

Linux Firewall Exploration Lab

Name:Nikhil T M
SRN:PES1UG20CS821
Section:F

Lab Setup

Vm1	10.0.2.8
Vm2	10.0.2.9
Vm3	10.0.2.14

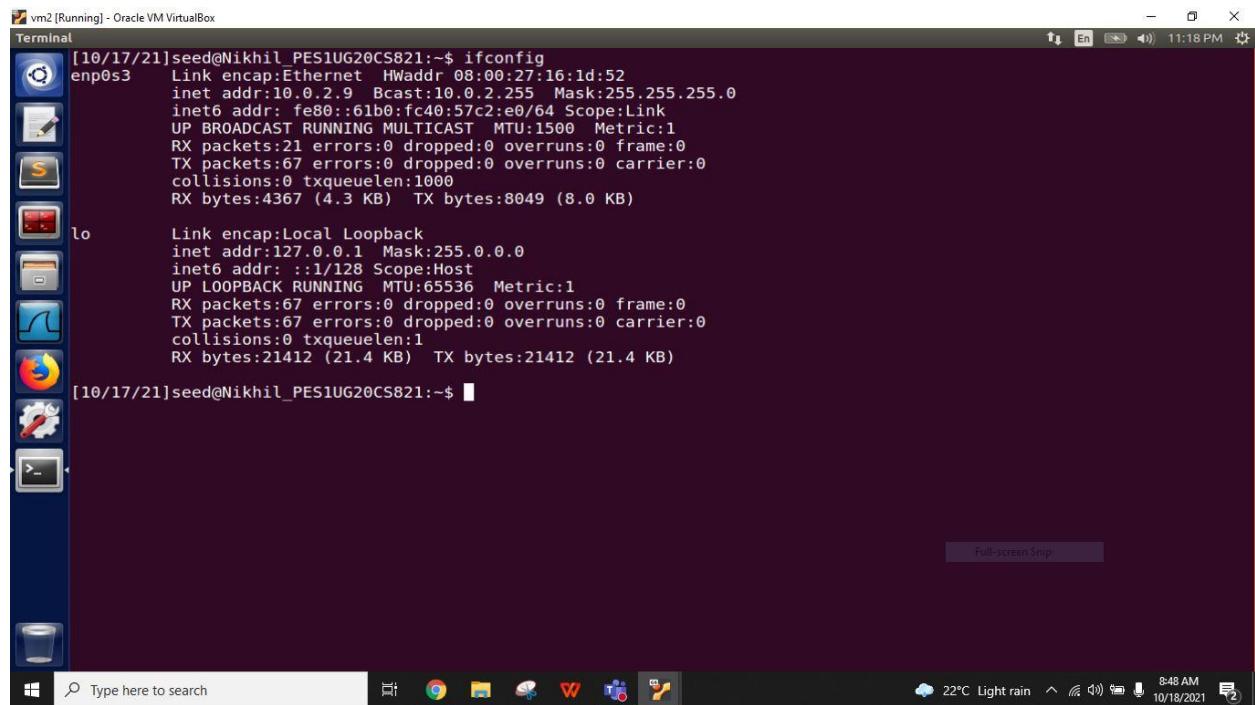
Vm1

```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:ab:41:94
             inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
                     inet6 addr: fe80::1441:2a5e:5579:48c2/64 Scope:Link
                         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                         RX packets:61 errors:0 dropped:0 overruns:0 frame:0
                         TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
                         collisions:0 txqueuelen:1000
                         RX bytes:9702 (9.7 KB)  TX bytes:8180 (8.1 KB)

lo          Link encap:Local Loopback
             inet addr:127.0.0.1  Mask:255.0.0.0
                     inet6 addr: ::1/128 Scope:Host
                         UP LOOPBACK RUNNING  MTU:65536  Metric:1
                         RX packets:70 errors:0 dropped:0 overruns:0 frame:0
                         TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
                         collisions:0 txqueuelen:1
                         RX bytes:21553 (21.5 KB)  TX bytes:21553 (21.5 KB)

[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

Vm2



vm2 [Running] - Oracle VM VirtualBox

Terminal

```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:16:1d:52
            inet addr:10.0.2.9  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::61b0:fc40:57c2:0/64 Scope:Link
                    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                    RX packets:21 errors:0 dropped:0 overruns:0 frame:0
                    TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
                    collisions:0 txqueuelen:1000
                    RX bytes:4367 (4.3 KB)  TX bytes:8049 (8.0 KB)

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
                    UP LOOPBACK RUNNING MTU:65536 Metric:1
                    RX packets:67 errors:0 dropped:0 overruns:0 frame:0
                    TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
                    collisions:0 txqueuelen:1
                    RX bytes:21412 (21.4 KB)  TX bytes:21412 (21.4 KB)

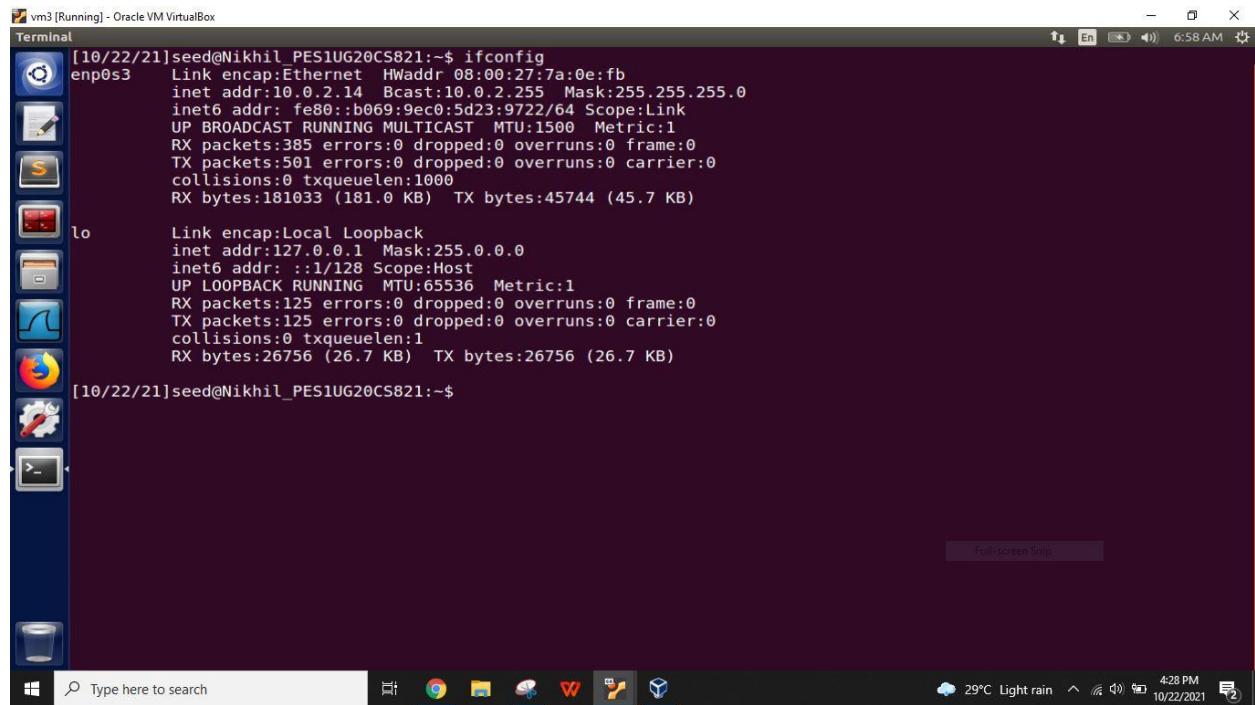
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ █
```

Full-screen Snip

Type here to search

22°C Light rain 8:48 AM 10/18/2021

Vm3



vm3 [Running] - Oracle VM VirtualBox

Terminal

```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:7a:0e:fb
            inet addr:10.0.2.14  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: b069:9ec0:5d23:9722/64 Scope:Link
                    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                    RX packets:385 errors:0 dropped:0 overruns:0 frame:0
                    TX packets:501 errors:0 dropped:0 overruns:0 carrier:0
                    collisions:0 txqueuelen:1000
                    RX bytes:181033 (181.0 KB)  TX bytes:45744 (45.7 KB)

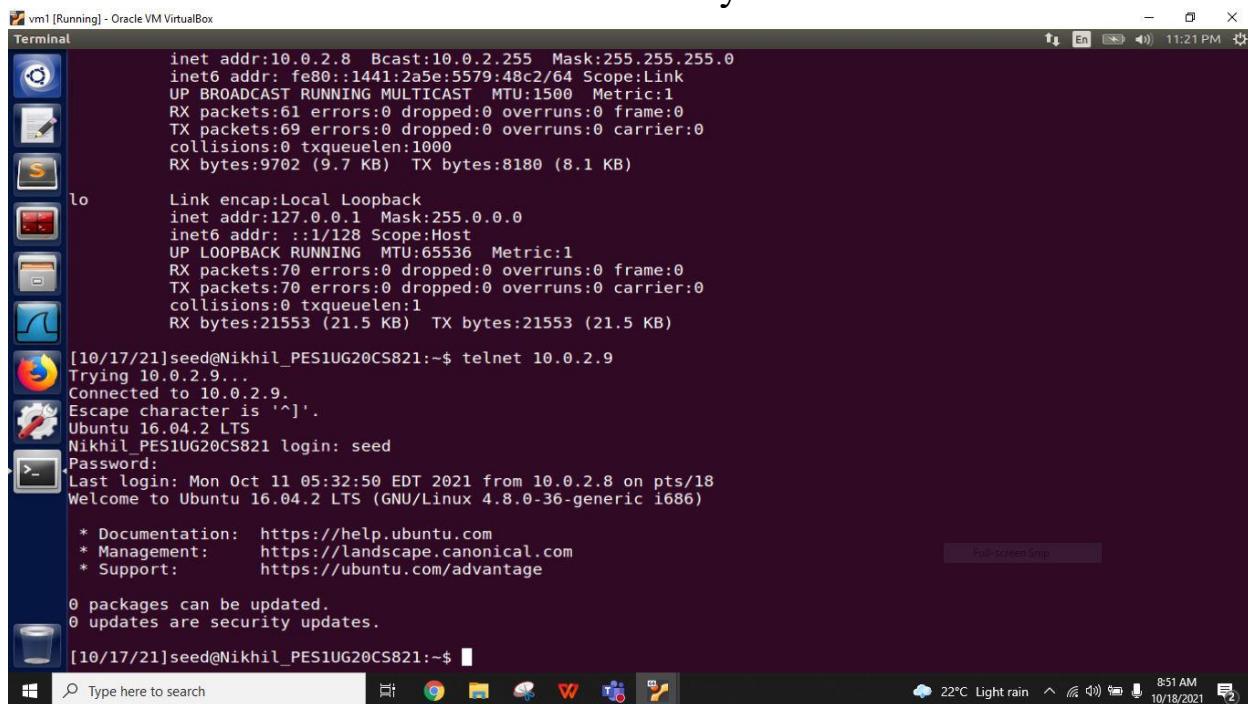
lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
                    UP LOOPBACK RUNNING MTU:65536 Metric:1
                    RX packets:125 errors:0 dropped:0 overruns:0 frame:0
                    TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
                    collisions:0 txqueuelen:1
                    RX bytes:26756 (26.7 KB)  TX bytes:26756 (26.7 KB)

[10/22/21]seed@Nikhil_PES1UG20CS821:~$ █
```

29°C Light rain 4:28 PM 10/22/2021

Task 1: Using Firewall

first we check whether we able to connect to vm2 from vm1 using telnet. We can see that we connected successfully.



