

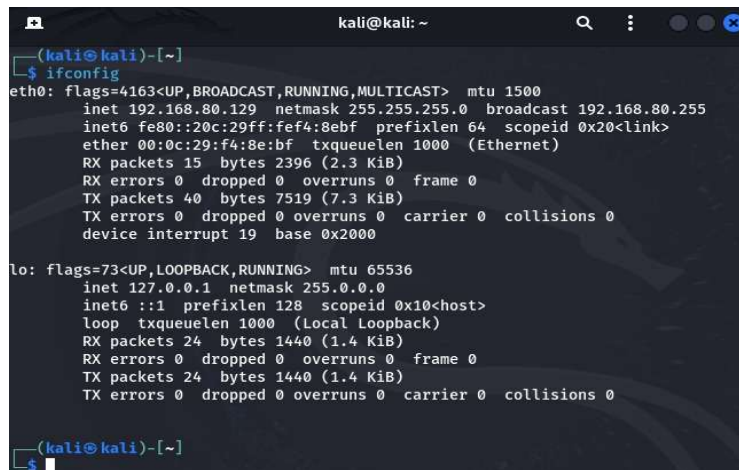
## PRACTICAL – 3

**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.



```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.80.129 netmask 255.255.255.0 broadcast 192.168.80.255
    inet6 fe80::20c:29ff:fe4:8ebf prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f4:8e:bf txqueuelen 1000 (Ethernet)
    RX packets 15 bytes 2396 (2.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 7519 (7.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

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 24 bytes 1440 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1440 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$
```

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

### Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::1ae9:d42f:b054:7ea5%
IPv4 Address. . . . . : 192.168.1.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

### Ethernet adapter Bluetooth Network Connection:

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

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

```
kali@kali: ~
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ ping 10.209.5.162
PING 10.209.5.162 (10.209.5.162) 56(84) bytes of data:
64 bytes from 10.209.5.162: icmp_seq=1 ttl=128 time=0.869 ms
64 bytes from 10.209.5.162: icmp_seq=2 ttl=128 time=1.73 ms
64 bytes from 10.209.5.162: icmp_seq=3 ttl=128 time=0.875 ms
64 bytes from 10.209.5.162: icmp_seq=4 ttl=128 time=1.82 ms
64 bytes from 10.209.5.162: icmp_seq=5 ttl=128 time=2.15 ms
64 bytes from 10.209.5.162: icmp_seq=6 ttl=128 time=1.75 ms
64 bytes from 10.209.5.162: icmp_seq=7 ttl=128 time=1.48 ms
64 bytes from 10.209.5.162: icmp_seq=8 ttl=128 time=2.08 ms
64 bytes from 10.209.5.162: icmp_seq=9 ttl=128 time=1.84 ms
64 bytes from 10.209.5.162: icmp_seq=10 ttl=128 time=2.07 ms
64 bytes from 10.209.5.162: icmp_seq=11 ttl=128 time=1.48 ms
^C
--- 10.209.5.162 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10033ms
rtt min/avg/max/mdev = 0.869/1.648/2.150/0.421 ms
(kali@kali)-[~]
$
```

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

```
root@kali: /home/kali
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# iptables -h
iptables v1.8.10 (nf_tables)

Usage: iptables -[ACD] chain rule-specification [options]
iptables -I chain [rulenum] rule-specification [options]
iptables -R chain rulenum rule-specification [options]
iptables -D chain rulenum [options]
iptables -[LS] [chain [rulenum]] [options]
iptables -[FZ] [chain] [options]
iptables -[NX] chain
iptables -E old-chain-name new-chain-name
iptables -P chain target [options]
iptables -h (print this help information)

Commands:
Either long or short options are allowed.
--append -A chain          Append to chain
--check -C chain          Check for the existence of a rule
--delete -D chain         Delete matching rule from chain
--delete -D chain rulenum Delete rule rulenum (1 = first) from chain
--insert -I chain [rulenum] Insert in chain as rulenum (default 1=first)
--replace -R chain rulenum Replace rule rulenum (1 = first) in chain
--list -L [chain [rulenum]] List the rules in a chain or all chains
--list-rules -S [chain [rulenum]] Print the rules in a chain or all chains
--flush -F [chain]        Delete all rules in chain or all chains
--zero -Z [chain [rulenum]] Zero counters in chain or all chains
--new -N chain           Create a new user-defined chain
--delete-chain -X [chain] Delete a user-defined chain
--policy -P chain target Change policy on chain to target
--rename-chain
```

```
root@kali: /home/kali
Commands:
Either long or short options are allowed.
--append -A chain          Append to chain
--check -C chain          Check for the existence of a rule
--delete -D chain         Delete matching rule from chain
--delete -D chain rulenum Delete rule rulenum (1 = first) from chain
--insert -I chain [rulenum] Insert in chain as rulenum (default 1=first)
--replace -R chain rulenum Replace rule rulenum (1 = first) in chain
--list -L [chain [rulenum]] List the rules in a chain or all chains
--list-rules -S [chain [rulenum]] Print the rules in a chain or all chains
--flush -F [chain]        Delete all rules in chain or all chains
--zero -Z [chain [rulenum]] Zero counters in chain or all chains
--new -N chain           Create a new user-defined chain
--delete-chain -X [chain] Delete a user-defined chain
--policy -P chain target Change policy on chain to target
--rename-chain
```

