**AIM: To Study working of Firewall in UBUNTU.**

**THEORY:**

**Software Requirements:**

UBUNTU: For working with its firewall.

**1.What is Firewall?**

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

**2.Explain the Chains in Firewall.**

Chains are a set of rules defined for a particular task. We have three chains(set of rules) which are used to process the traffic:-

1. INPUT Chains: Any traffic coming from the internet(network) towards your local machine has to go through the input chains. That means they have to go through all the rules that have been set up in the Input chain.

2. OUTPUT Chains: Any traffic going from your local machine to the internet needs to go through the output chains.

3. FORWARD Chain: Any traffic which is coming from the external network and going to another network needs to go through the forward chain. It is used when two or more computers are connected and we want to send data between them.

Different Policies :-

There are three actions which the iptables can perform on the traffic

1. ACCEPT: When traffic passes the rules in its specified chain, then the iptable accepts the traffic. That means it opens up the gate and allows the person to go inside the kingdom of Thanos.

2. DROP: When the traffic is unable to pass the rules in its specified chain, the iptable blocks that traffic.That means the firewall is closed.

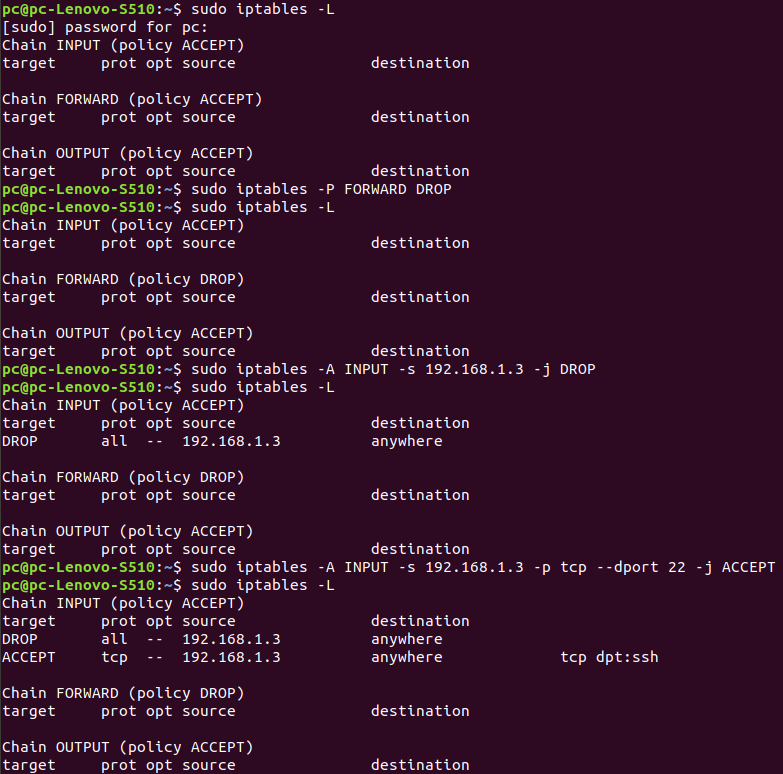
3. REJECT: This type of action is similar to the drop action but it sends a message to the sender of the traffic stating that the data transfer has failed.

As a general rule, use REJECT when you want the other end to know the port is unreachable’ use DROP for connections to hosts you don’t want people to see

