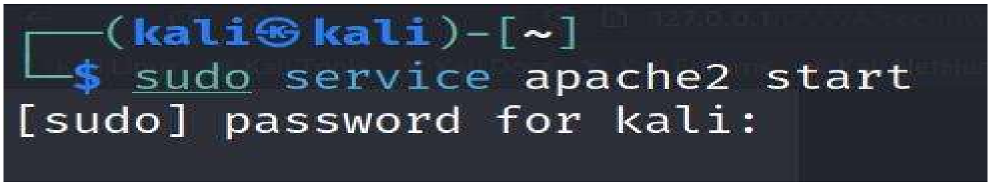
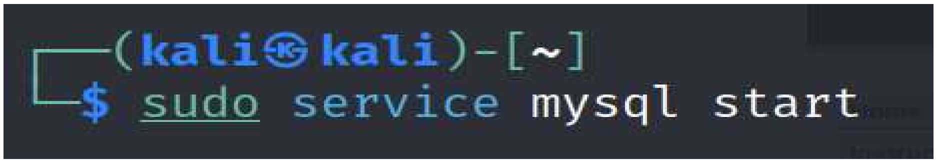
Experiment 5: Implement a firewall for an organization.

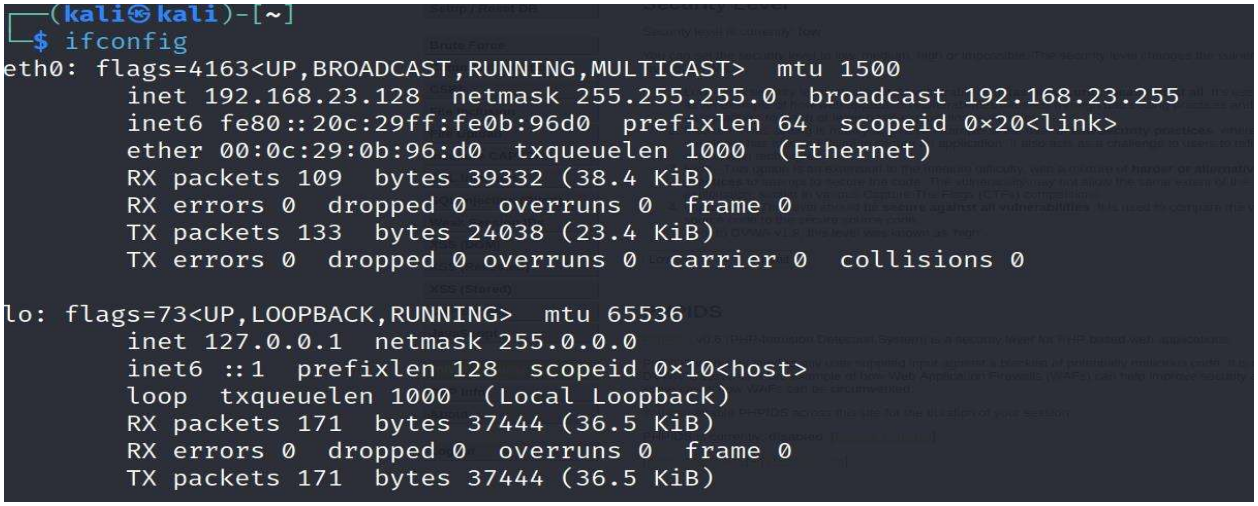


```
┌──(kali㉿kali)-[~]
└─$ sudo service apache2 start
[sudo] password for kali:
```