```
inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::1441:2a5e:5579:48c2/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
  RX packets:61 errors:0 dropped:0 overruns:0 frame:0
  TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:9702 (9.7 KB)  TX bytes:8180 (8.1 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21553 (21.5 KB)  TX bytes:21553 (21.5 KB)

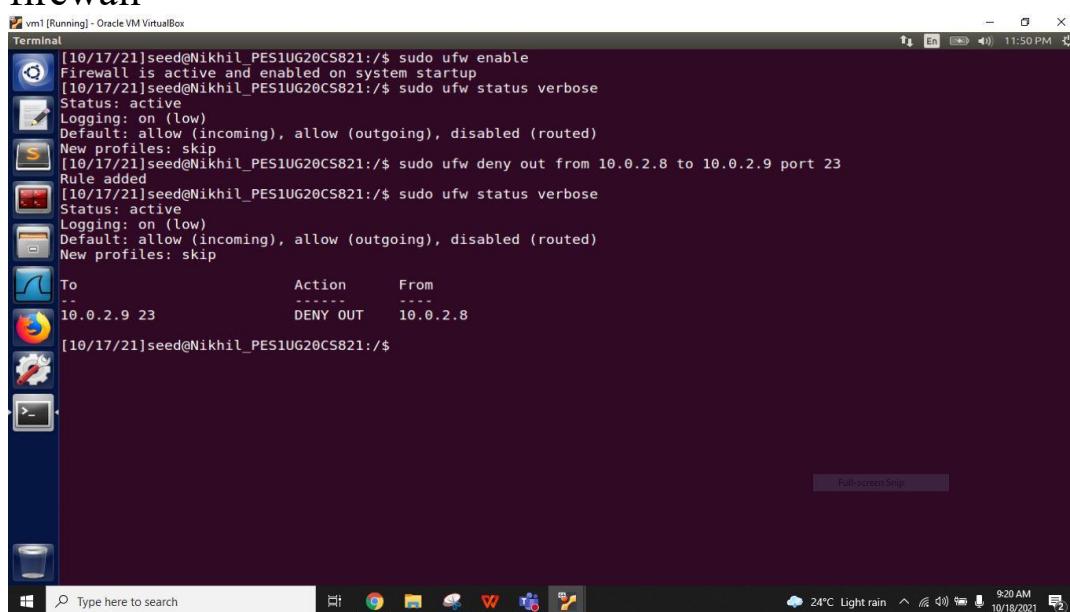
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.9
Trying 10.0.2.9...
Connected to 10.0.2.9.
Escape character is '^>'.
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Mon Oct 11 05:32:50 EDT 2021 from 10.0.2.8 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation: https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:      https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

[10/17/21]seed@Nikhil_PES1UG20CS821:~$
```

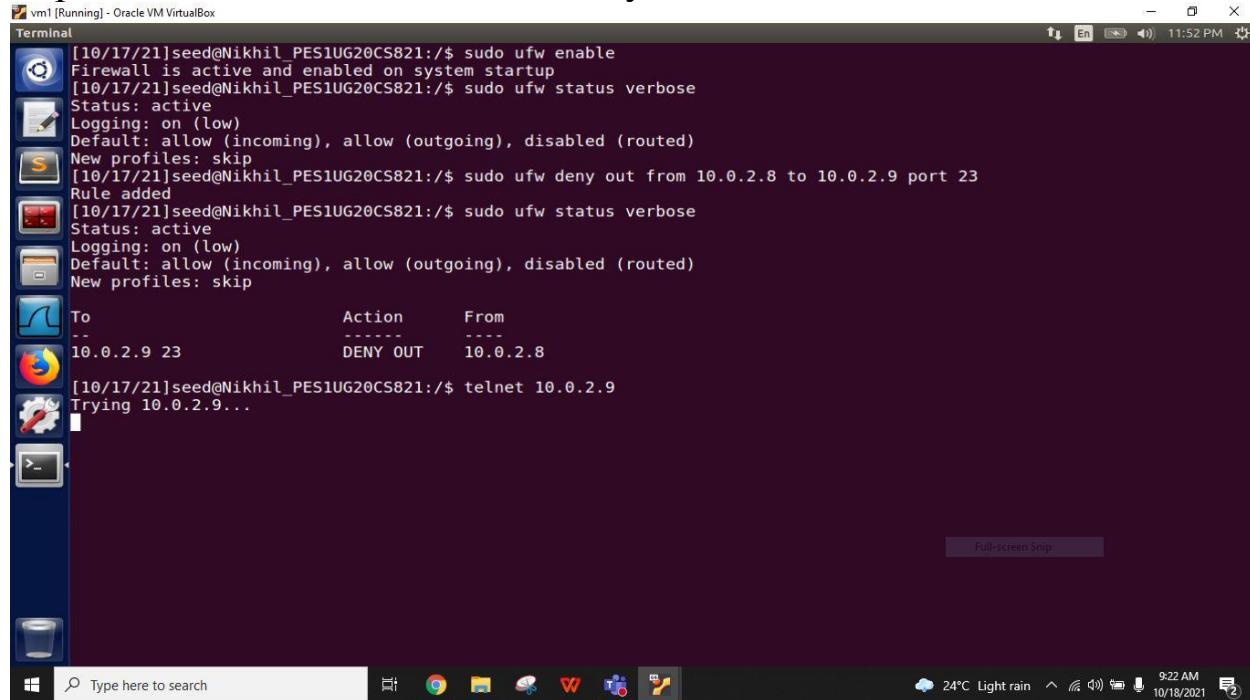
Now on vm1 we are going to enable the firewall and set an rule sucj that from port 23 that is telnet from vm1 to vm2 is going to block And we can see that the rules is successfully added by checking the status of the firewall



```
[10/17/21]seed@Nikhil_PES1UG20CS821:/$ sudo ufw enable
Firewall is active and enabled on system startup
[10/17/21]seed@Nikhil_PES1UG20CS821:/$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[10/17/21]seed@Nikhil_PES1UG20CS821:/$ sudo ufw deny out from 10.0.2.8 to 10.0.2.9 port 23
Rule added
[10/17/21]seed@Nikhil_PES1UG20CS821:/$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To           Action      From
--           ----      --
10.0.2.9 23    DENY OUT    10.0.2.8

[10/17/21]seed@Nikhil_PES1UG20CS821:/$
```

On we try to establish a connection using telnet from vm1 to vm2 which we blocked using firewall we can see that we are not able to connect that implies the rule is added successfully

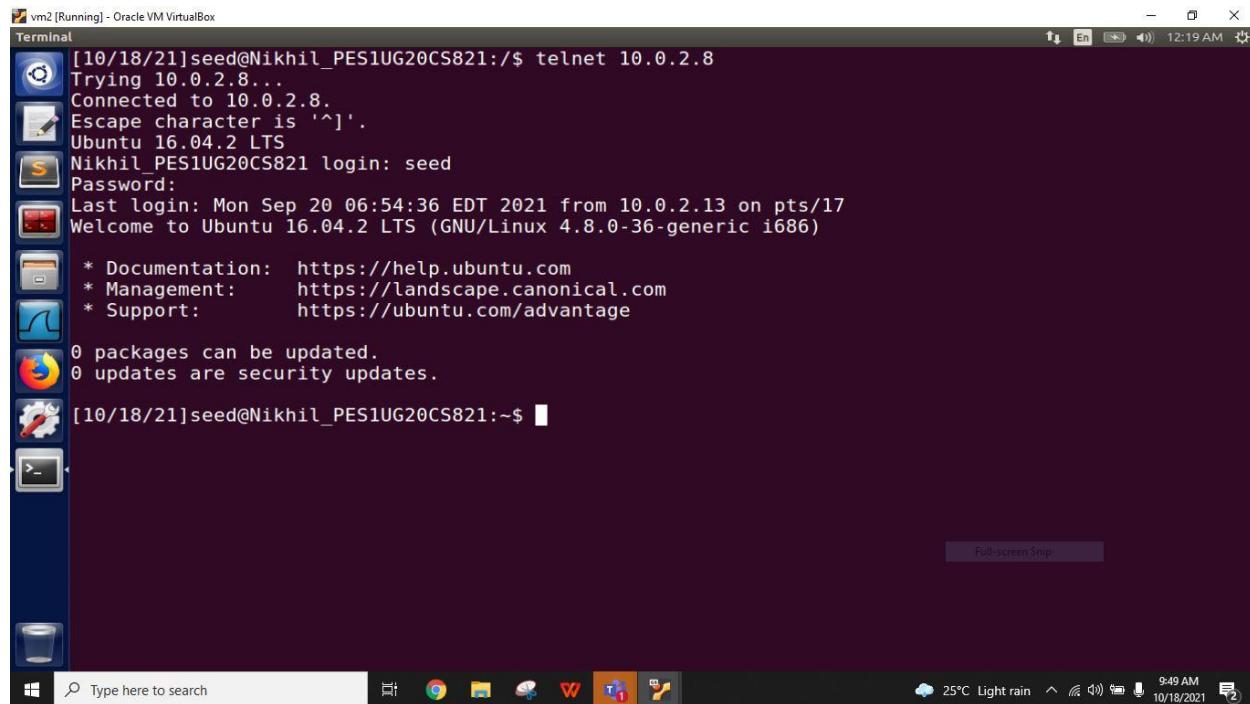


vm1 [Running] - Oracle VM VirtualBox
Terminal

```
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw enable
Firewall is active and enabled on system startup
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny out from 10.0.2.8 to 10.0.2.9 port 23
Rule added
[10/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To           Action      From
--          ----      ---
10.0.2.9 23  DENY OUT   10.0.2.8

