Faculty of Engineering And Technology

Name: Kumavat Rahul

Subject Name: Cyber Security
Subject Code : 203105327
B.Tech CSE Year:3rd Sem:6th

Practical : 1

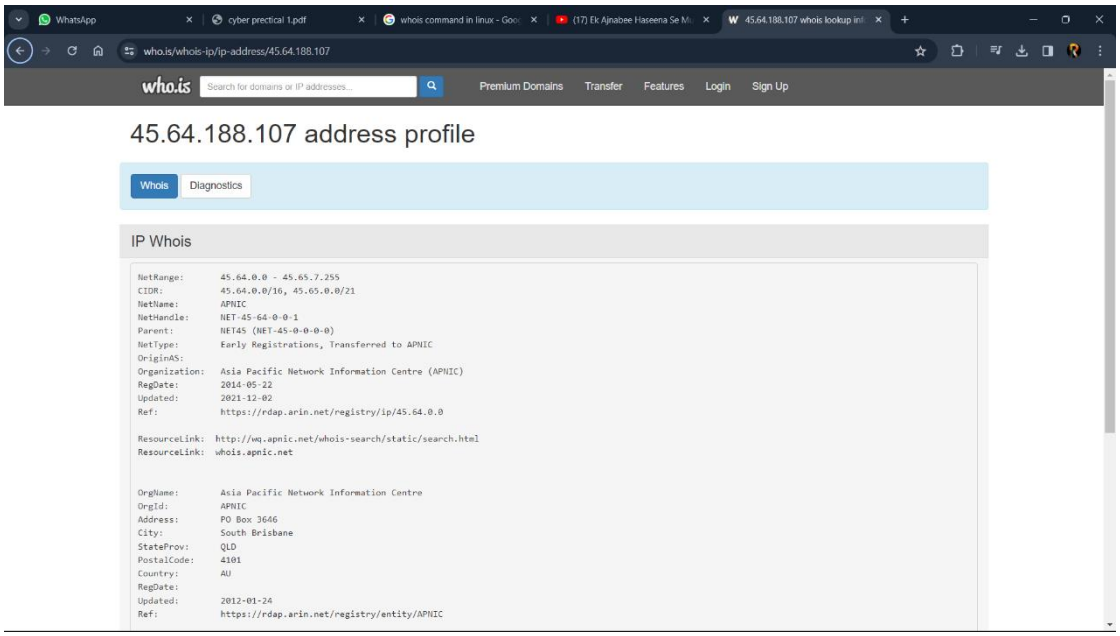
AIM : Implementation to gather information from any PC's connected to the LAN using whois, port scanner, network scanning, ANGRY IP scanners etc.

Theory :

WHOIS:

The 'whois' command in Linux is a utility for retrieving information about a domain or an IP address. You can use it like this: whois example.com . This command will return information about the 'example.com' domain.

To use whois open a who.is on chrome and write any IP address to know about it.



1. **Port Scanner:**
   Nmap is convenient during penetration testing of networked systems. Nmap provides the network details, and also helps to determine the security flaws present in the system. Nmap is **platform independent** and runs on popular **operating systems** such as **Linux**, **Windows** and **Mac**.

