

Practical : 1

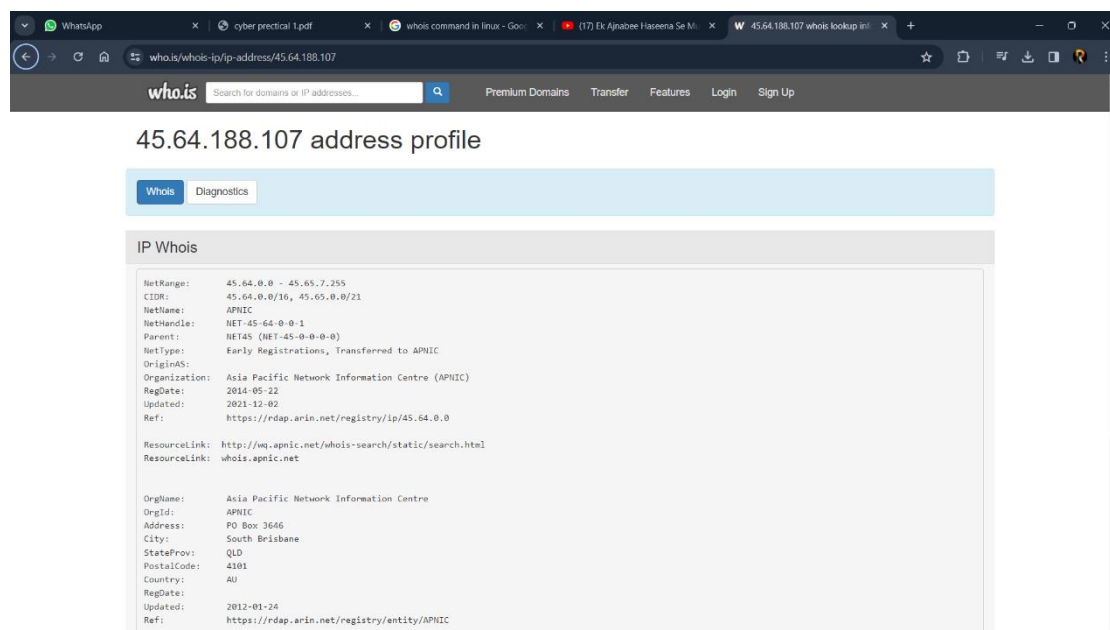
AIM : Implementation to gather information from any PC's connected to the LAN using whois, port scanner, network scanning, ANGRY IP scanners etc.

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:

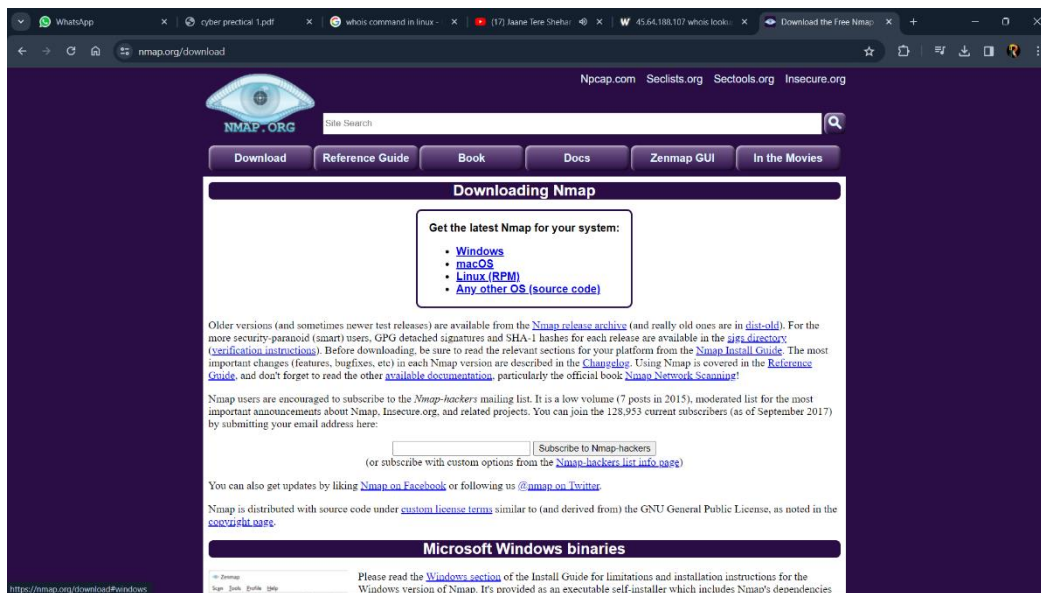
Nmap is convenient during penetration testing of networked systems. Nmap provides the network details, and also helps to determine the security flaws present in the system. Nmap is **platform independent** and runs on popular **operating systems** such as Linux, Windows and Mac.