**3.Explanation for each rule.**

1.sudo iptables -L

Used to list the rules of the current iptables

****

**Figure 1**

2. sudo iptables -F

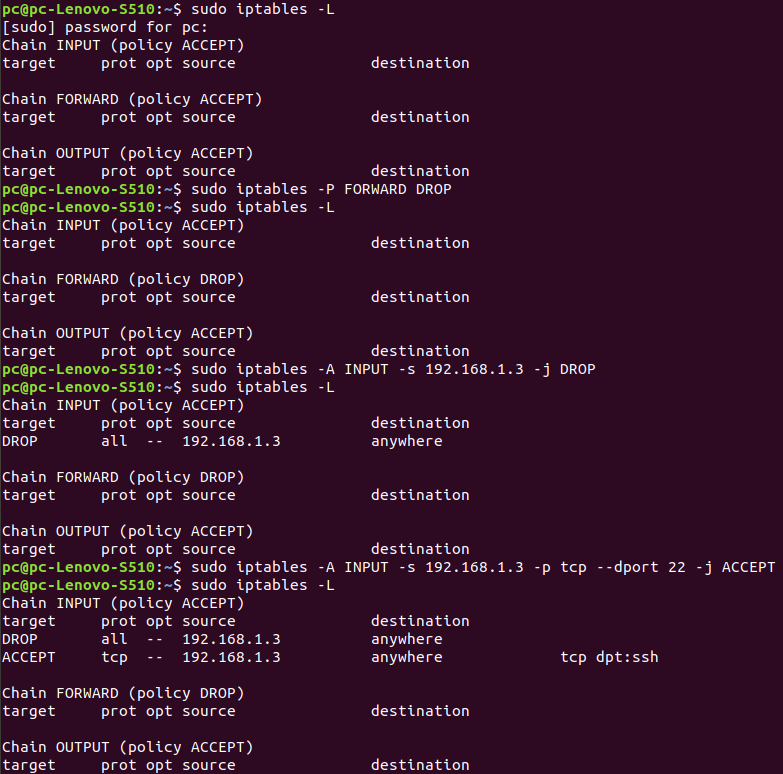
If you ever want to clear/flush out all the existing rules. Run the following command will reset the iptables.

3. sudo iptables -P Chain\_name Action\_to\_be\_taken

The default policy of each of the chain is ACCEPT. In order to change the policy of forwarding to drop:-

sudo iptables -P FORWARD DROP

The above command will stop any traffic to be forwarded through your system. That means no other system can your system as an intermediary to pass the data.

****

**Figure 2**

4. sudo iptables -A/-I chain\_name -s source\_ip -j action\_to\_take

Implementing the DROP rule.

sudo iptables -A INPUT -s 192.168.1.3 -j DROP

The components:-

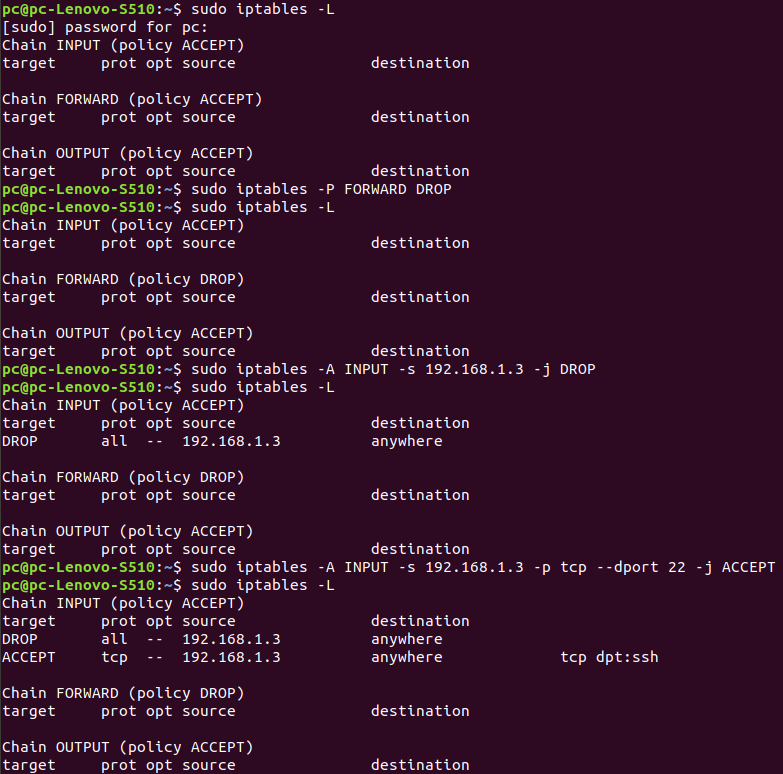
-A INPUT :- The flag -A is used to append a rule to the end of a chain. This part of the command tells the iptable that we want to add a rule to the end of the INPUT chain.