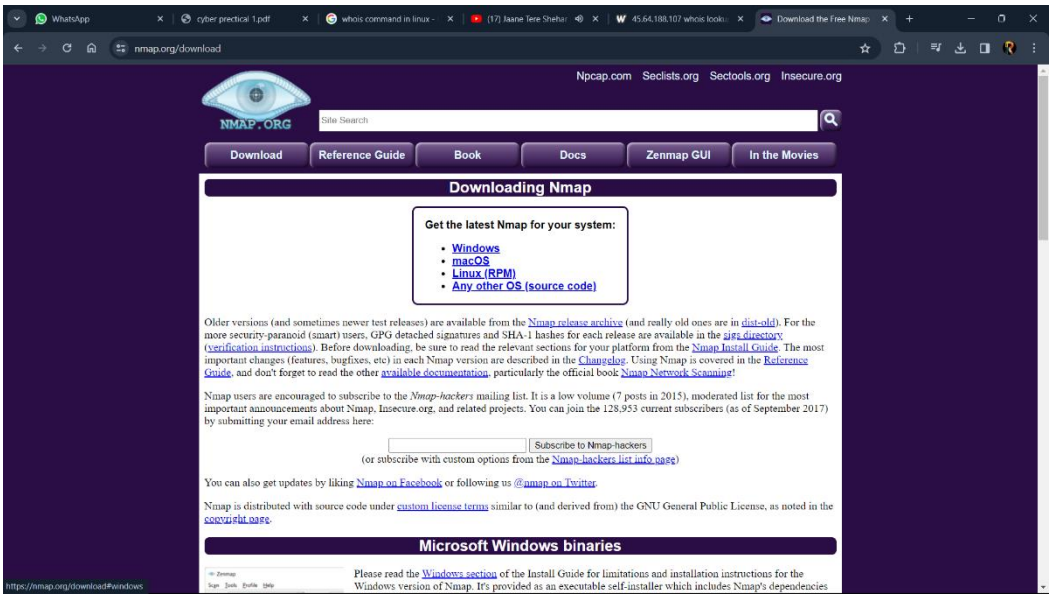
Enrollment No. :-210305105475

- Nmap can search for hosts connected to the network
- It can search for free ports on the target host.
- It detects all services running on the host with the help of OS.

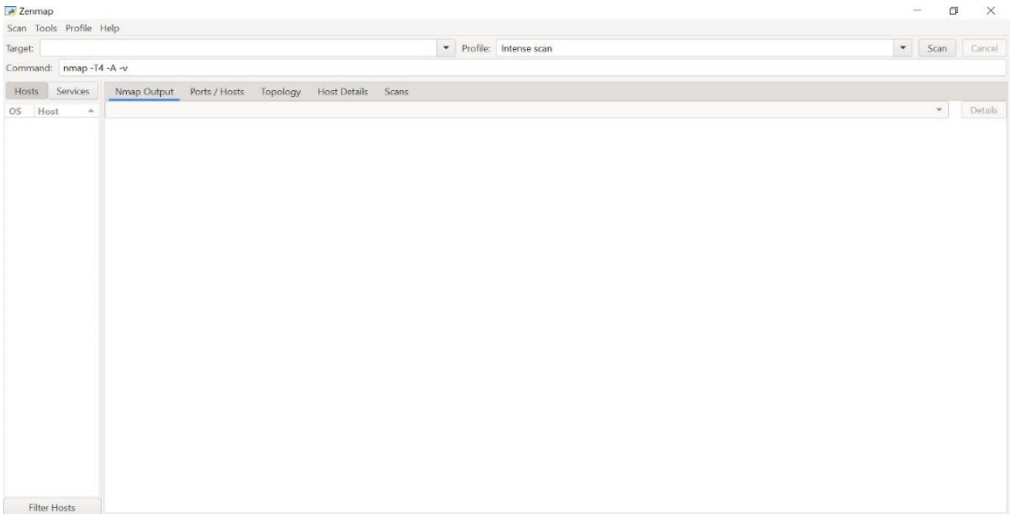
Advantages of Nmap:

Nmap has a lot of advantages that make it different from other network scanning tools.