[10/17/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.9...
Trying 10.0.2.9...
```

Now we go back to vm2 and establish a connection to vm1 using telnet and we can achieve this as rules only added from connecting vm1 to vm2 not vm2 to vm1



vm2 [Running] - Oracle VM VirtualBox
Terminal

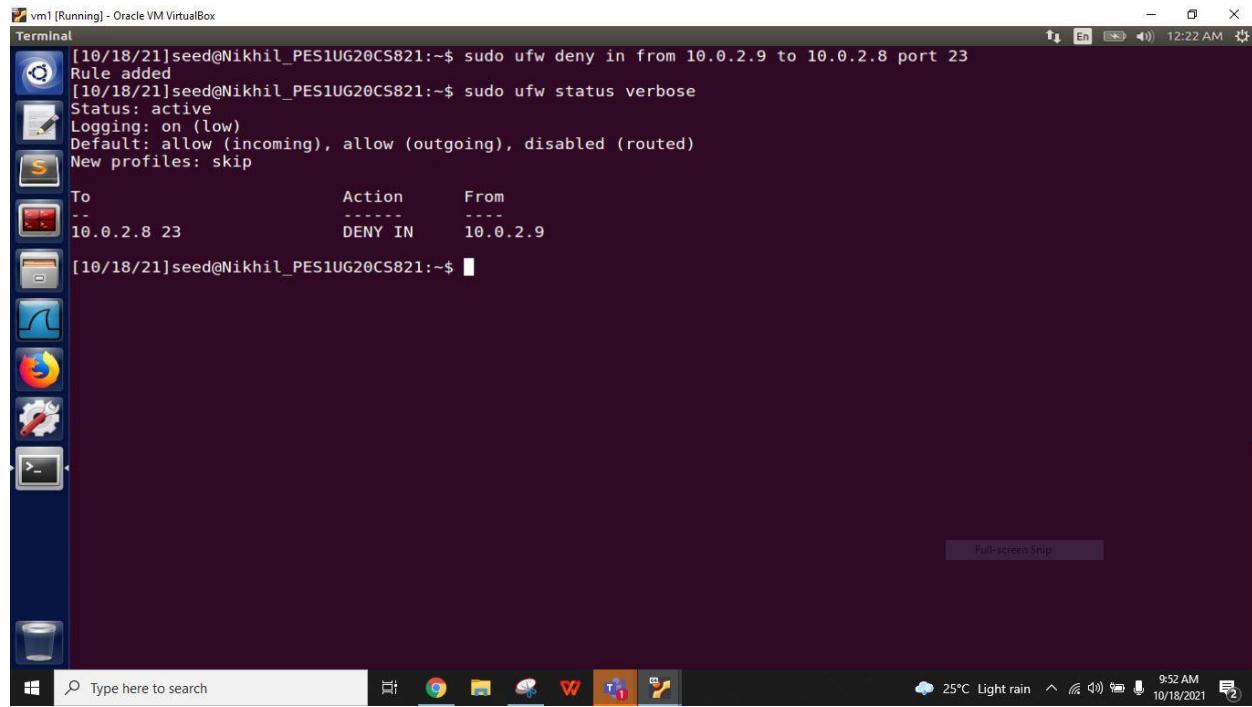
```
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Mon Sep 20 06:54:36 EDT 2021 from 10.0.2.13 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

[10/18/21]seed@Nikhil_PES1UG20CS821:~$
```

Now we add another rule in vm1 such that to block port 23 that is telnet from vm2 to vm1

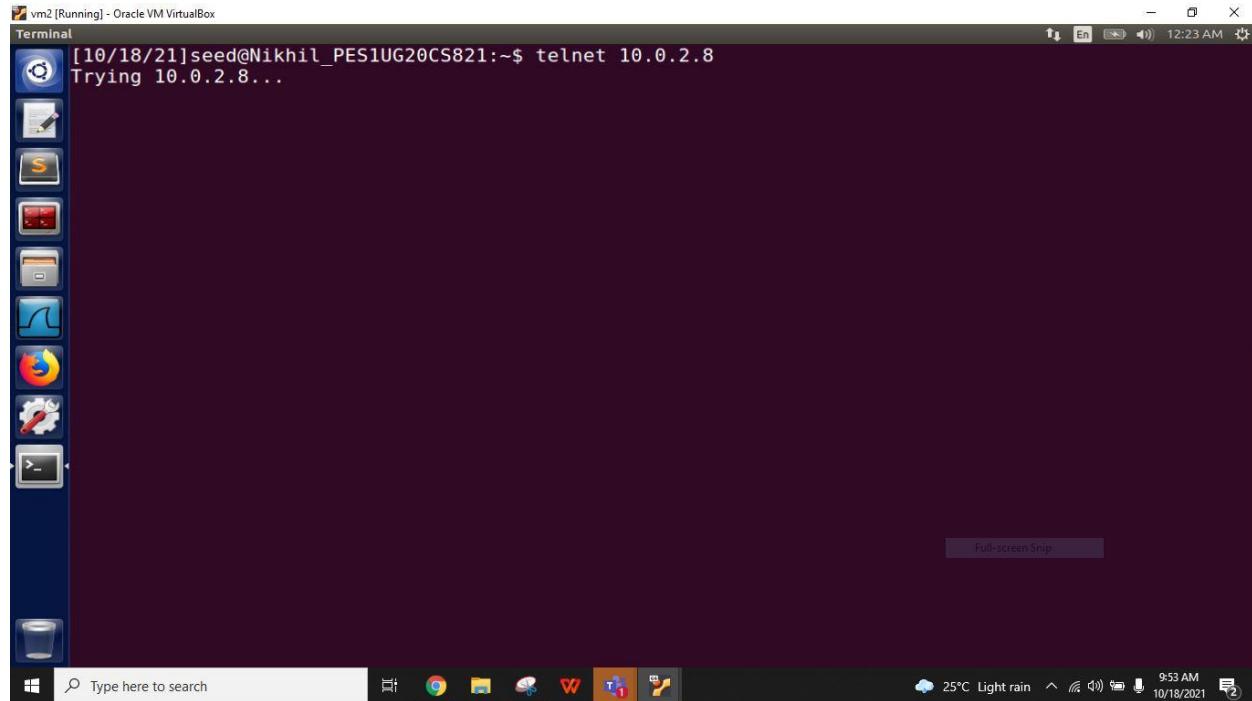


```
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny in from 10.0.2.9 to 10.0.2.8 port 23
Rule added
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To           Action      From
---          -----      ---
10.0.2.8 23  DENY IN    10.0.2.9

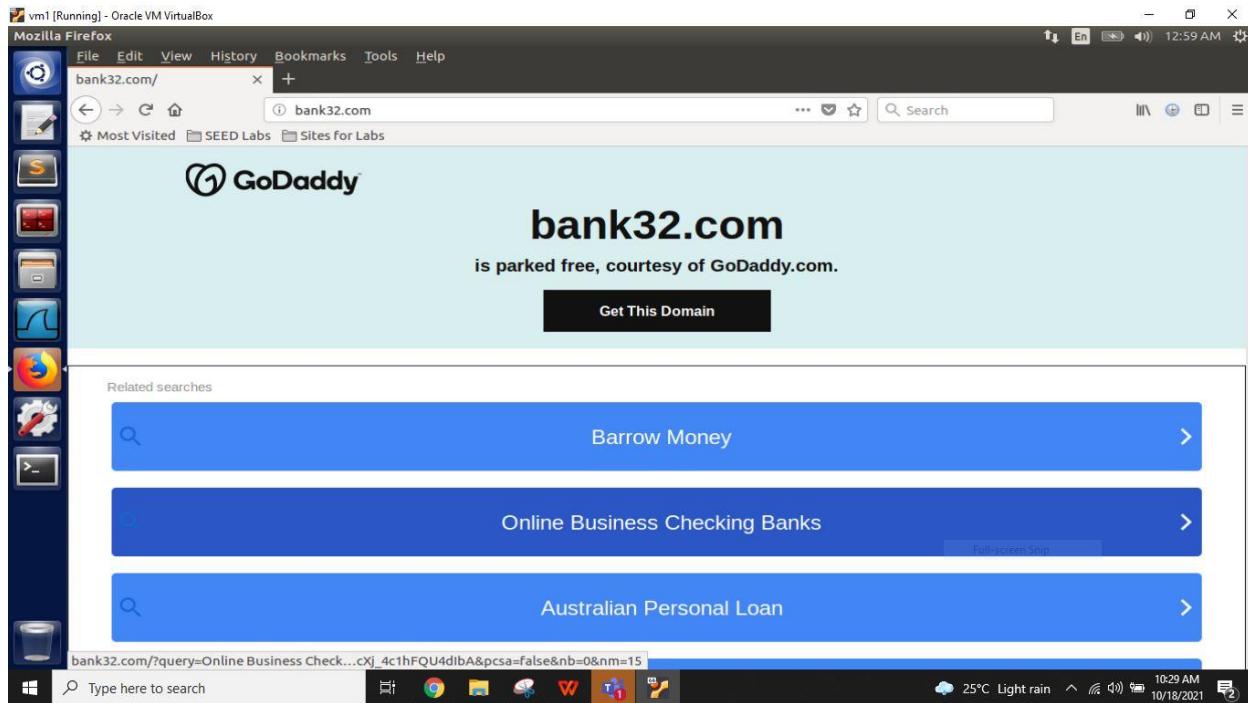
[10/18/21]seed@Nikhil_PES1UG20CS821:~$
```

After adding the rule in vm1 now we go back to vm2 and try to connect to vm1 through telnet which is not possible as the telnet port 23 in vm1 is blocked

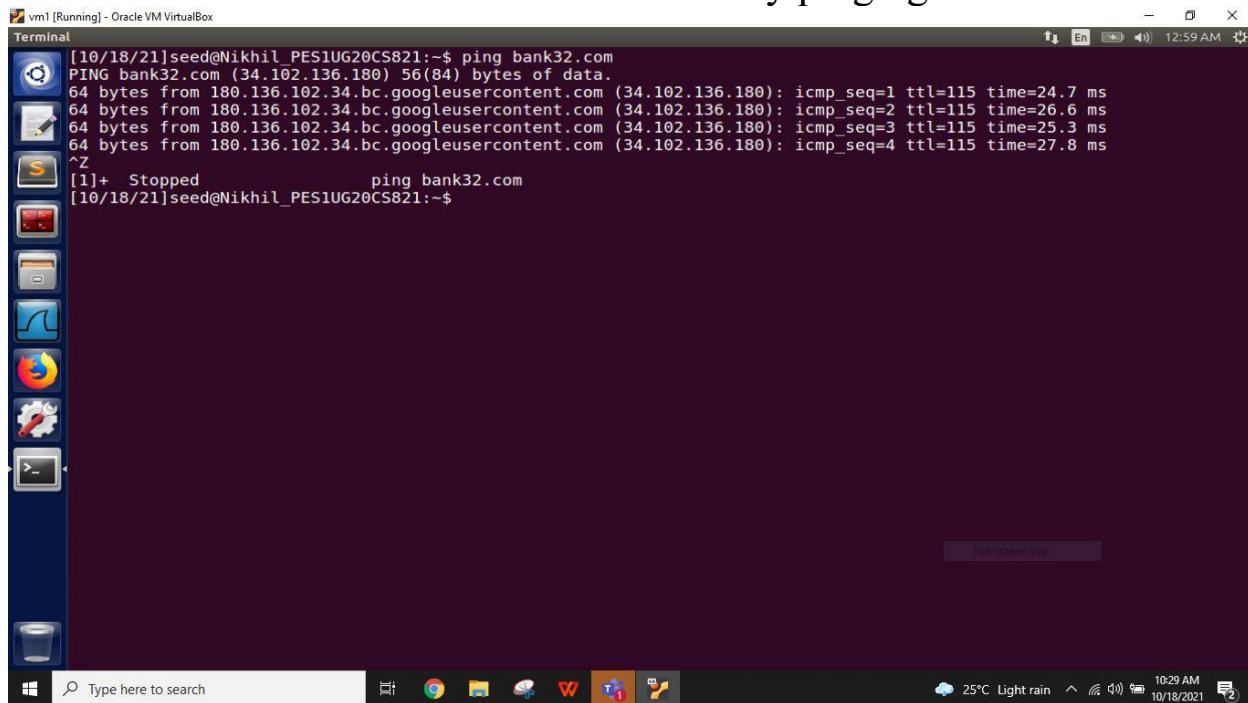