- 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.

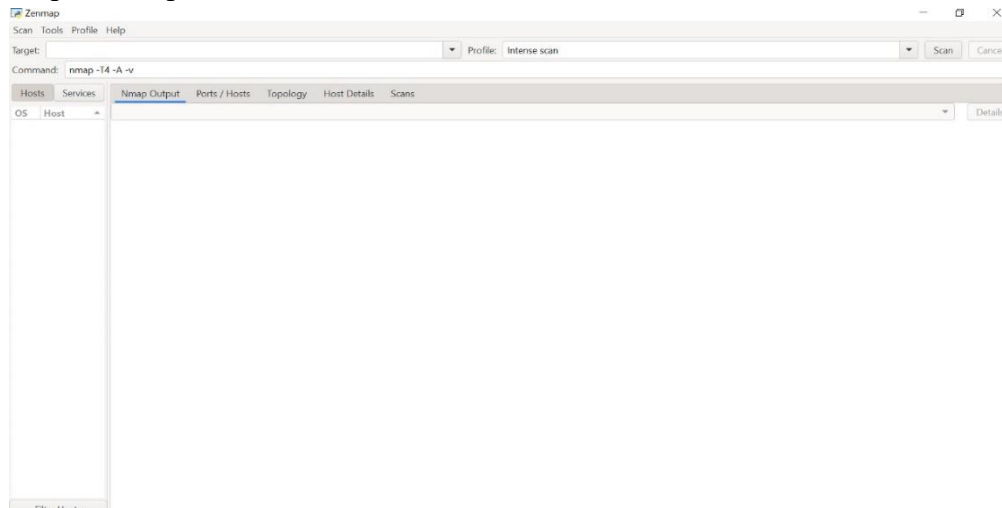
Advantages of Nmap:

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

```
Administrator: Command Prompt

Unknown adapter Local Area Connection 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

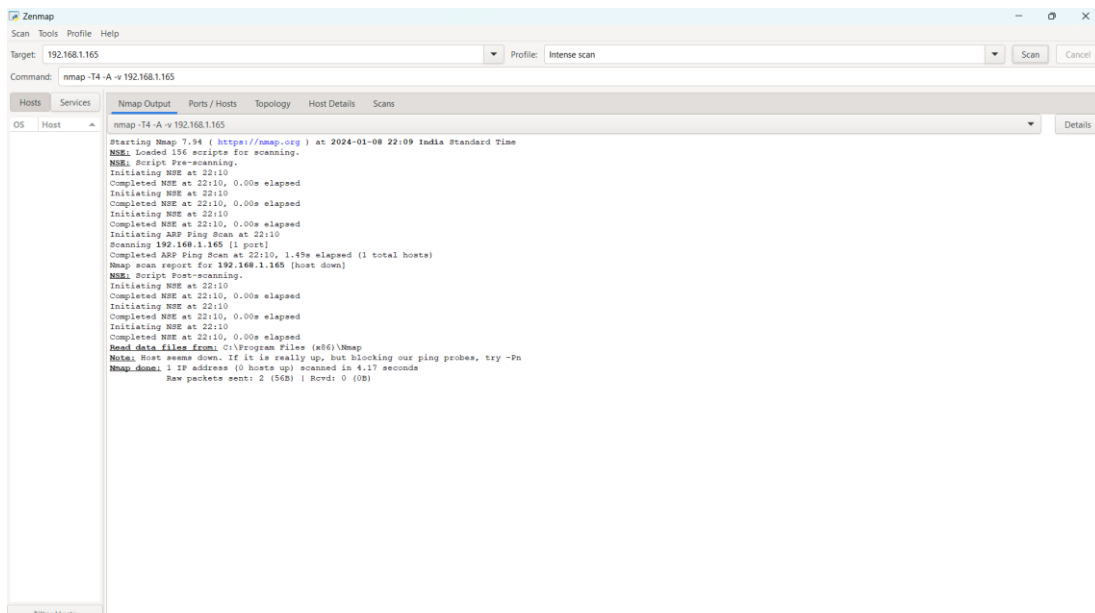
    Connection-specific DNS Suffix  . : www.tendawifi.com
    Link-local IPv6 Address . . . . . : fe80::9ea2:b3ba:355:72a6%18
    IPv4 Address. . . . . : 192.168.1.195
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.23

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Windows\System32>
```