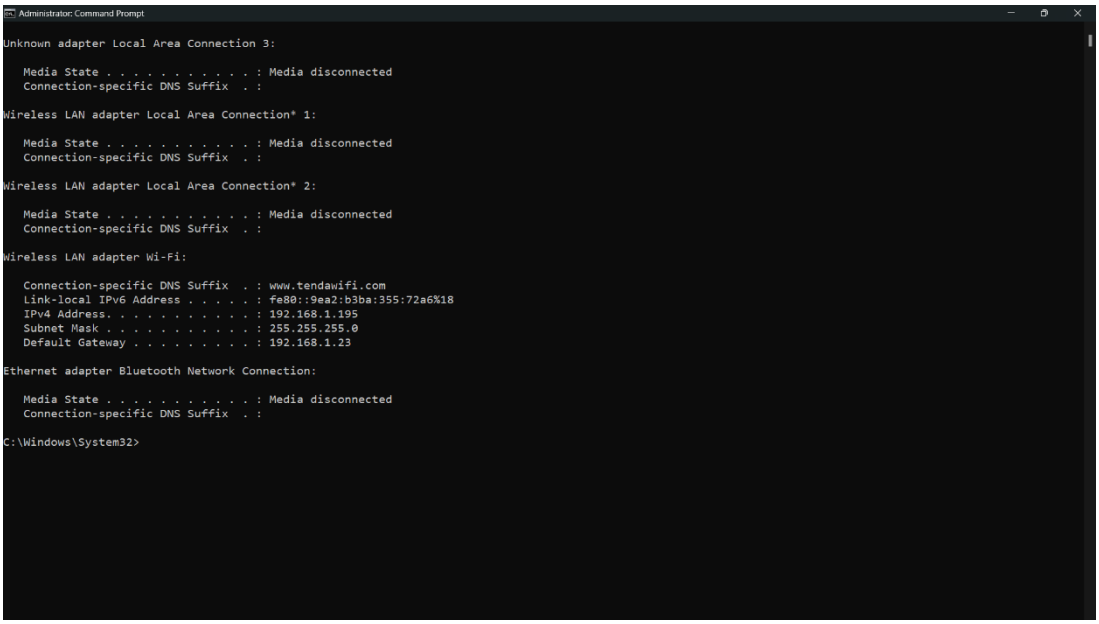
Step 1: Install NMAP in windows



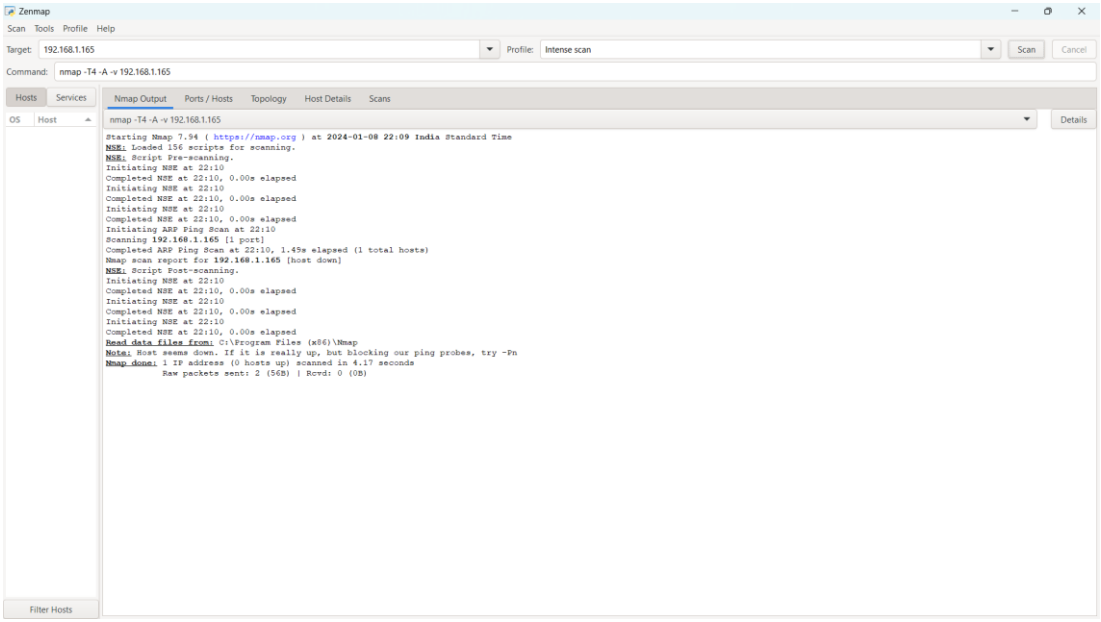
Step 2 : Open Nmap



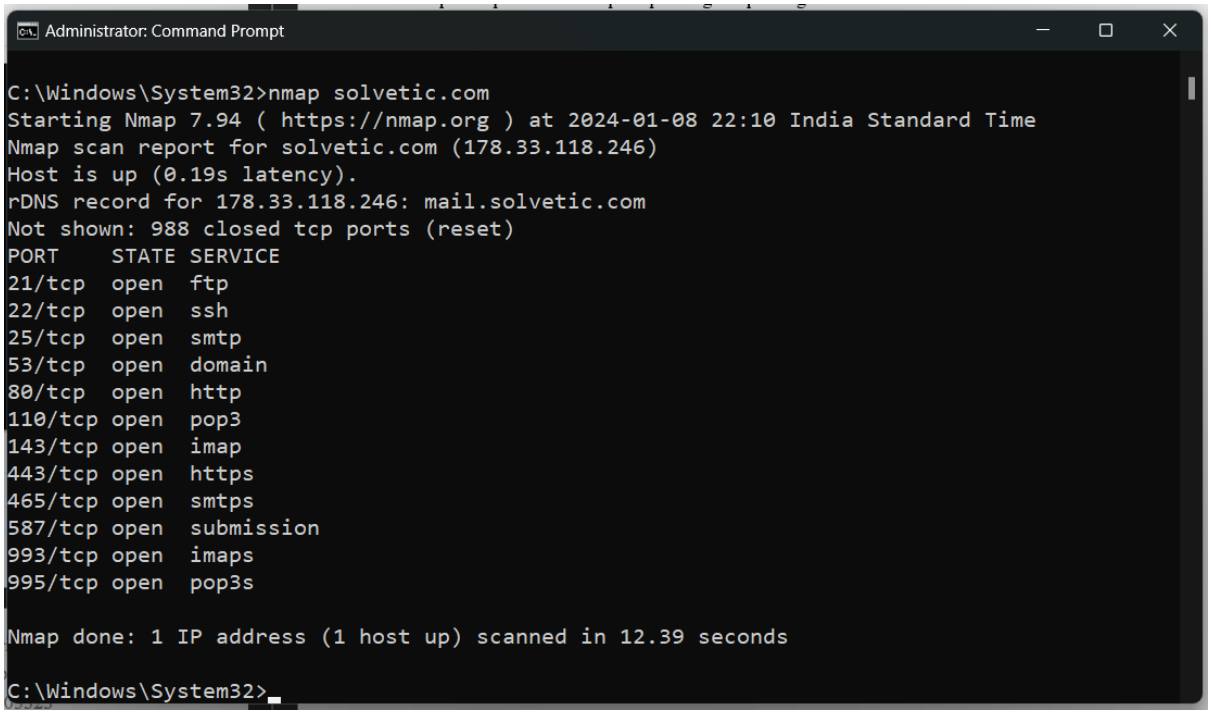
Step 3 : Open command prompt and give ipconfig command



Step 4 : paste IP address in target select scan type and press scan button.



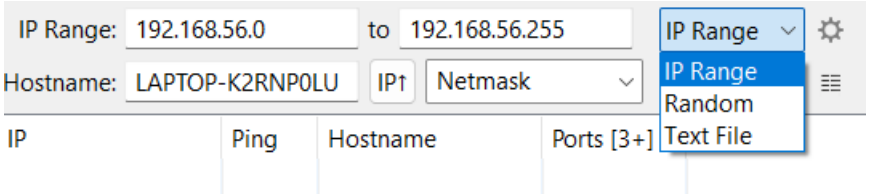
Step 5 : open command prompt and run as admin to see the open ports run:



2. Angry IP Scanner

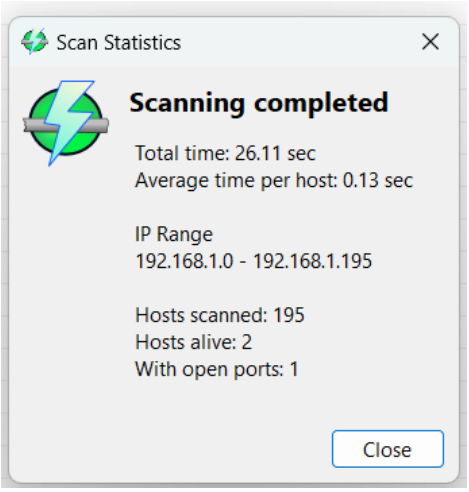
Implementation:

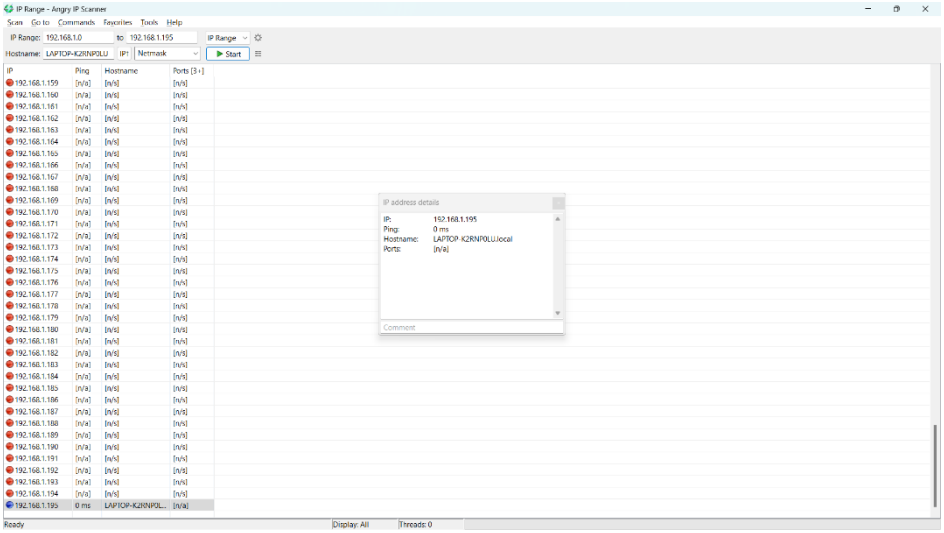
Once installed, open the application by searching for it in the Start Menu. As you can see, the home screen of the application is pretty simple and straightforward. By default, Angry IP scanner will enter your local IP address range and your computer name as the hostname.