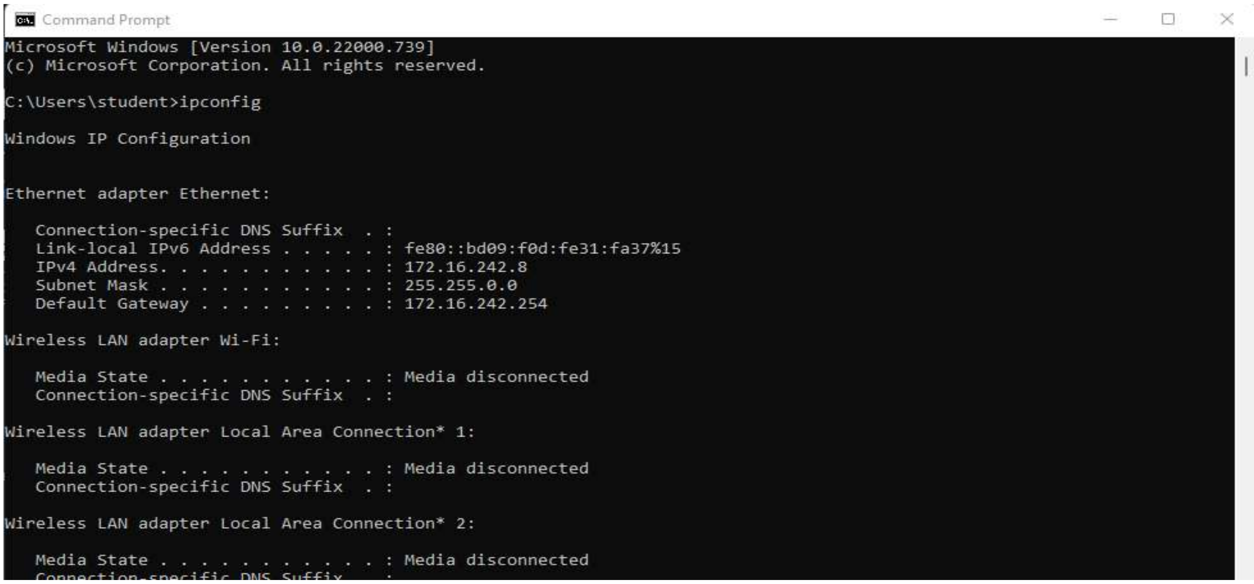
```
┌──(kali㉿kali)-[~]
└─$ sudo service mysql start
```

Check ip address in kali



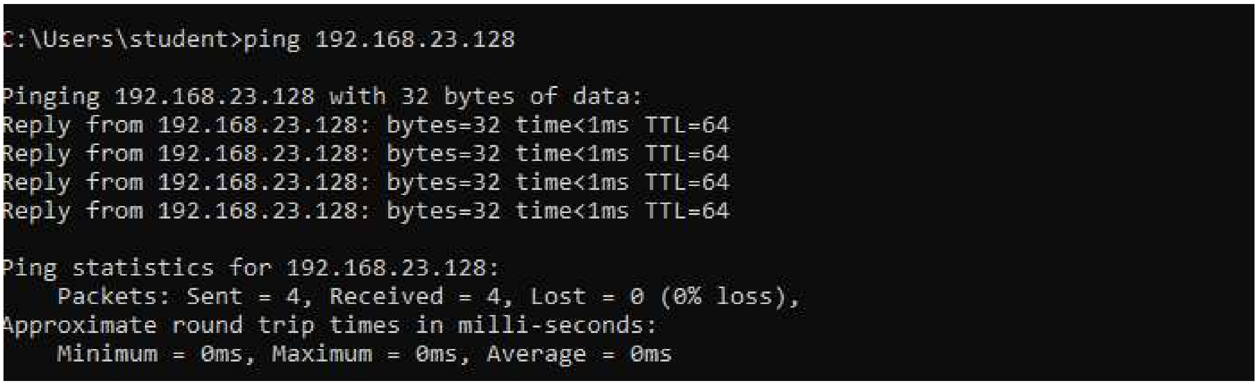
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.23.128  netmask 255.255.255.0  broadcast 192.168.23.255
        inet6 fe80::20c:29ff:fe0b:96d0  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:0b:96:d0  txqueuelen 1000  (Ethernet)
        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 0×10<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



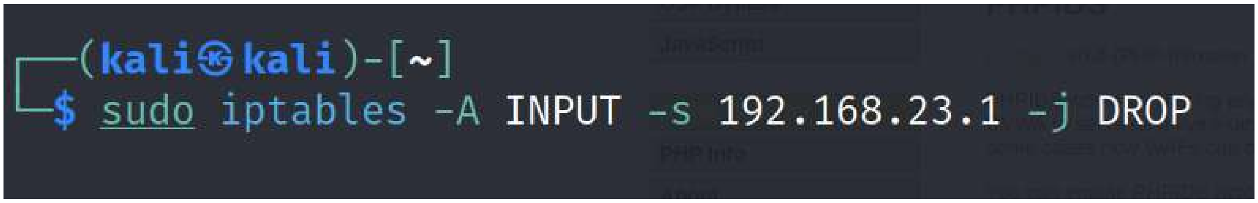
```
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bd09:f0d: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



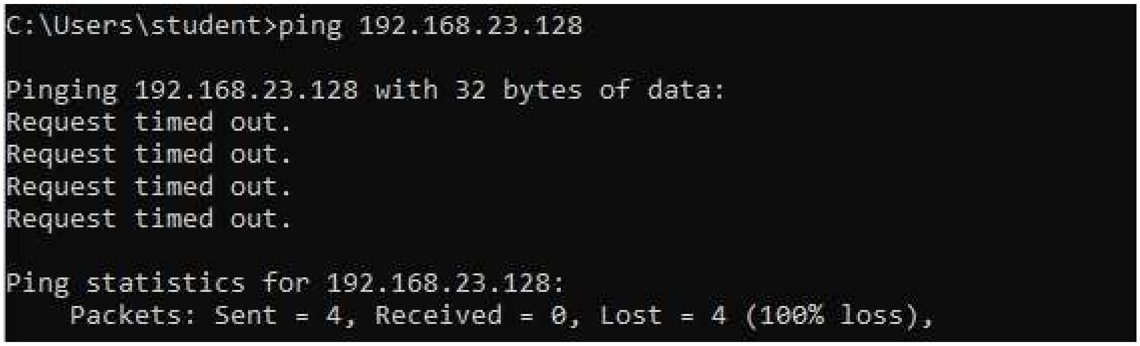
```
:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
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 address not ethernet’s address)