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



```

Zenmap
Scan Tools Profile Help
Target: 192.168.1.165 Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v 192.168.1.165

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host
nmap -T4 -A -v 192.168.1.165

Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-08 22:09 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script pre-scanning.
Initiating NSE at 22:10
Completed NSE at 22:10, 0.00s elapsed
Initiating NSE at 22:10
Completed NSE at 22:10, 0.00s elapsed
Initiating NSE at 22:10
Completed NSE at 22:10, 0.00s elapsed
Initiating ARP Ping Scan at 22:10
Completed ARP Ping Scan at 22:10, 1.45s elapsed (1 total hosts)
Nmap scan report for 192.168.1.165 (host down)
NSE: Script post-scanning.
Initiating NSE at 22:10
Completed NSE at 22:10, 0.00s elapsed
Initiating NSE at 22:10
Completed NSE at 22:10, 0.00s elapsed
Initiating NSE at 22:10
Completed NSE at 22:10, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.17 seconds
Raw packets sent: 2 (568) Rcvd: 0 (0)
  
```

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

```
Administrator: Command Prompt

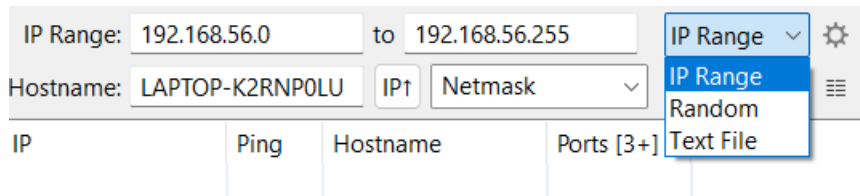
C:\Windows\System32>nmap solvetic.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-08 22:10 India Standard Time
Nmap scan report for solvetic.com (178.33.118.246)
Host is up (0.19s latency).
rDNS record for 178.33.118.246: mail.solvetic.com
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 12.39 seconds
C:\Windows\System32>
```