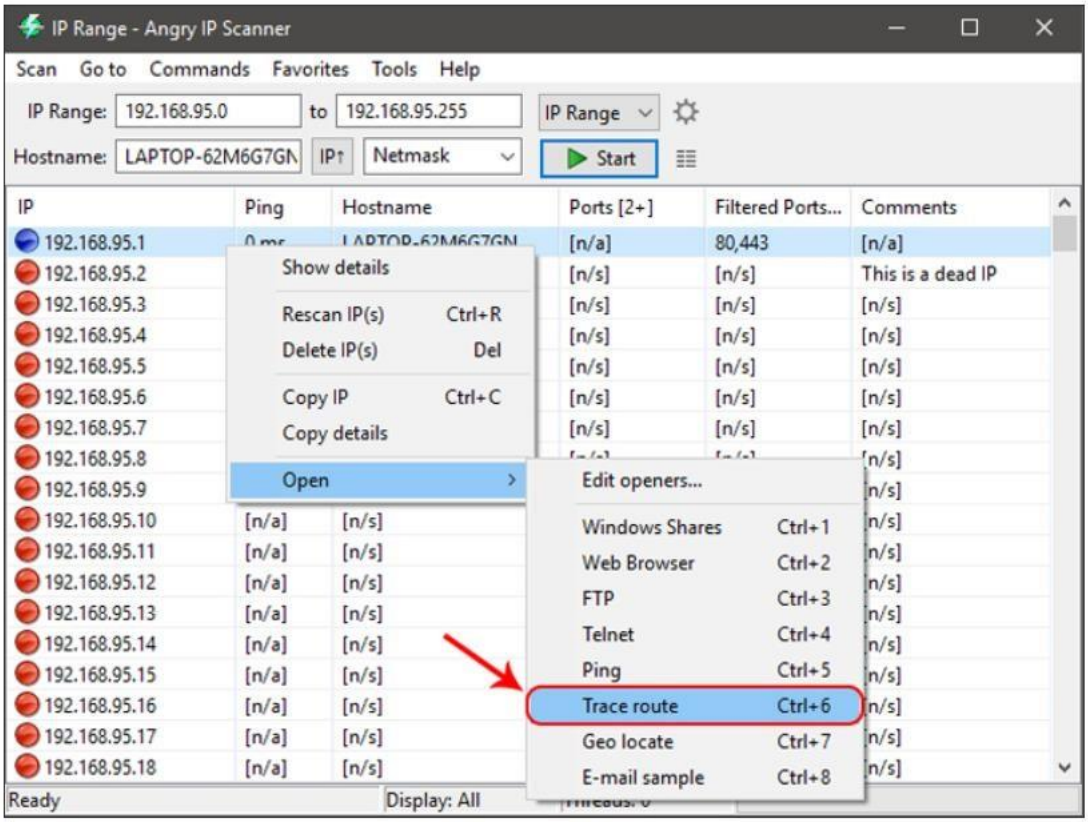
The good thing about Angry IP Scanner is that it lets you scan IP addresses in three different ways. They are, the range you specified, a random IP address or a list of IP addresses from a text file. You can easily select the scan mode from the drop-down menu next to the IP address field.

Now click start to scan you will see result of the scan.





Apart from copying the details of an IP address, you can also perform a range of different activities on the entries. You can open an IP address in the web browser, do an FTP, trace routing, etc. For instance, if you want to traceroute an IP address, simply right-click on the target IP address. After that, select the option Open and click on Traceroute.



Once you are done scanning an IP address or the IP address range, you can save the scan results. To do that, select the option Scan from the menu bar.

PRACTICAL : 2

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

A firewall is a computer network security system that restricts internet traffic in to, out of, or within a private network.

This software or dedicated hardware-software unit functions by selectively blocking or allowing data packets. It is typically intended to help prevent malicious activity and to prevent anyone—inside or outside a private network from engaging in unauthorized web activities.

