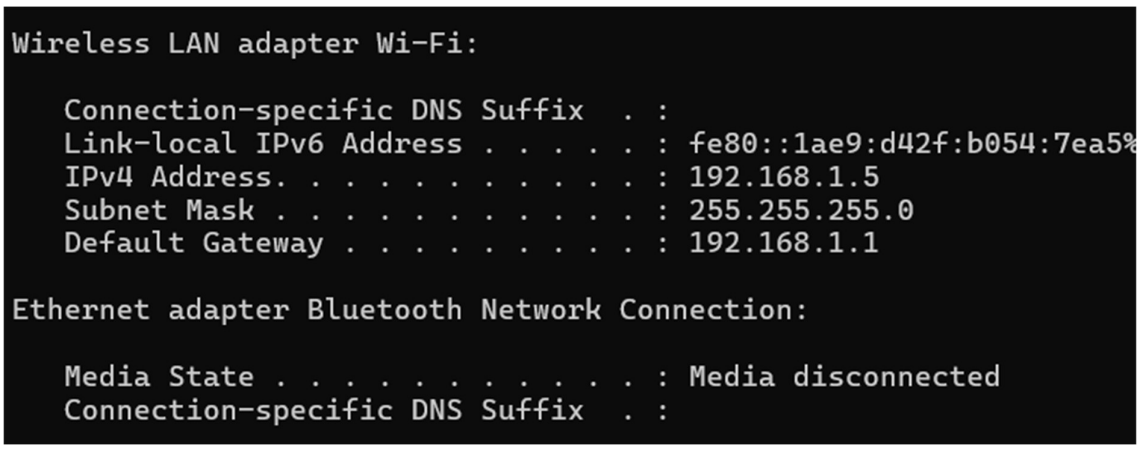
•Kali Linux: -Kali Linux is a Linux operating system that we can use digitally for testing and forensics. It is famous because it is freely available and also easy to setup. To use this OS, we just need a Virtual Box and we can directly start using Kali Linux on our system.

•Virtual Box: - VM ware is a tool for virtualizing x86 and AMD64/Intel64 computing architecture, enabling users to deploy desktops, servers, and operating systems as virtual machines. In simple words Virtual Tool is a tool provided by Oracle using which we can use Kali Linux easily on our device. So, in this practical we are going to use some well-known commands and firewall rules in Kali Linux to test attacks and its defence measures.

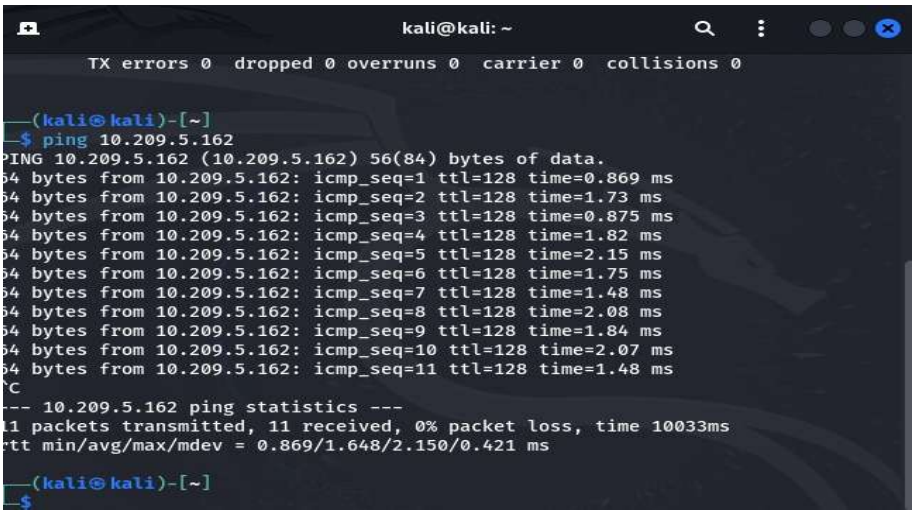
Step 1: Open the terminal in kali Linux and enter ifconfig.



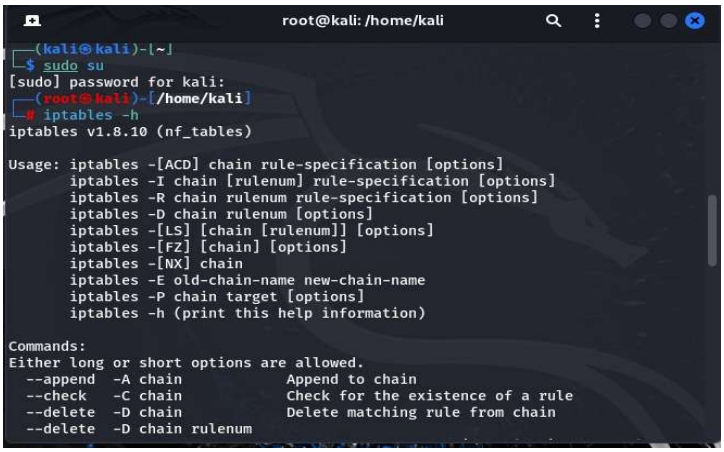
Step 2: open the command prompt in windows and enter the ipconfig.