2. Angry IP Scanner Implementation:

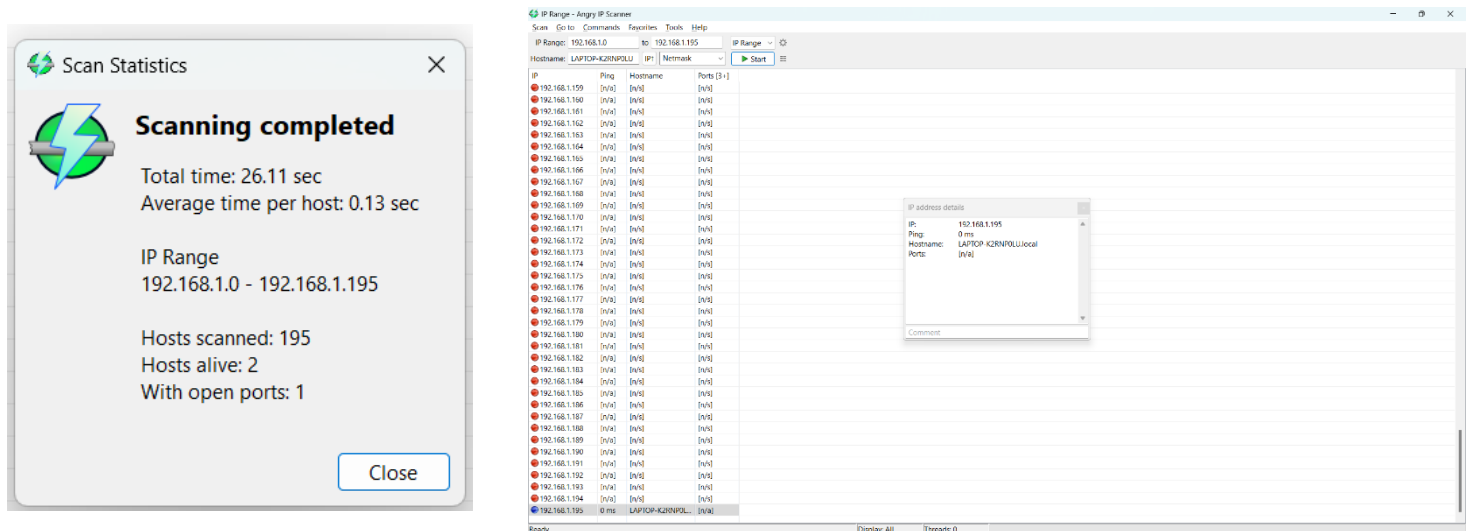


Once installed, open the application by searching for it in the Start Menu. As you can see, the home screen of the application is pretty simple and straightforward. By default, Angry IP scanner will enter your local IP address range and your computer name as the hostname.



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.



Scan Statistics

Scanning completed

Total time: 26.11 sec
Average time per host: 0.13 sec

IP Range
192.168.1.0 - 192.168.1.195

Hosts scanned: 195
Hosts alive: 2
With open ports: 1

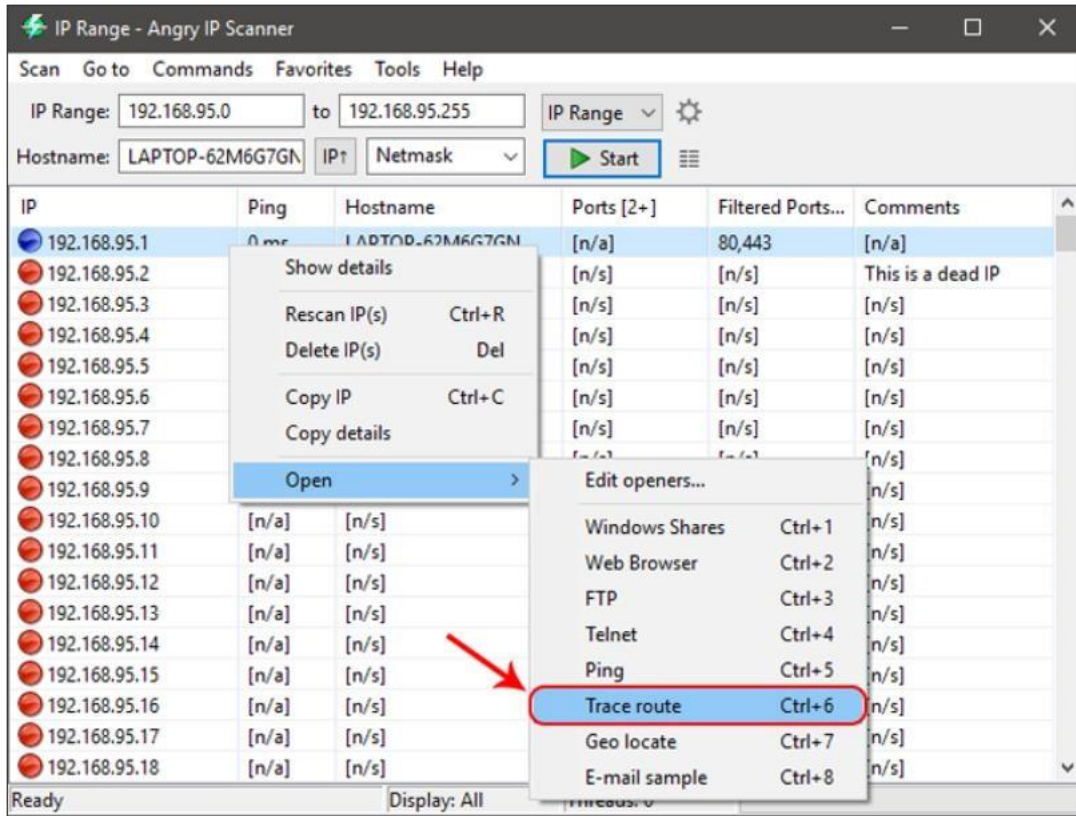
Close

IP address details

IP: 192.168.1.195
Ping: 0 ms
Hostname: LAPTOP-K2RNP0LU
Ports: [N/A]

Comment

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.