-I INPUT:- In this flag the rules are added to the top of the chain.

-s 192.168.1.3:- The flag -s is used to specify the source of the packet. This tells the iptable to look for the packets coming from the source 192.168.1.3

-j DROP: This specifies what the iptable should do with the packet.

In short, the above command adds a rule to the INPUT chain which says, if any packet arrives whose source address is 192.168.1.3 then drop that packet, that means do not allow the packet reach the computer.

****

**Figure 3**

5. sudo iptables -A/-I chain\_name -s source\_ip -p protocol\_name --dport port\_number -j Action\_to\_take

Implementing a ACCEPT rule :

sudo iptables -A INPUT -s 192.168.1.3 -p tcp --dport 22 -j ACCEPT

Used if you want to add rules to specific ports of your network

-p protocol\_name:-

This option is used to match the packets that follow the protocol protocol\_name.

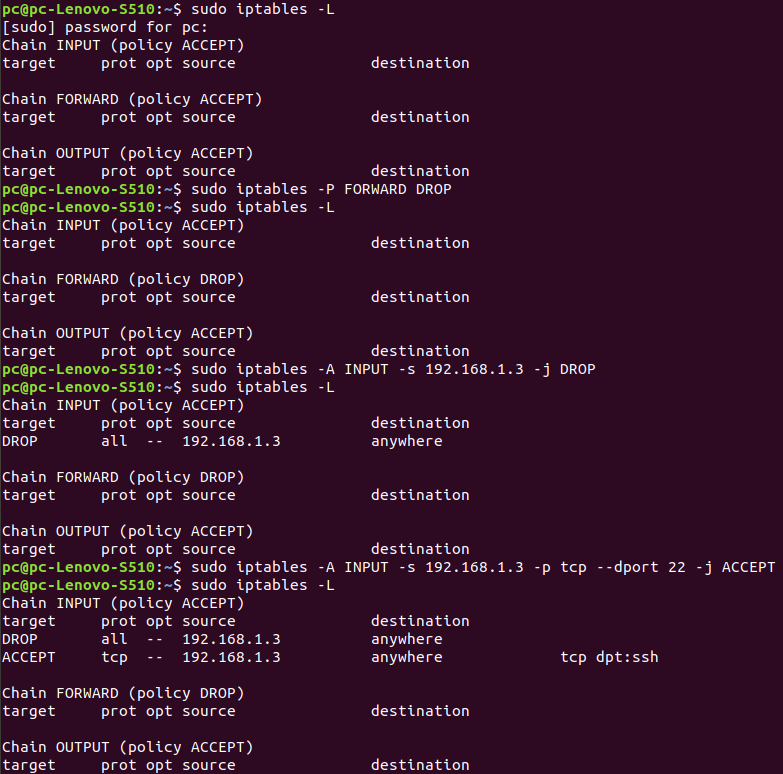
-dport port\_number:

This is option is available only if you give the -p protocol\_name option. It specifies to look for the packets that are going to the port “port\_number”.

Example:-

Let’s say we want to keep our SSH port open (we will assume in this guide that the default SSH port is 22) from the 192.168.1.3 network we blocked in the above case. That is we only want to allow those packets coming from 192.168.1.3 and which wants to go to the port 22.

The below shown command says looks for the packets originating from the IP address 192.168.1.3, having a TCP protocol and who wants to deliver something at the port 22 of my computer. If you find those packets then Accept them.