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

Now check whether ping requests are allowed in windows

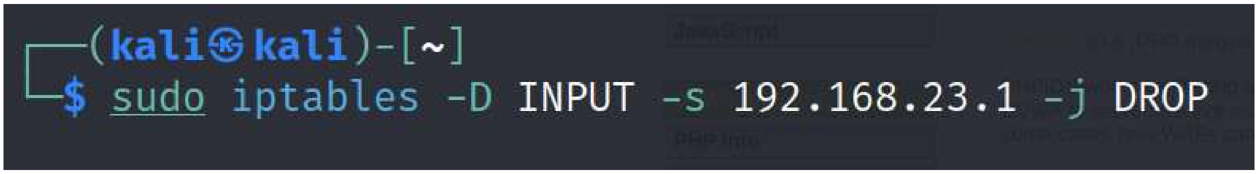


```
C:\Users\student>ping 192.168.23.128

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.

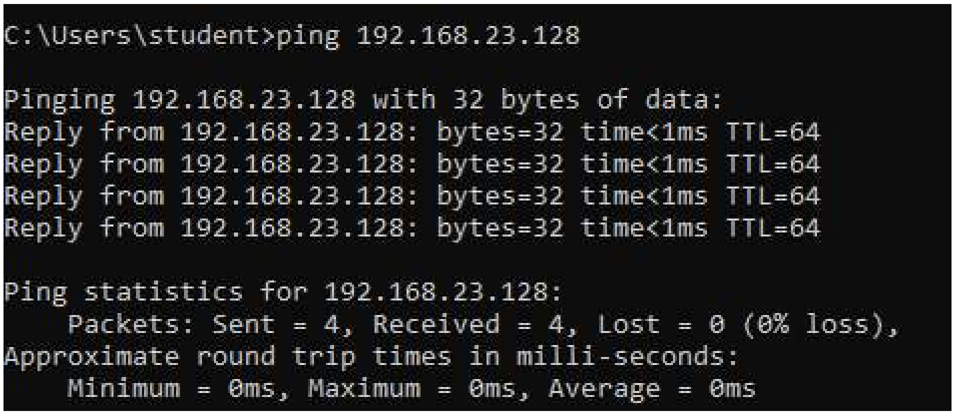
—--

To unblock the ping packets use the commands



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

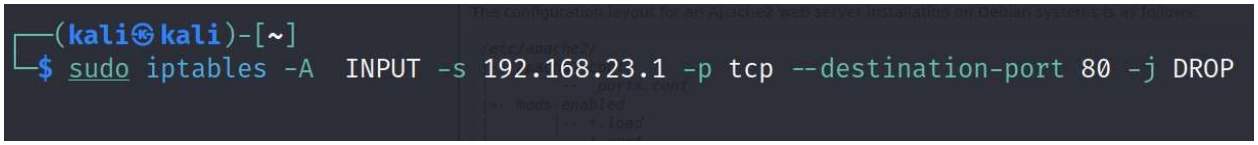
Let’s check its unblocking the ping packets in the windows command prompt