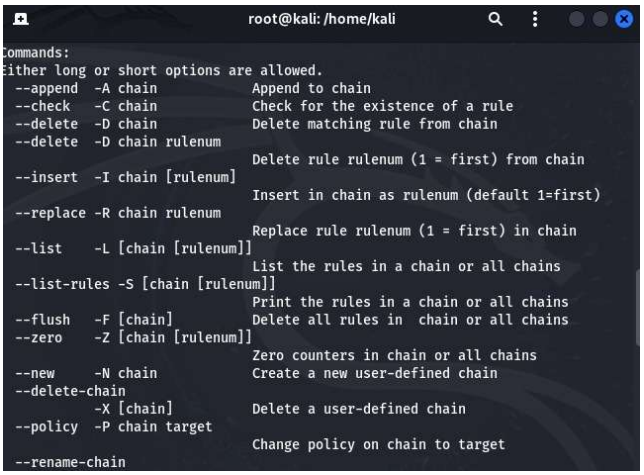


Step 3: copy the IP address and open the terminal in kali linux and enter the ping command with IP address.



Step 4: Enter the sudo su command and enter password. After entering password enter iptables -h command in terminal.



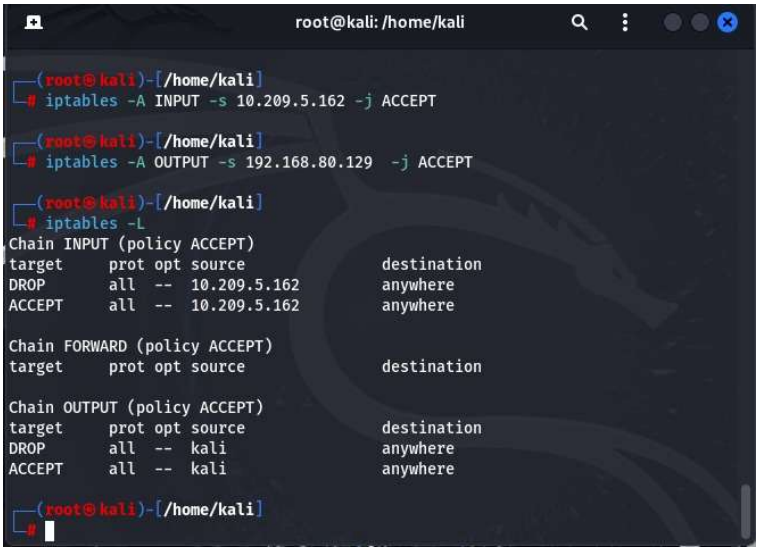


Step 5: Enter the command iptables -L.

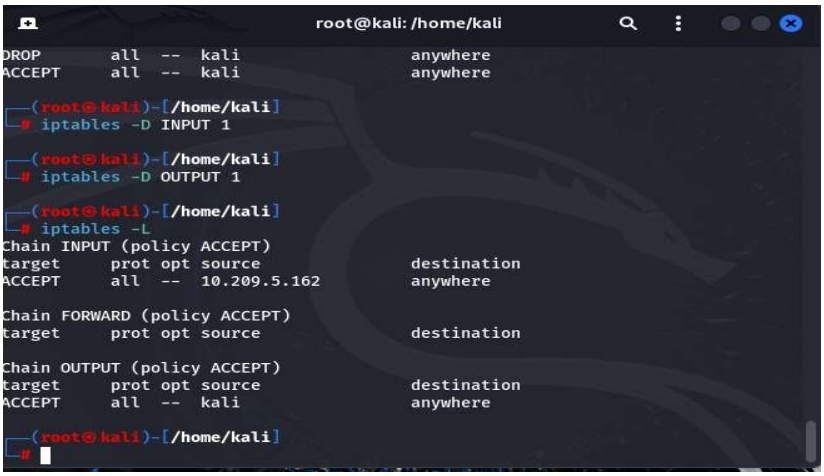
Step 6: Enter iptables -A INPUT -s 10.209.5.162 -j DROP command in terminal and click enter.
Step 7: Enter iptables -L and click enter it will show all chain inputs which are accepting policy.

Step 8: Enter iptables -A OUTPUT -s 192.168.80.129 -j DROP command in terminal and click enter.
Step 9: Enter iptables -L and click enter it will show all chain inputs which are accepting policy.

Step 10: Enter iptables -A INPUT -s 10.209.5.162 -j ACCEPT command in terminal and click enter.
Step 11: Enter iptables -L and click enter it will show all chain inputs which are accepting policy
Step 12: Enter iptables -A INPUT -s 192.168.80.129 -j ACCEPT command in terminal and click enter.
Step 14: Enter iptables -L and click enter it will show all chain inputs which are accepting policy



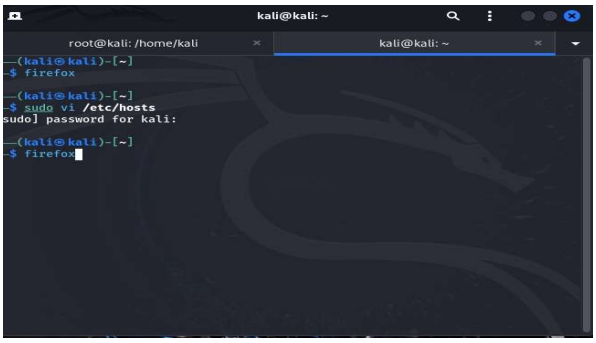
Step 15: Enter iptables -D INPUT 1 command in linux click enter and enter iptables -D OUTPUT 1 click enter and enter iptables -L



Step 16: Enter sudo iptables -A OUTPUT -p tcp -o etho -s 192.168.80.129 –dport 443 -j DROP and iptables -D OUTPUT 1 and iptables -L in linux

To block the website in kali linux:

Step 1: Enter sudo vi /etc/hosts command in terminal and click enter after that enter password.



Step 2: Enter the 127.0.1.1 and targeted website address in terminal and press esc and type :wq to save

Step 3: It will back to terminal and type firefox in terminal and wait for sometime now enter your targeted website.