Experiment-5

Implement Firewall for an Organization

AIM

Implement a firewall for an organization.

PROCEDURE

Step-1: Login to Kali Linux, open terminal and find the IP address.

Step-2: In Windows open Command Prompt and find the IP address.

Step-3: First block the IP packets using Kali Linux. Check whether IP packets are blocked using ping command in Windows Operating System.

Step-4: Unblock the IP packets. Check whether IP packets are unblocked using ping command in Windows Operating System.

Step-5: Block the port number. To check port is blocked, open any browser in windows operating system and run the IP address of Kali Linux.

Step-6: Unblock the port number. To check port is unblocked, by open any browser in windows OS and run the IP address of Kali Linux.

SOURCECODE

```
$ open vmware . click on open virtual machine.
Enter username and password as kali.
Go to terminal
$ if config
Note down the inet address : 192.168.164.138
$ sudo service apache2 start
```

Password for Kali : Kali
$sudo Sewice mysql start
check ip address for windows in command prompt
Go to Command prompt
ipConfig
Note the ipaddress which is there in vmnet 8 ip
address   vmnet 8 : 192.168.164.1 (ip address of
windows)
Connect windows and Kali by
> ping 192.168.164.138
There we can get the output like we can observe the
replies from linux.
→ In vmware terminal type the command to block
$ sudo iptables -A INPUT -S 192.168.164.138 -j DROP

→ Go to Command prompt
> ping   192.168.164.138
Pinging 192.168.164.138 with 32 bytes of data :
Request timed out
Request timed out
Request timed out
→ In vmware terminal type command to unblock.
$ sudo iptable -D INPUT -S 192.168.164.1 -j
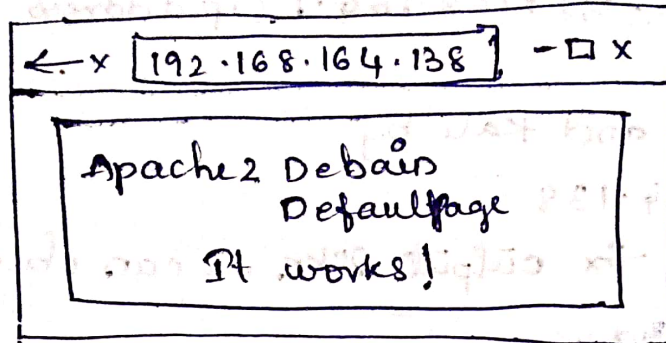DROP.
→ Go to Command prompt
> ping 192.168.164.138.

Pinging 192.168.164.138 with 82 bytes of data:

Reply from 192.168.164.138: bytes =32 time <1ms TTL=64

Reply from 192.168.164.138: bytes =32 time < 1ms TTL=64

⇒Go to browser and type in tab 192.168.164.138 which the ip address of linine.

```
←—x [192.168.164.138]  -□x


     Apache2 Debain
           Defaulpage
        It works!
```

⇒In vmware Type Command

[$ sudo iptables -A INPUT -s 192.168.164.1 -p tcp -destination -port 80 j DROP]

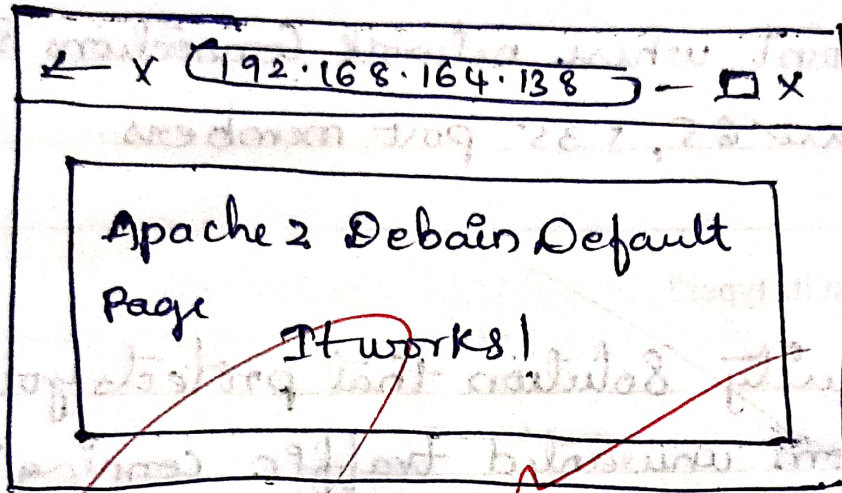⇒Go to browser and again type the same IP address you typed before then you can see the output like below.

```
←—x (192.168.164.138)  -□x

    [•_4]


This sit Can't be reached
    192.168.164.138.
```
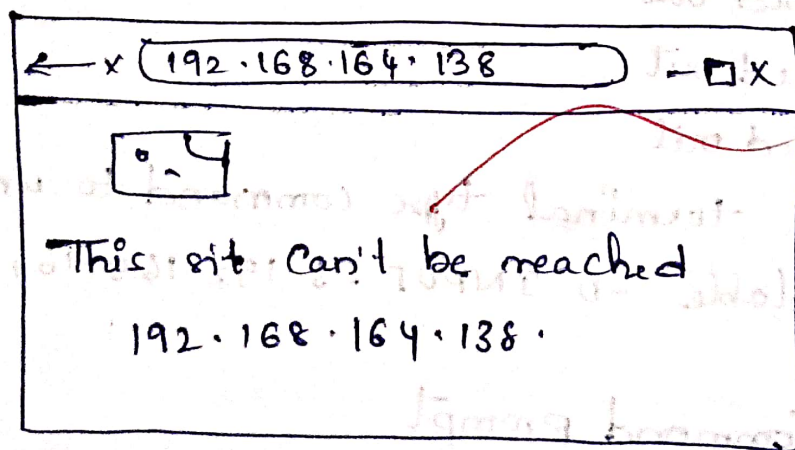
OUTPUT

→ In vmware type command

\$ Sudo iptables —D INPUT —S 192.168.164.1 —p tcp
—destination —port —j DROP

⇒ Again type the IP address in browser tab.

```
←  X  ⟨ 192.168.164.138 ⟩  —  □ X

Apache 2 Debain Default
Page
        It works!
```