

Experiment 5: Implement a firewall for an organization.

```
(kali㉿kali)-[~]
$ sudo service apache2 start
[sudo] password for kali:
```

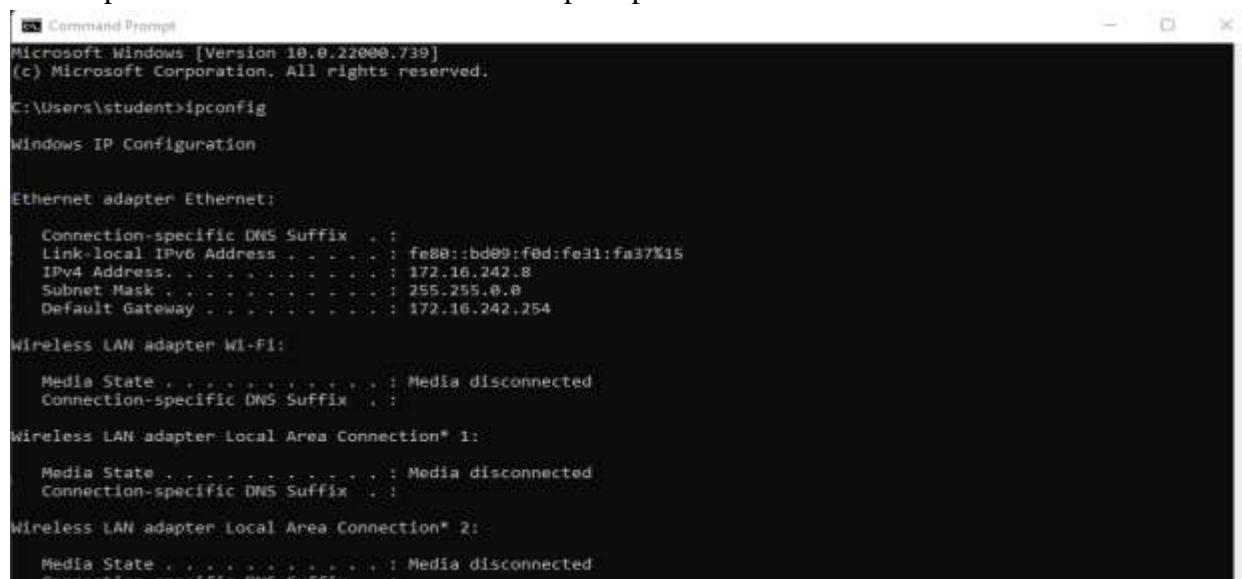
```
(kali㉿kali)-[~]
$ sudo service mysql start
```

Check ip address in kali

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.23.128 netmask 255.255.255.0 broadcast 192.168.23.255
          inet6 fe80::20c:29ff:fe0b:96d0 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:0b:96:d0 txqueuelen 1000 (Ethernet)
              RX packets 109 bytes 39332 (38.4 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 133 bytes 24038 (23.4 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 171 bytes 37444 (36.5 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 171 bytes 37444 (36.5 KiB)
```

Check ip address for windows in command prompt



A screenshot of a Windows Command Prompt window titled "Command Prompt". The window shows the output of the "ipconfig" command. The output includes information for several network adapters, including "Ethernet adapter Ethernet", "Wireless LAN adapter Wi-Fi", and "Wireless LAN adapter Local Area Connection* 1" and "Wireless LAN adapter Local Area Connection* 2". For each adapter, it displays connection-specific DNS suffixes, link-local IPv6 addresses, IPv4 addresses, subnet masks, and default gateways. In this case, the "Media State" for all adapters is listed as "Media disconnected".

```
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . : fe80::bd09:fed:fe31:fa37%15
  IPv4 Address . . . . . : 172.16.242.8
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 172.16.242.254

Wireless LAN adapter Wi-Fi:

  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 . :
```

Connect windows and kali using command prompt in windows

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

To block pinging of windows system use the following command(should consider only IP

```
(kali㉿kali)-[~]
$ sudo iptables -A INPUT -s 192.168.23.1 -j DROP
```

address not ethernet's address)

Now check whether ping requests are allowed in windows

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

This way we can block ping packets.

To unblock the ping packets use the commands

```
(kali㉿kali)-[~]
$ sudo iptables -D INPUT -s 192.168.23.1 -j DROP
```

Let's check its unblocking the ping packets in the windows command prompt

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -s 192.168.23.1 -p tcp --destination-port 80 -j DROP
```

Task 2: Block the port numbers

Open browser in windows and search for its ip address in the address of kali linux bar – it opens the web page.



This site can't be reached

192.168.23.128 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

[Reload](#)

We need to block the availability of port 80.

Instead of -A use -D

```
(kali㉿kali)-[~]
$ sudo iptables -D INPUT -s 192.168.23.1 -p tcp --destination-port 80 -j DROP
```

Now check the ip address of the kali linux in windows



Result:

Thus the implement a firewall for an organization completed sucessfully.