Step 5: Enter the command iptables -L.

```
root@kali: /home/kali
--table -t table      table to manipulate (default: 'filter')
--verbose -v          verbose mode
--wait -w [seconds]  maximum wait to acquire xtables lock before give
up
--line-numbers        print line numbers when listing
--exact -x            expand numbers (display exact values)
--fragment -f         match second or further fragments only
--modprobe=<command>  try to insert modules using this command
--set-counters -c PKTS BYTES set the counter during insert/append
--version -V          print package version.

(root@kali)-[/home/kali]
# iptables -L
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

(root@kali)-[/home/kali]
#
```

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.

```
root@kali: /home/kali
target     prot opt source                destination

(root@kali)-[/home/kali]
# iptables -A
iptables v1.8.10 (nf_tables): option "-A" requires an argument
Try 'iptables -h' or 'iptables --help' for more information.

(root@kali)-[/home/kali]
# iptables -A INPUT -s 10.209.5.162 -j DROP

(root@kali)-[/home/kali]
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      all  --  10.209.5.162          anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

(root@kali)-[/home/kali]
#
```

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.

```
root@kali: /home/kali
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@kali: /home/kali
# iptables -A OUTPUT -s 192.168.80.129 -j DROP
root@kali: /home/kali
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      all  --  10.209.5.162          anywhere
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
DROP      all  --  kali                  anywhere
root@kali: /home/kali
#
```

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

```
root@kali: /home/kali
# iptables -A INPUT -s 10.209.5.162 -j ACCEPT
root@kali: /home/kali
# iptables -A OUTPUT -s 192.168.80.129 -j ACCEPT
root@kali: /home/kali
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      all  --  10.209.5.162          anywhere
ACCEPT    all  --  10.209.5.162          anywhere
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
DROP      all  --  kali                  anywhere
ACCEPT    all  --  kali                  anywhere
root@kali: /home/kali
#
```

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

```
root@kali: /home/kali
DROP    all -- kali anywhere
ACCEPT  all -- kali anywhere

root@kali: /home/kali
# iptables -D INPUT 1

root@kali: /home/kali
# iptables -D OUTPUT 1

root@kali: /home/kali
# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 10.209.5.162 anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- kali anywhere

root@kali: /home/kali
#
```

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

```
root@kali: /home/kali
ACCEPT tcp -- kali anywhere tcp dpt:https

root@kali: /home/kali
# sudo iptables -A OUTPUT -p tcp -o etho -s 192.168.80.129 --dport 443 -j DROP

root@kali: /home/kali
# iptables -D OUTPUT 1

root@kali: /home/kali
# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 10.209.5.162 anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
DROP tcp -- kali anywhere tcp dpt:https

root@kali: /home/kali
#
```

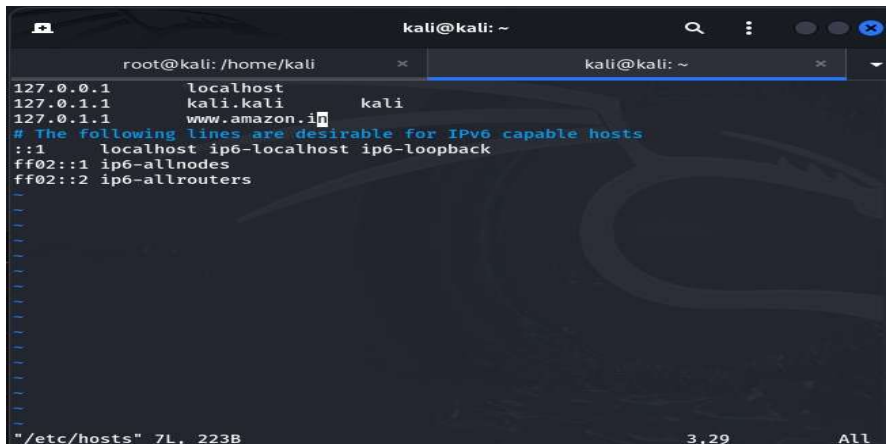
### To block the website in kali linux:

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

```
kali@kali: ~
root@kali: /home/kali
(kali@kali)~
$ firefox
(kali@kali)~
$ sudo vi /etc/hosts
sudo: password for kali:
(kali@kali)~
$ firefox
```



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



```
root@kali: /home/kali
127.0.0.1    localhost
127.0.1.1    kali.kali    kali
127.0.1.1    www.amazon.in
# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

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