```
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.8
Trying 10.0.2.8...
```

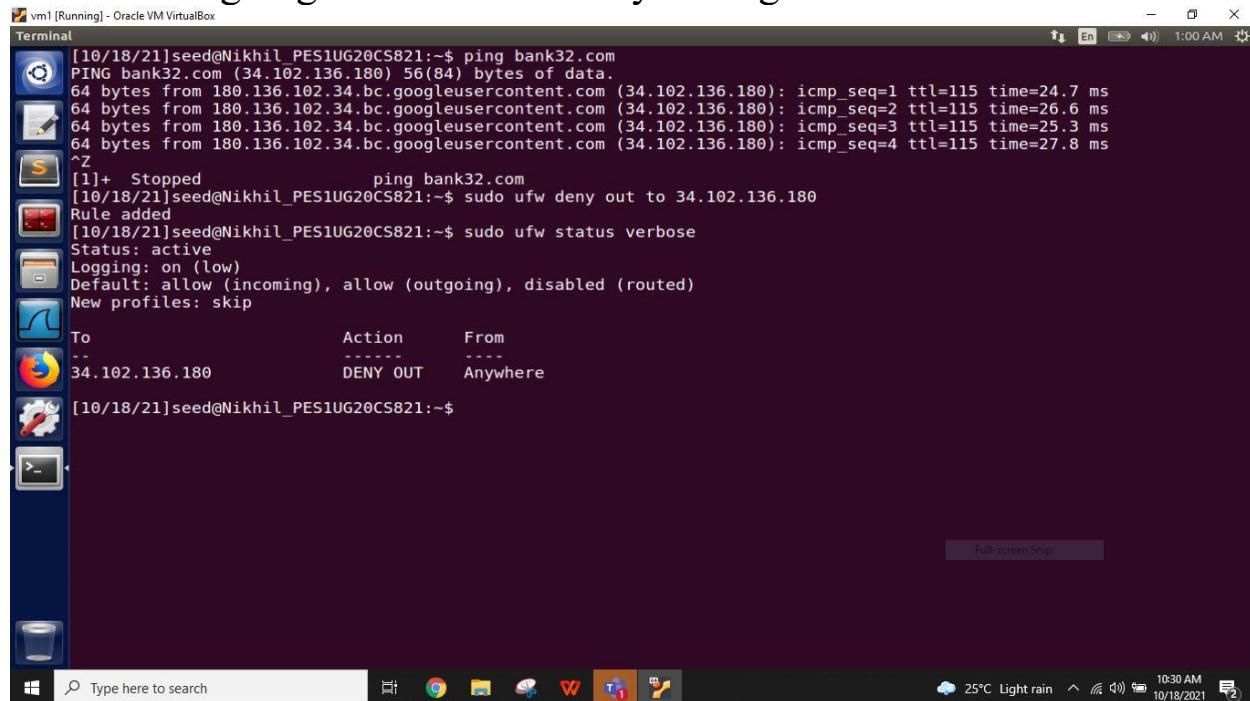
In this task first we are going to visit www.bank32.com in the vm1 browser and which is loaded in the browser of vm1



Now we obtain IP address of bank32.com by pinging it

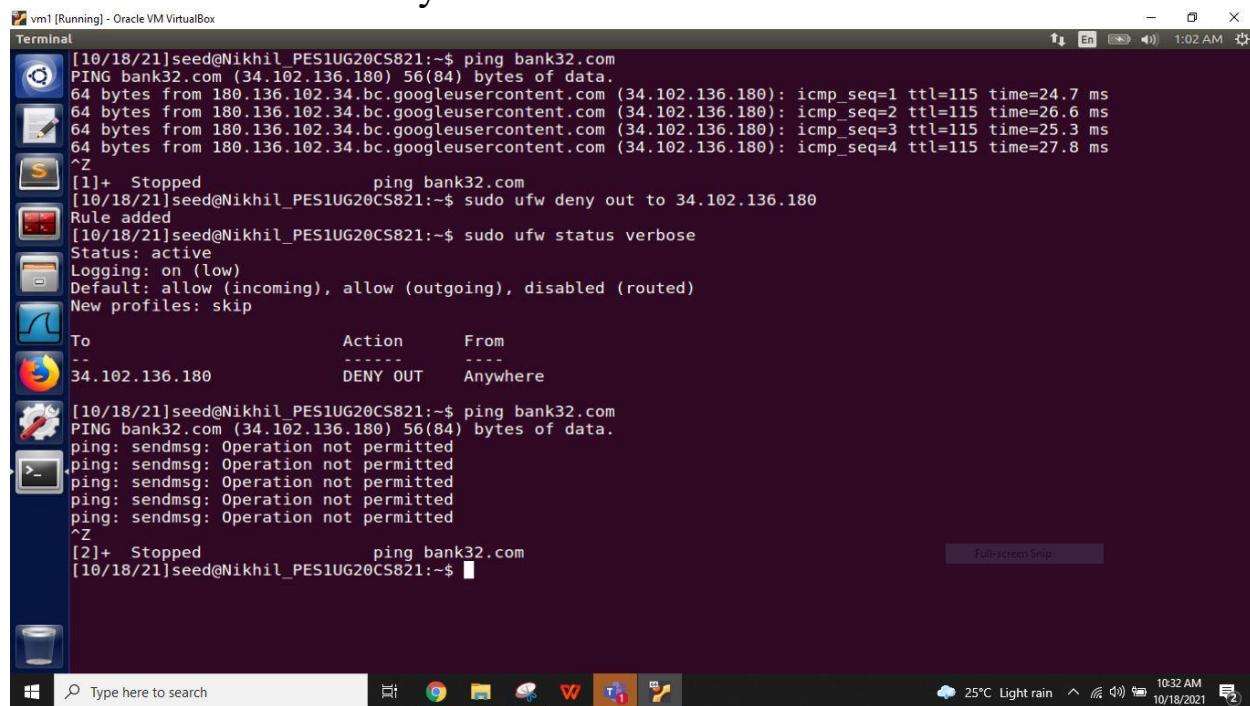


Now we block vm1 from visiting the site by adding the rule in the vm1.we are going to block the site by adding its IP address



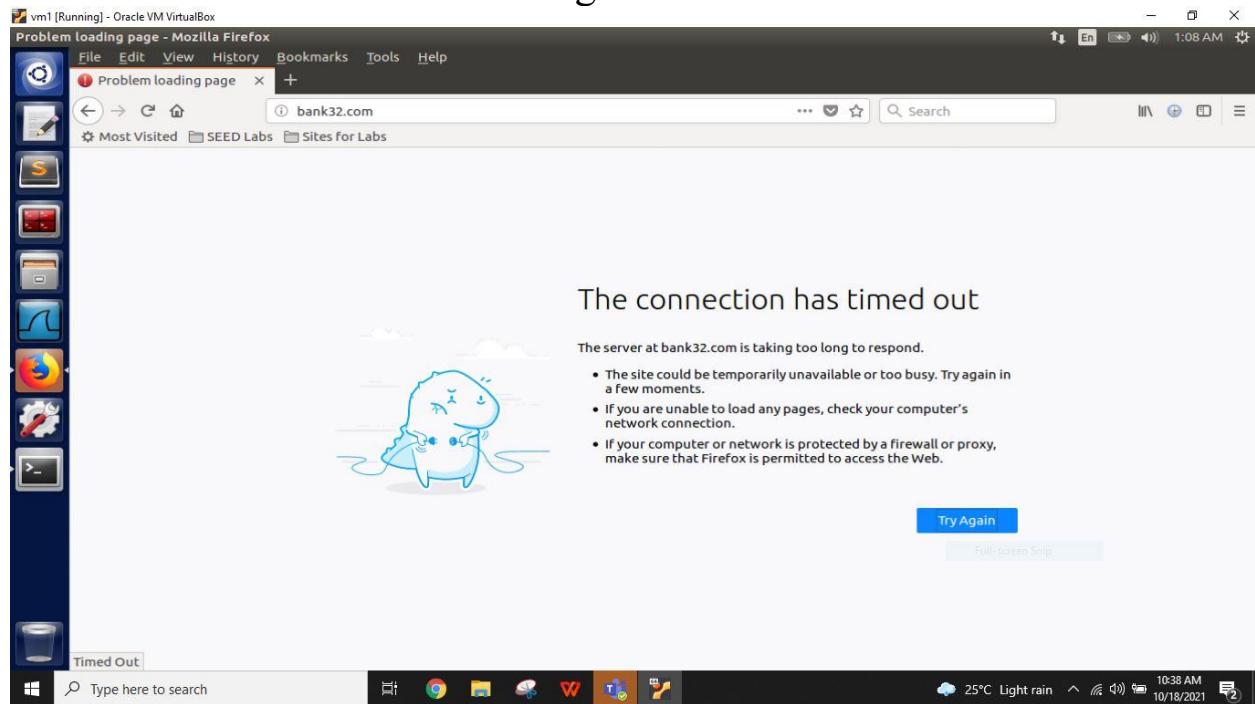
```
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ ping bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=1 ttl=115 time=24.7 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=2 ttl=115 time=26.6 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=3 ttl=115 time=25.3 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=4 ttl=115 time=27.8 ms
^Z
[1]+ Stopped ping bank32.com
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny out to 34.102.136.180
Rule added
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To Action From
-- DENY OUT Anywhere
[10/18/21]seed@Nikhil_PES1UG20CS821:~$
```

After adding the rule and blocking it we are going to ping the same site and we can see that in terminal it shows operation not permitted this means the rule is successfully added and we blocked the site bank32.com successfully



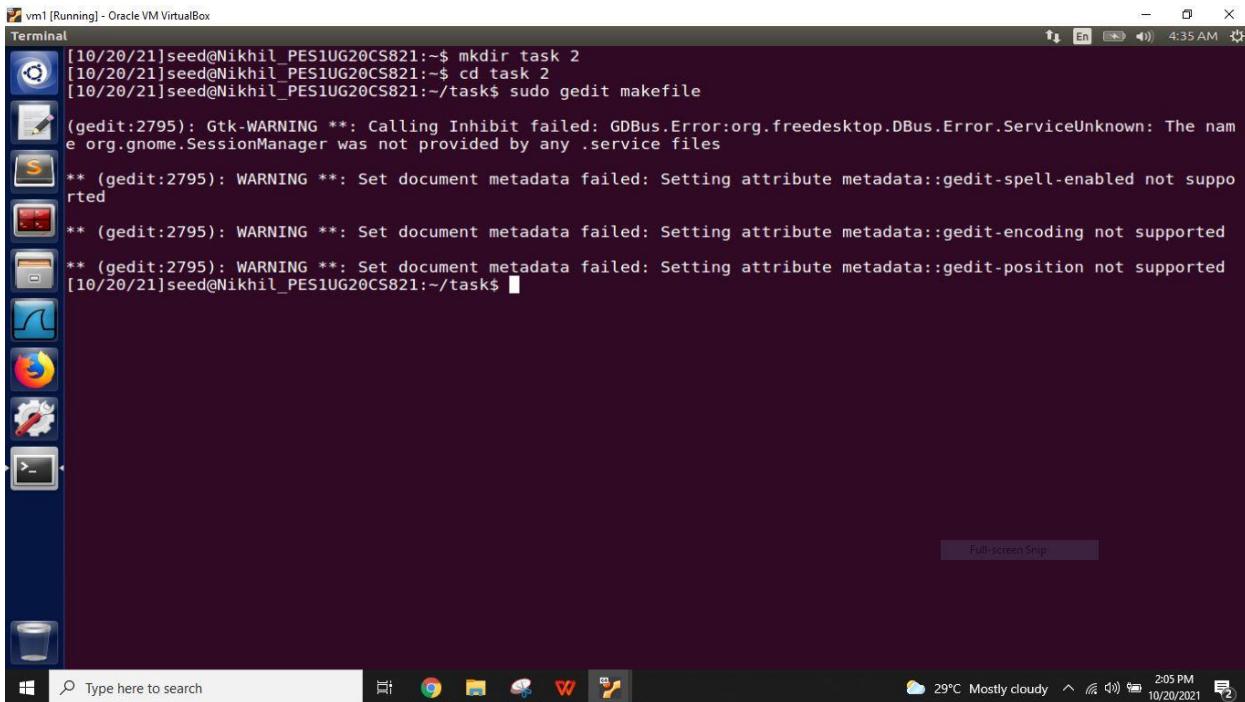
```
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ ping bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=1 ttl=115 time=24.7 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=2 ttl=115 time=26.6 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=3 ttl=115 time=25.3 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=4 ttl=115 time=27.8 ms
^Z
[1]+ Stopped ping bank32.com