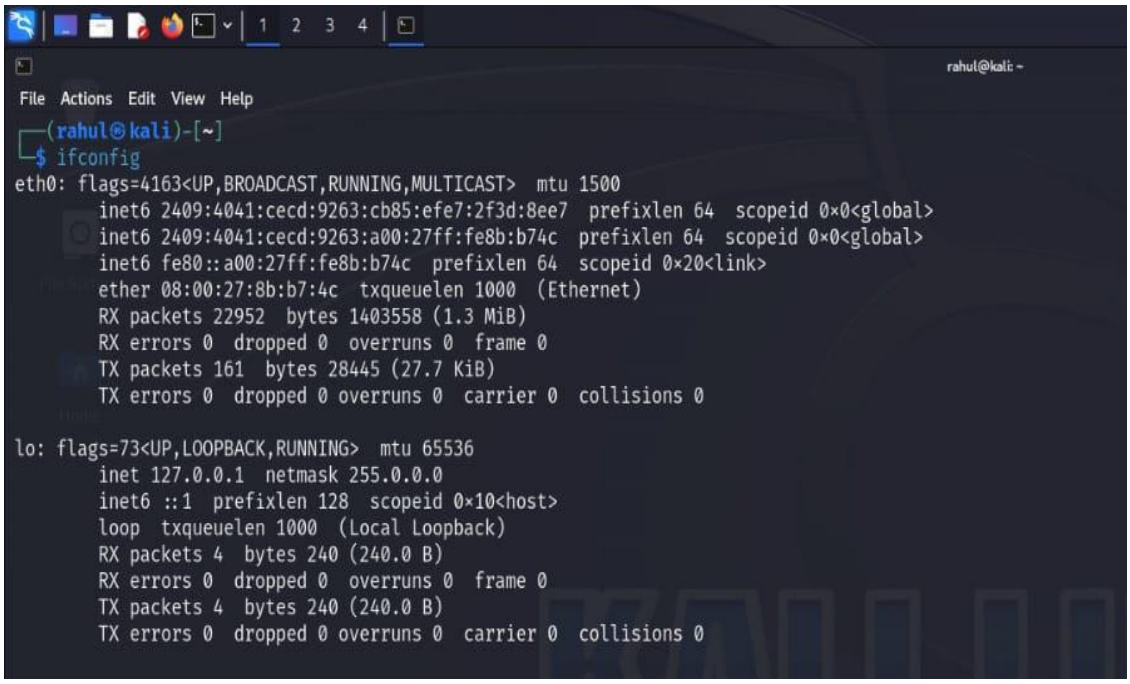
Types of firewalls:

1) Hardware firewall

2) Software firewall

Commands:

1. IFCONFIG : This command is used to find IP address of linux/kali



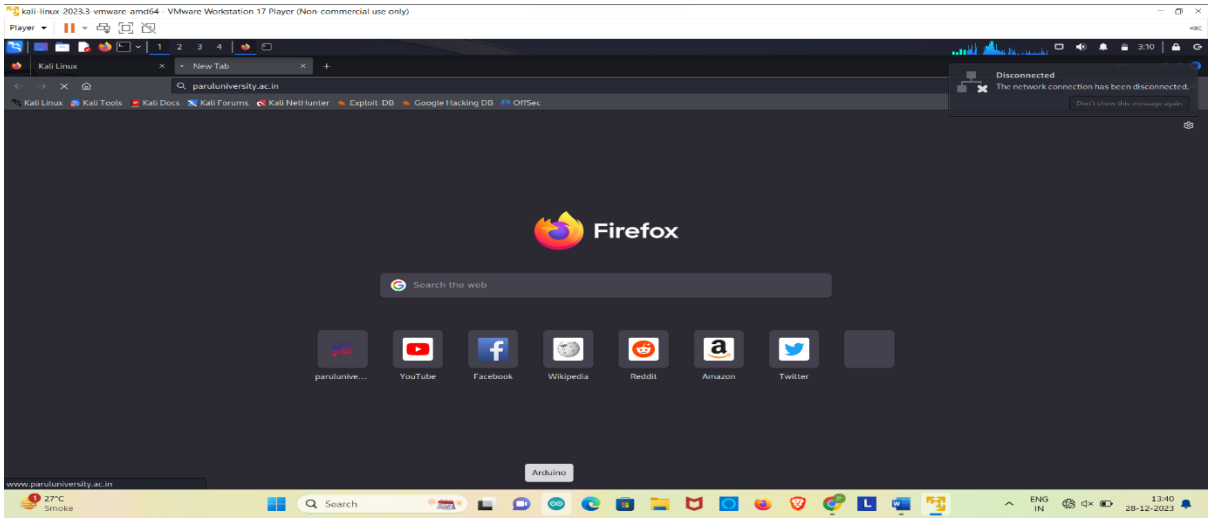
2. $sudo iptables -L : This command is used to show list of rules.

```
┌──(rahul㉿kali)-[~]
└─$ sudo iptables -L
[sudo] password for rahul:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

3. $sudo iptables -A INPUT -s paruluniversity.ac.in -j DROP:
   This command is used to drop/block the website