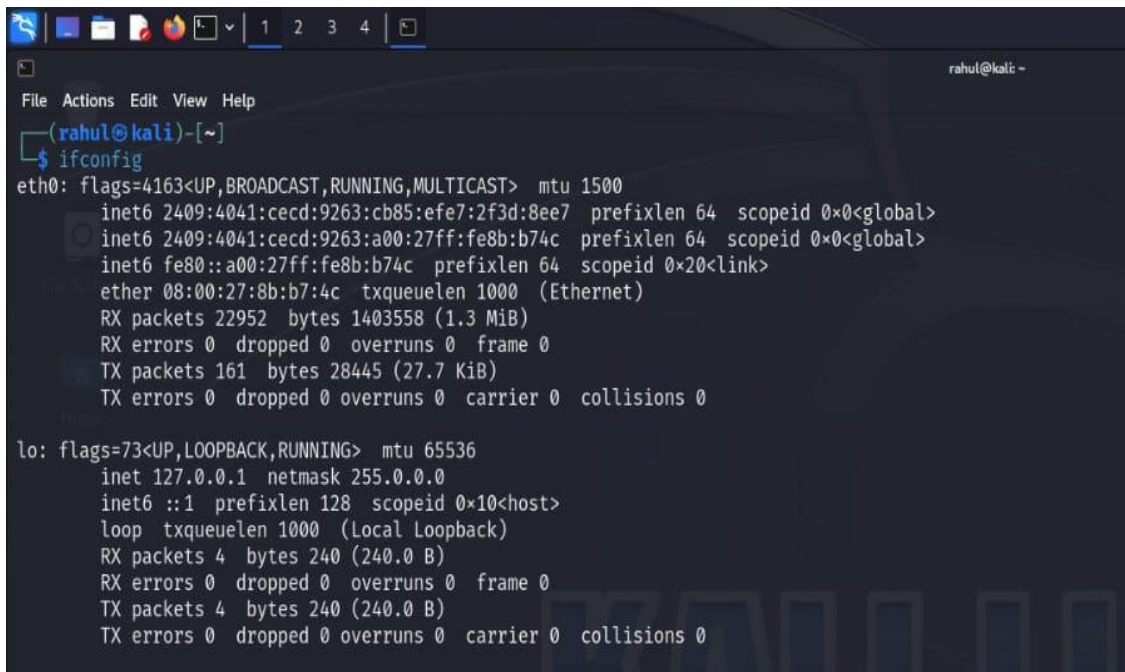
This software or dedicated hardware-software unit functions by selectively blocking or allowing data packets. It is typically intended to help prevent malicious activity and to prevent anyone—inside or outside a private network from engaging in unauthorized web activities.

Types of firewalls:

- 1) Hardware firewall
- 2) Software firewall

Commands:

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



```
File Actions Edit View Help
(rahul@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 2409:4041:cecd:9263:cb85:efe7:2f3d:8ee7 prefixlen 64 scopeid 0x0<global>
    inet6 2409:4041:cecd:9263:a00:27ff:fe8b:b74c prefixlen 64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:fe8b:b74c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8b:b7:4c txqueuelen 1000 (Ethernet)
    RX packets 22952 bytes 1403558 (1.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 161 bytes 28445 (27.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

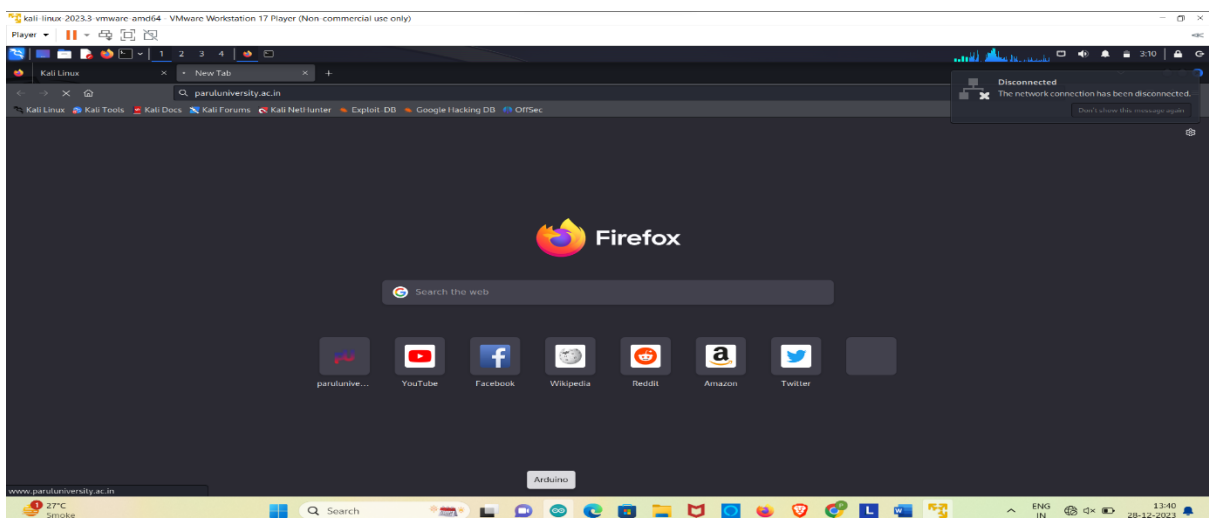
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

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.

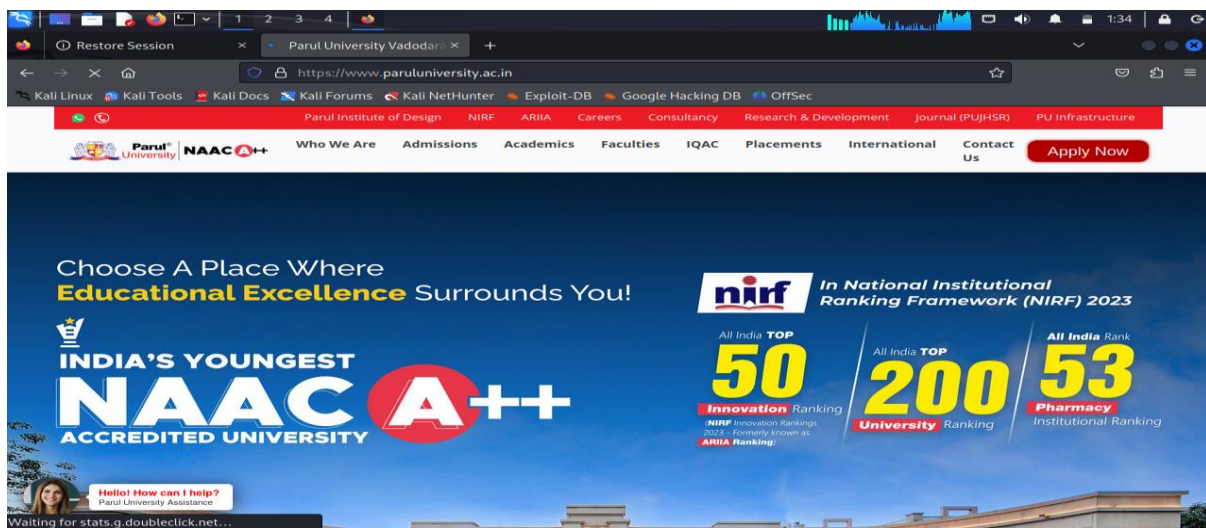


4. \$sudo iptables -A INPUT -s paruluniversity.ac.in -j ACCEPT:

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          tcp dpt:https
DROP      tcp  --  anywhere              anywhere

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          tcp dpt:https
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)-[~]
$

```