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny out to 34.102.136.180
Rule added
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To Action From
-- DENY OUT Anywhere
[10/18/21]seed@Nikhil_PES1UG20CS821:~$ ping bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
^Z
[2]+ Stopped ping bank32.com
[10/18/21]seed@Nikhil_PES1UG20CS821:~$
```

And we clear the cache and history in the web browser and going to access the site again in the browser and can see that it cant able to load it as that IP address is blocked using firewall



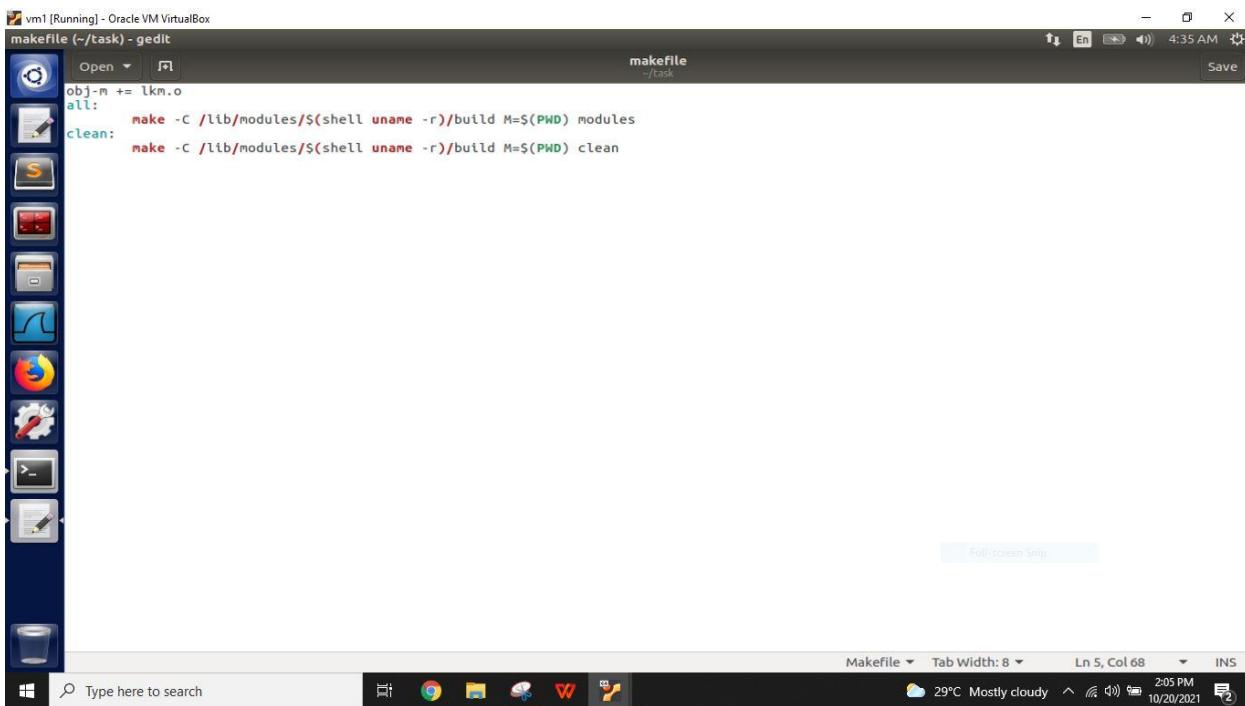
Task 2: How Firewall Works

in task2 we create a new folder named task 2 and create a c file names as lkm.c and a Make file



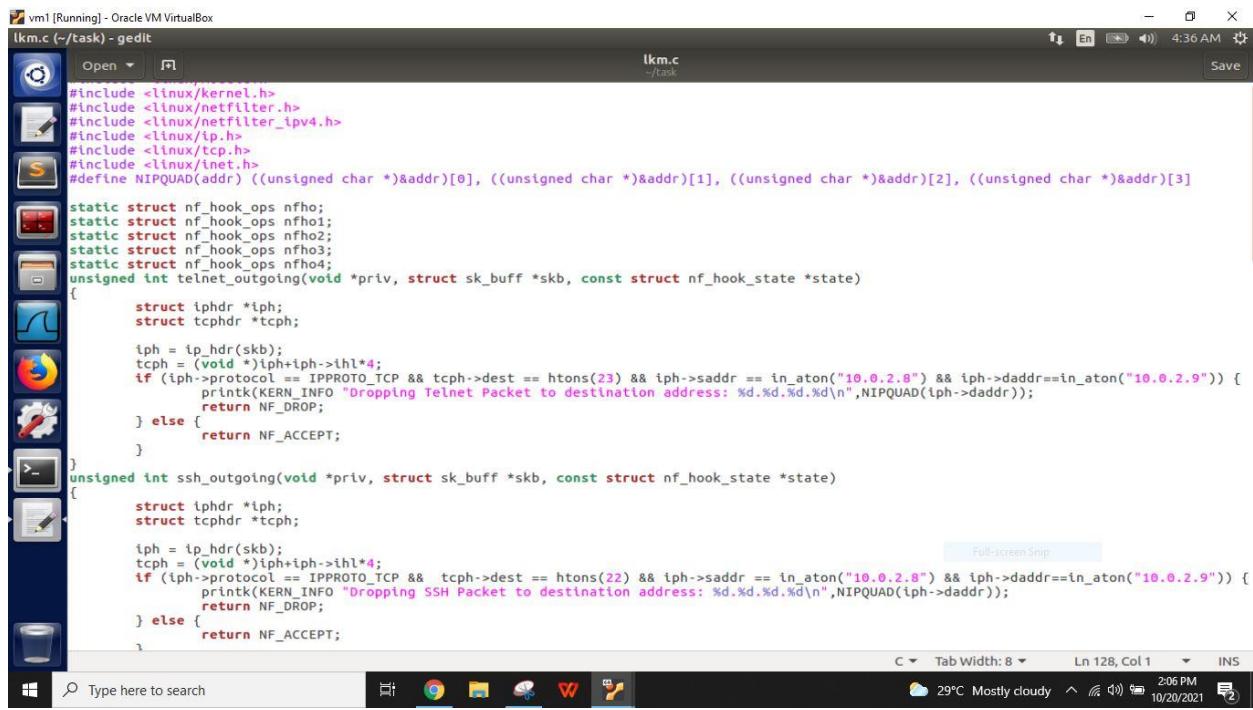
vm1 [Running] - Oracle VM VirtualBox
Terminal
[10/20/21]seed@Nikhil_PES1UG20CS821:~\$ mkdir task 2
[10/20/21]seed@Nikhil_PES1UG20CS821:~\$ cd task 2
[10/20/21]seed@Nikhil_PES1UG20CS821:~/task\$ sudo gedit makefile
(gedit:2795): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:2795): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:2795): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2795): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/20/21]seed@Nikhil_PES1UG20CS821:~/task\$ █

Code for the file Make



vm1 [Running] - Oracle VM VirtualBox
makefile (~/task) - gedit
makefile (~/task)
Open Save
obj-m += lkm.o
all:
 make -C /lib/modules/\$(shell uname -r)/build M=\$(PWD) modules
clean:
 make -C /lib/modules/\$(shell uname -r)/build M=\$(PWD) clean

Code for the lk.c file



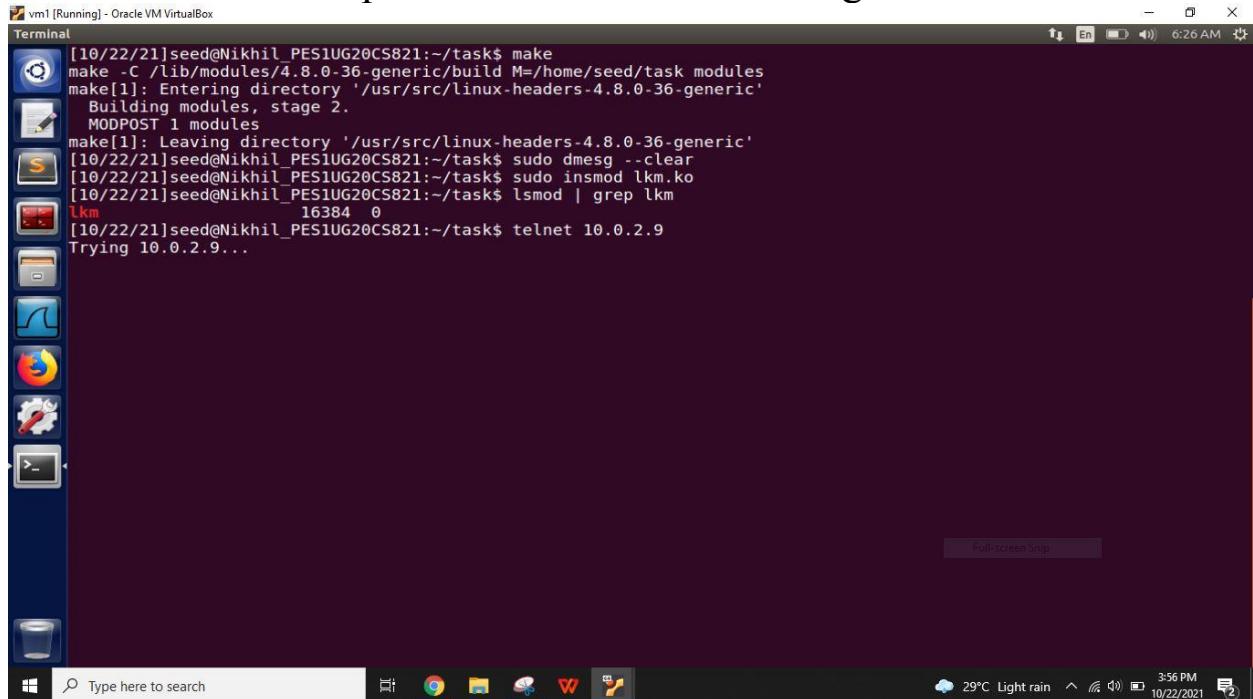
```
#include <linux/kernel.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/inet.h>
#define NIPQUAD(addr) ((unsigned char *)&addr)[0], ((unsigned char *)&addr)[1], ((unsigned char *)&addr)[2], ((unsigned char *)&addr)[3]