```
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
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
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
```

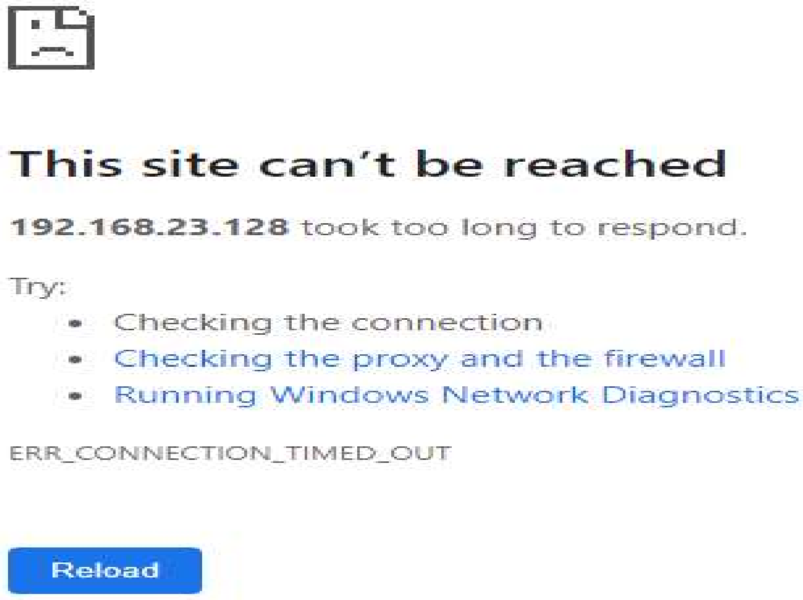
—---

Task 2: Block the port numbers



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

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.

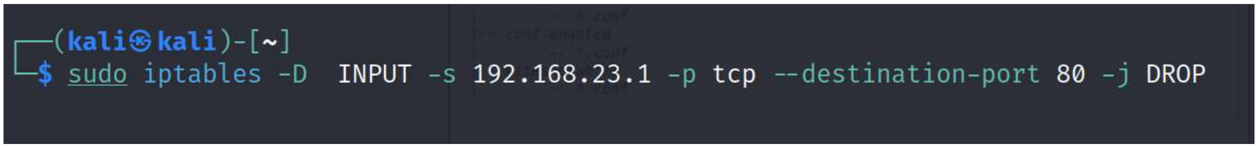
Try:

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

ERR_CONNECTION_TIMED_OUT

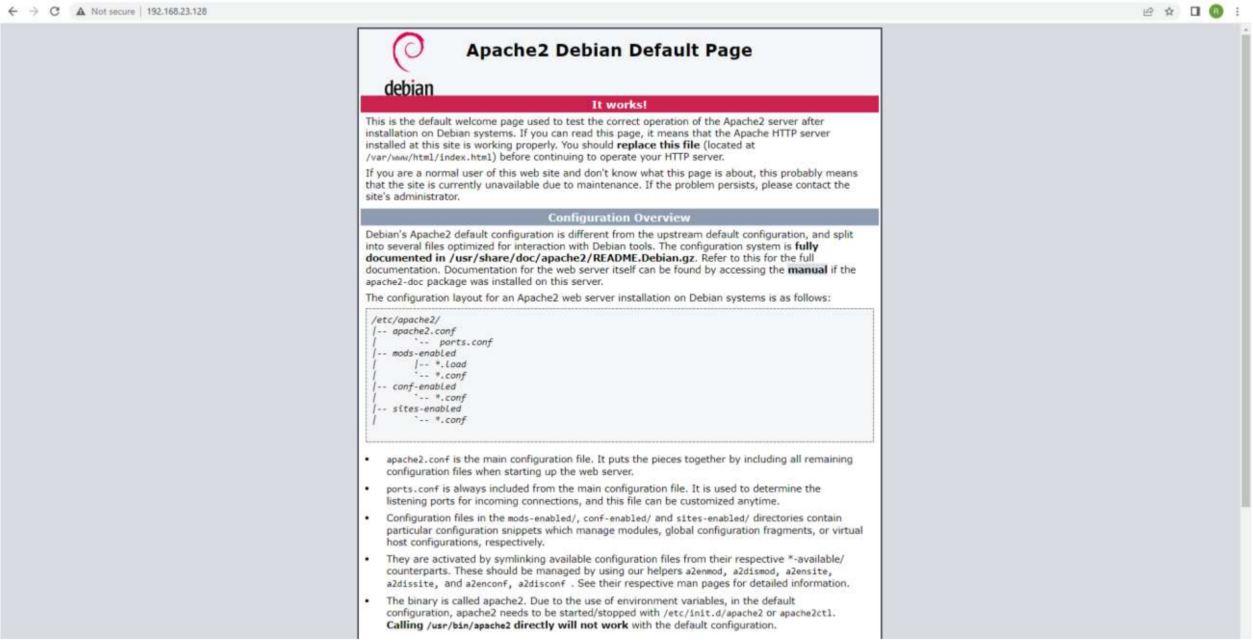
We need to block the availability of port 80.

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



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf` . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.