```
┌──(rahul㉿kali)-[~]
└─$ sudo iptables -A INPUT -s paruluniversity.ac.in -j DROP

┌──(rahul㉿kali)-[~]
```

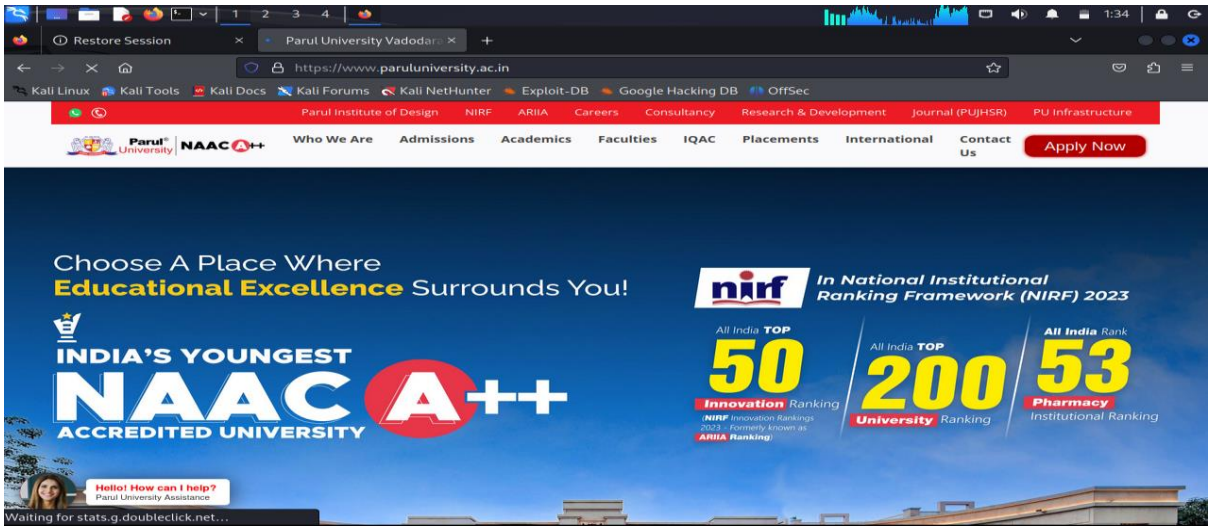
OUTPUT : Website is not accessible.



4. $sudo iptables -A INPUT -s paruluniversity.ac.in -j ACCEPT:
   This command is used to accept the website which is blocked by us.

```
┌──(rahul㉿kali)-[~]
└─$ sudo iptables -A INPUT -s paruluniversity.ac.in -j ACCEPT
```

OUTPUT : Now this site is available.



5. Sudo iptables -D INPUT 1: this command is used to delete a particular command.

```
┌──(rahul㉿kali)-[~]
└─$ sudo iptables -D INPUT 1
```

6. Sudo iptables -F : This command is used to flush all rules.

```
┌──(rahul㉿kali)-[~]
└─$ sudo iptables -F
```

```
┌──(rahul㉿kali)-[~]
└─$ sudo iptables -L
[sudo] password for rahul:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

7. sudo iptables -A INPUT -p tcp –dport 443 -j DROP &
   sudo iptables -A INPUT -p tcp –dport 443 -j ACCEPT.

   This Commands is used to drop and allow any traffic on TCP port 443.
   This command blocks all incoming HTTPS traffic to your system.

   This can be useful for security purposes, but it can also have unintended consequences.

   sudo iptables -A INPUT -p tcp –dport 443 -j ACCEPT: this command is used to accept the traffic we blocked using DROP command.

```
┌──(rahul㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 443 -j DROP
[sudo] password for rahul:

┌──(rahul㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:https

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

┌──(rahul㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

┌──(rahul㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

┌──(rahul㉿kali)-[~]
└─$
```