static struct nf_hook_ops nfho;
static struct nf_hook_ops nfho1;
static struct nf_hook_ops nfho2;
static struct nf_hook_ops nfho3;
static struct nf_hook_ops nfho4;
unsigned int telnet_outgoing(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
    struct iphdr *iph;
    struct tcphdr *tcph;

    iph = ip_hdr(skb);
    tcph = (void *)iph+iph->ihl*4;
    if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(23) && iph->saddr == in_aton("10.0.2.8") && iph->daddr==in_aton("10.0.2.9")) {
        printk(KERN_INFO "Dropping Telnet Packet to destination address: %d.%d.%d.%d\n",NIPQUAD(iph->daddr));
        return NF_DROP;
    } else {
        return NF_ACCEPT;
    }
}
unsigned int ssh_outgoing(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
    struct iphdr *iph;
    struct tcphdr *tcph;

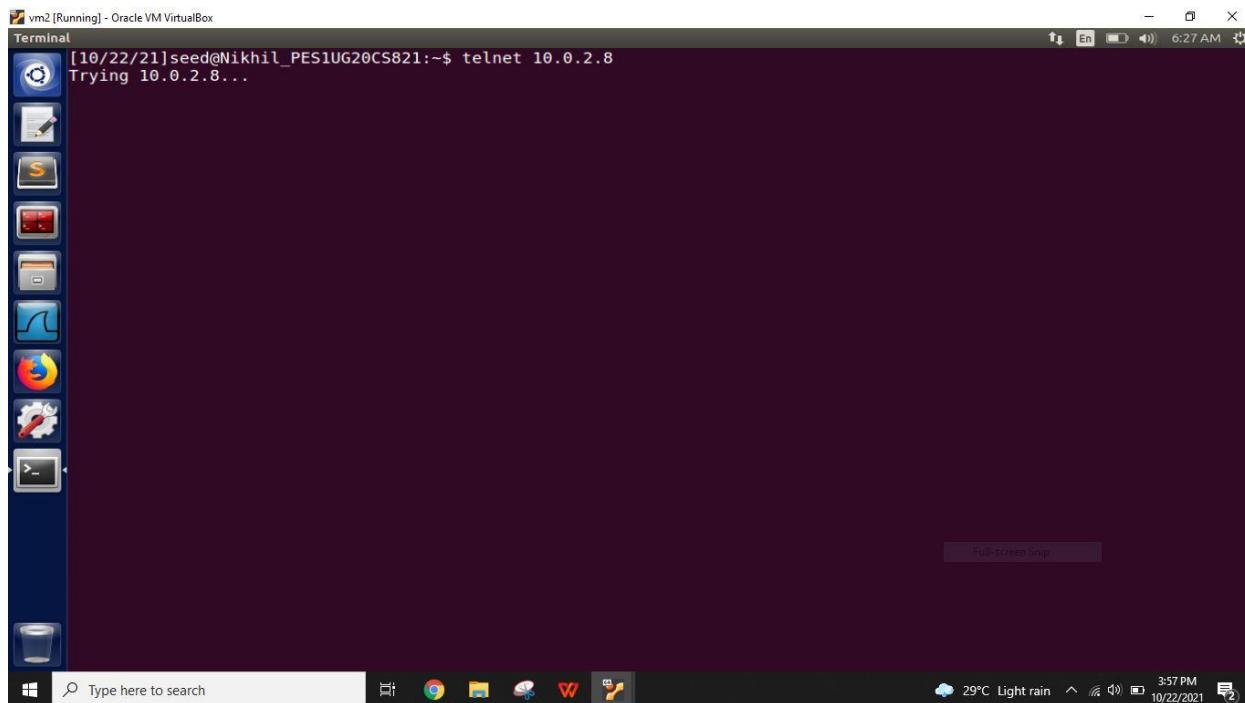
    iph = ip_hdr(skb);
    tcph = (void *)iph+iph->ihl*4;
    if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(22) && iph->saddr == in_aton("10.0.2.8") && iph->daddr==in_aton("10.0.2.9")) {
        printk(KERN_INFO "Dropping SSH Packet to destination address: %d.%d.%d.%d\n",NIPQUAD(iph->daddr));
        return NF_DROP;
    } else {
        return NF_ACCEPT;
    }
}
```

Now we build the make file by executing the command make in the same path where the lk.c and Make file present.now clear the dmesg section and The compiled lkm.ko is inserted using insmod



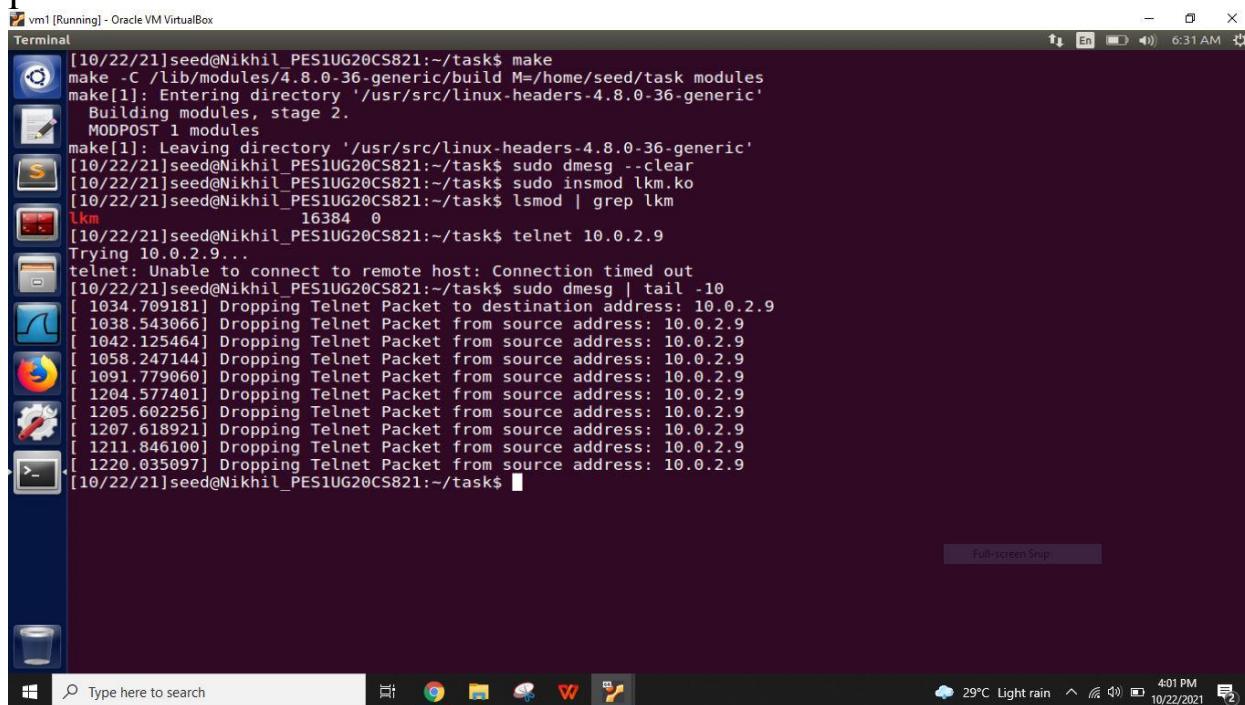
```
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed/task modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  Building modules, stage 2.
    MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ sudo dmesg --clear
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ sudo insmod lkm.ko
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ lsmod | grep lkm
lkm               16384  0
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ telnet 10.0.2.9
Trying 10.0.2.9...
```

After building the make file we try to connect vm1 from vm2 which is blocked and can be seen in the terminal below



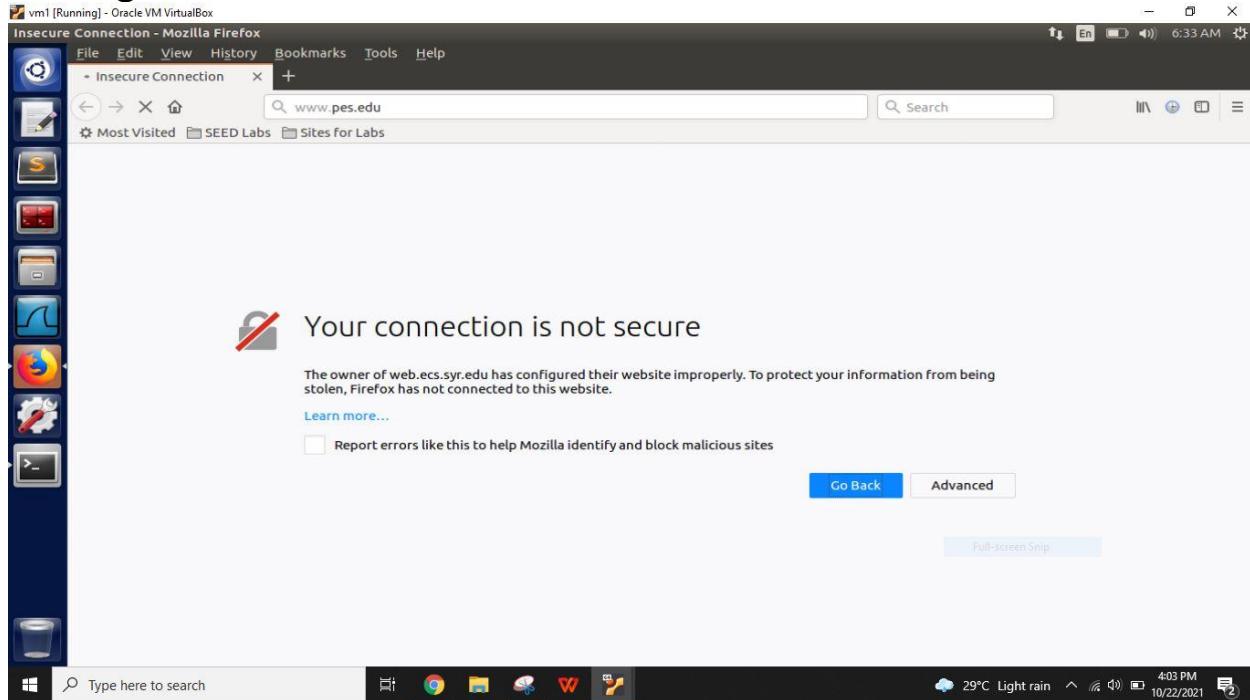
```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.8
Trying 10.0.2.8...
```

After executing the dmesg command we can see that the dropping telnet packets can be seen