****

**Figure 4**

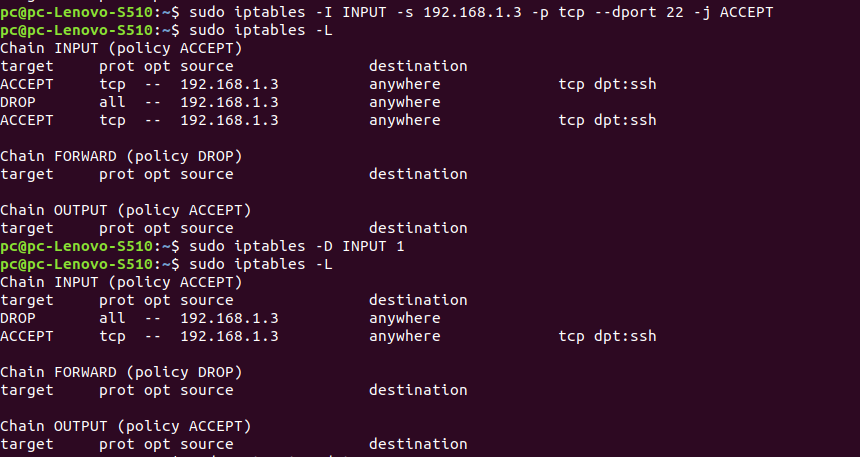
6. sudo iptables -I INPUT -s 192.168.1.3 -p tcp --dport 22 -j ACCEPT

The above command actually does not allow the packets(in Figure 4).

The Rules you set in the iptables are checked from the top to the bottom. Whenever a packet is processed to one of the top rules, it is not checked with the lower rules.

In our case, The packet was checked with the topmost rule, which says that the iptable must drop any packet coming from 192.168.1.3. Hence once the packet got accessed through this rule, it did not go to the next rule which allowed packets to the port 22. Therefore it failed.

So to solve it, Add the rule to the top of the chain. All you need to do is change the -A option to -I option.Therefore, any packet coming from 192.168.1.3 is first checked if it is going to the port 22 if it isn’t then it is run through the next rule in the chain. Else it is allowed to pass the firewall.

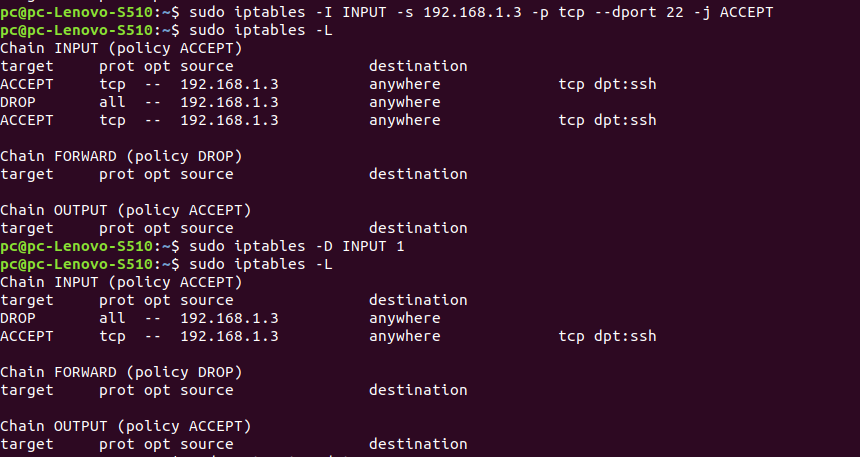
****

**Figure 5**

7. sudo iptables -D chain\_name rule\_number

sudo iptables -D INPUT 1

Used for Deleting the rules from iptables. Below we deleted Rule 1 by using the command.

****

**Figure 6**

8.For saving the configuration network administrators use:-

sudo apt-get update

sudo apt-get install iptables-persistent

Once the installation is complete, you can save your configuration using the command:-

sudo invoke-rc.d iptables-persistent save

**CONCLUSION:**

From this experiment we learnt about firewalls. In simple words, firewall is a network security door that will not allow any untrusted sources to enter our system. We learnt about the iptable of a firewall and rules in it. The rules are made up of chains and policy. Using them we can set up our own rules for the firewall.