```
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed/task modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  Building modules, stage 2.
    MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ sudo dmesg --clear
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ sudo insmod lkm.ko
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ lsmod | grep lkm
lkm               16384  0
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ telnet 10.0.2.9
Trying 10.0.2.9...
telnet: Unable to connect to remote host: Connection timed out
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ sudo dmesg | tail -10
[1034.709181] Dropping Telnet Packet to destination address: 10.0.2.9
[1038.543066] Dropping Telnet Packet from source address: 10.0.2.9
[1042.125464] Dropping Telnet Packet from source address: 10.0.2.9
[1058.247144] Dropping Telnet Packet from source address: 10.0.2.9
[1091.779060] Dropping Telnet Packet from source address: 10.0.2.9
[1204.577401] Dropping Telnet Packet from source address: 10.0.2.9
[1205.602256] Dropping Telnet Packet from source address: 10.0.2.9
[1207.618921] Dropping Telnet Packet from source address: 10.0.2.9
[1211.846100] Dropping Telnet Packet from source address: 10.0.2.9
[1220.035097] Dropping Telnet Packet from source address: 10.0.2.9
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$
```

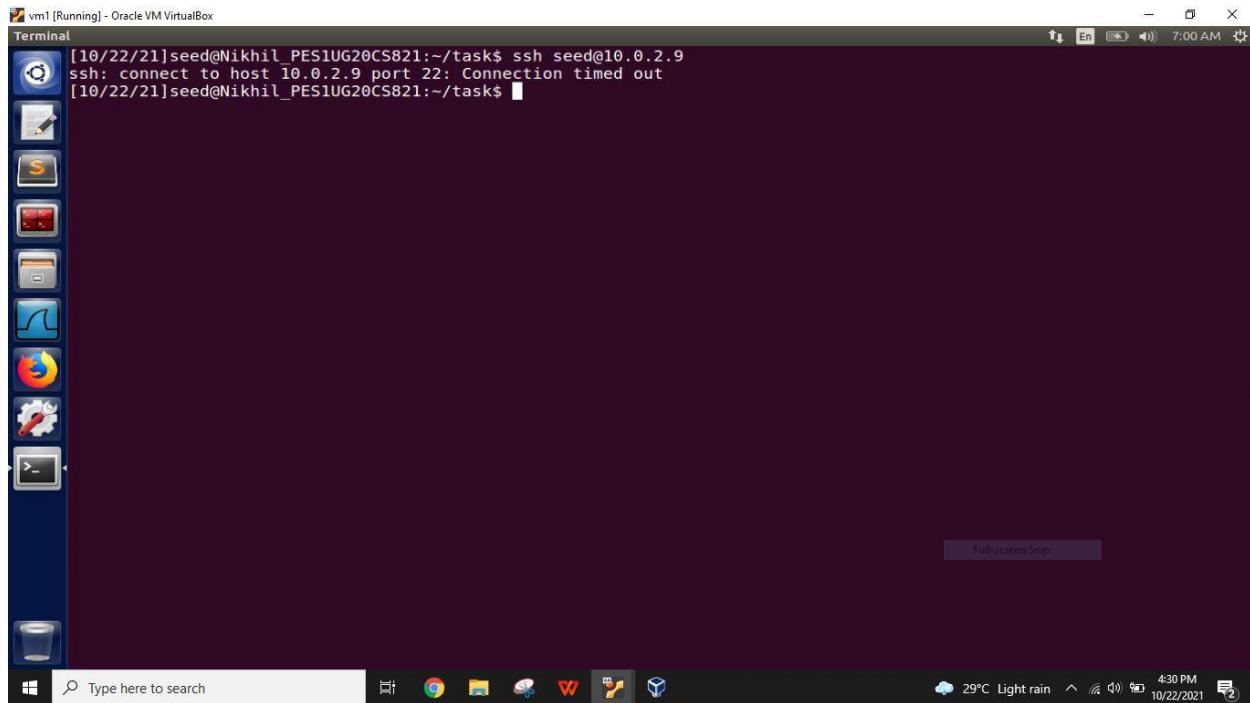
We also blocked the pes.edu site in the c file so now we go to the browser and browse the pes.edu site and can be seen that the site is not loading and it is blocked



While the pes.edu page is surfing we open the another terminal in the same vm and can see the telnet packets dropping with the help of dmesg command

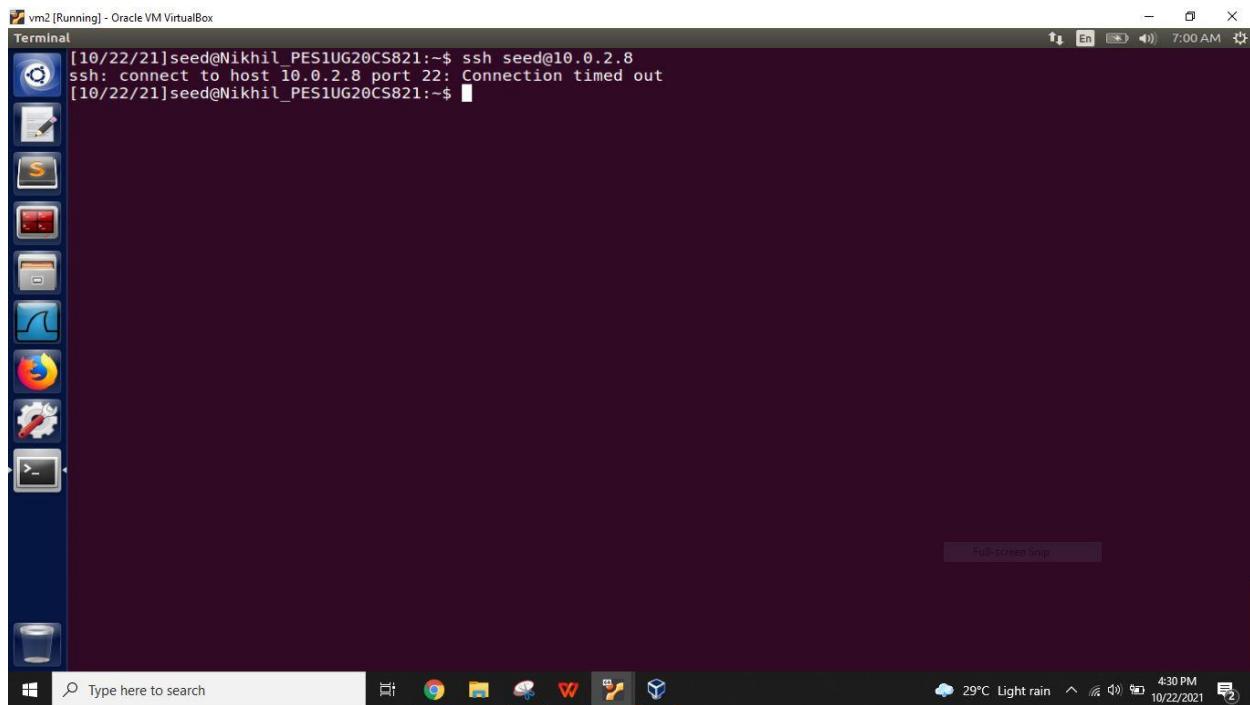
A screenshot of a Linux terminal window titled "Terminal". The terminal is displaying the output of the "dmesg" command. The output shows numerous entries indicating "Dropping Telnet Packet" or "Dropping Web Packet" from various source addresses (e.g., 1034.709181, 1038.543066, 1042.125464, etc.) to destination address 10.0.2.9. The timestamp for these entries spans from 10/22/21 to 10/22/21. The terminal window has a "Full-screen Snip" button at the bottom right. The desktop environment includes icons for various applications like a file manager, browser, and terminal, along with a taskbar showing the date and time (10/22/2021, 4:02 PM).

Now we test whether the ssh is blocked from vm1 to vm2 and we can see that it is blocked



```
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$ ssh seed@10.0.2.9
ssh: connect to host 10.0.2.9 port 22: Connection timed out
[10/22/21]seed@Nikhil_PES1UG20CS821:~/task$
```

Now we test whether the ssh is blocked from vm2 to vm1 and we can see that it is blocked



```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ ssh seed@10.0.2.8
ssh: connect to host 10.0.2.8 port 22: Connection timed out
[10/22/21]seed@Nikhil_PES1UG20CS821:~$
```

Task 3: Evading Egress Filtering

Task 3.a: Telnet to Machine B through the firewall

Now we delete the old rules that we applied for previous tasks

```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To           Action     From
--          ----      -----
34.102.136.180    DENY OUT   Anywhere

[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw delete 1
Deleting:
deny out to 34.102.136.180
Proceed with operation (y|n)? y
Rule deleted
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ █
```

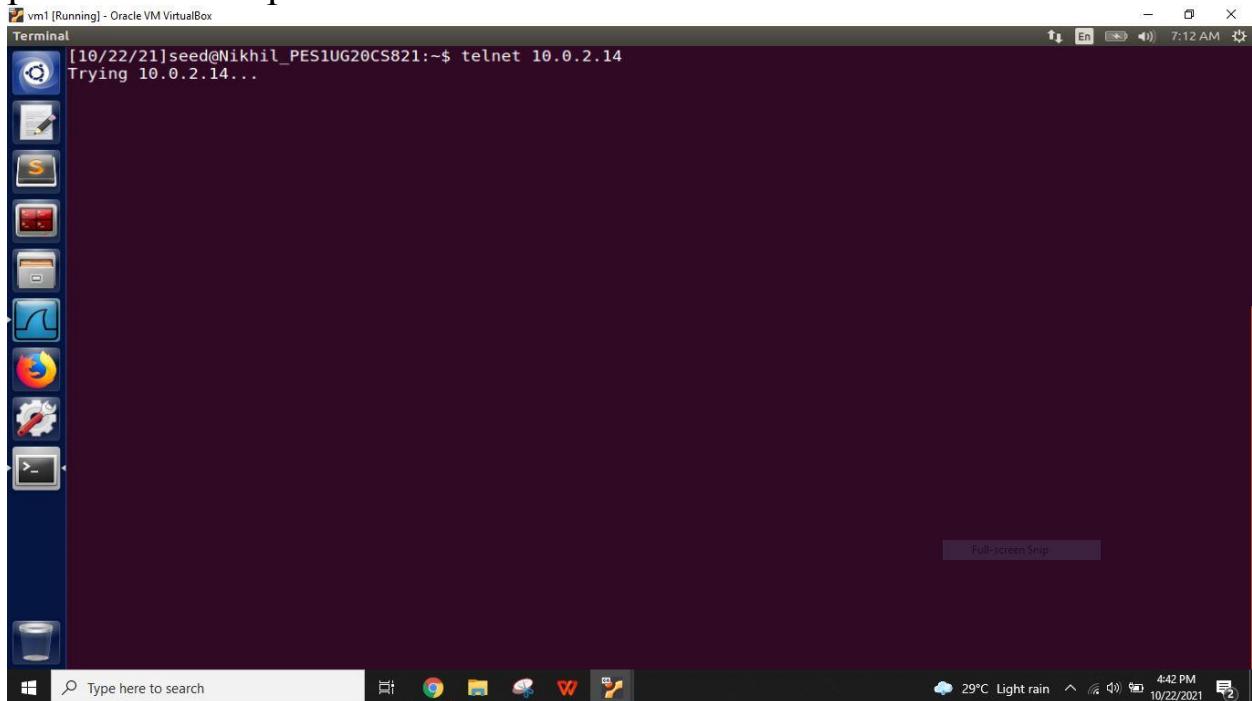
Now set the new rule on vm1 to block all the from port 23 from IP address 10.0.2.8

```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw enable
Firewall is active and enabled on system startup
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny out from 10.0.2.8 to any port 23
Rule added
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

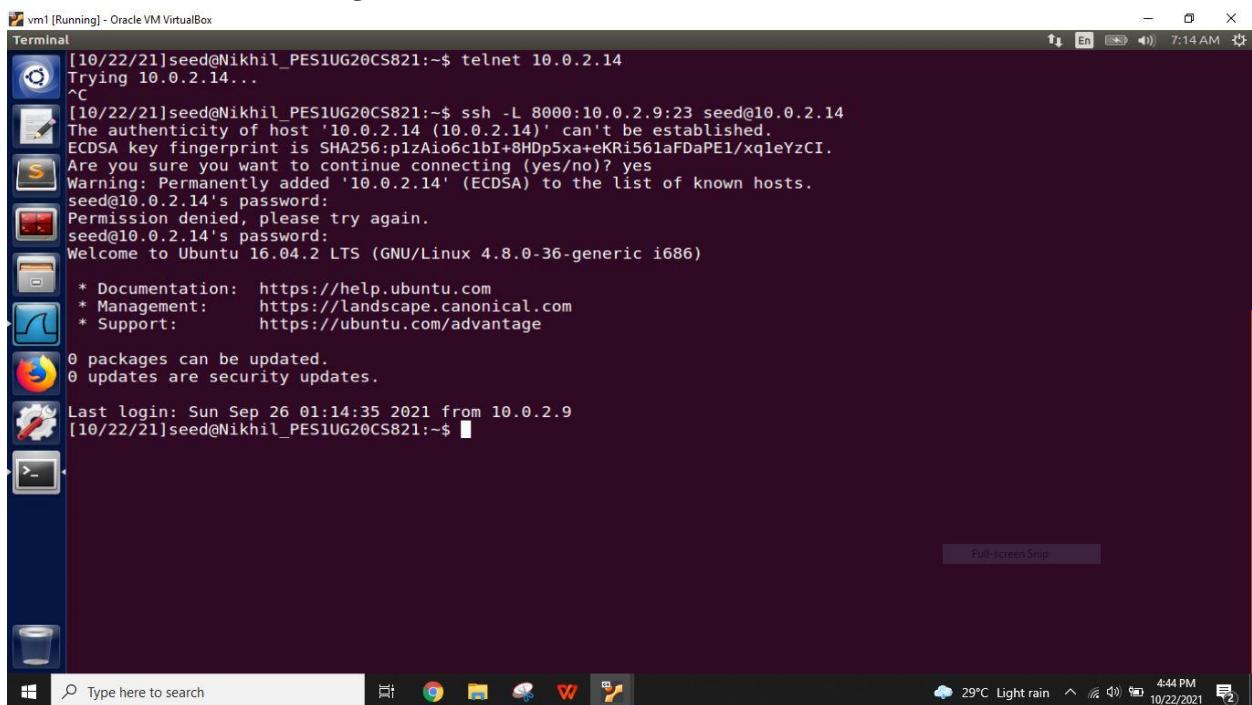
To           Action     From
--          ----      -----
23          DENY OUT   10.0.2.8

[10/22/21]seed@Nikhil_PES1UG20CS821:~$ █
```

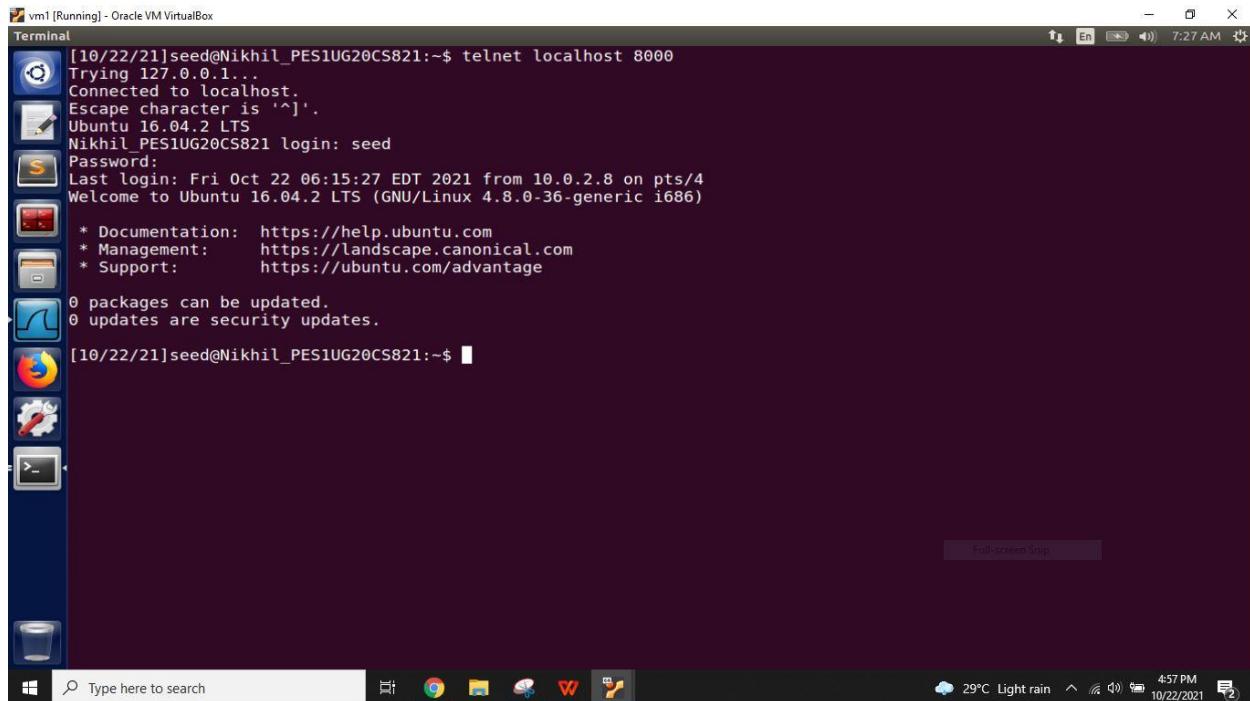
Now try to connect from vm1 to vm3 through telnet which is not possible as the port 23 is blocked from vm1



Since the port 23 is blocked we try to establish a connection using the ssh from vm1 to vm3



Through the ssh connection we can able to telnet the local host at port 8000



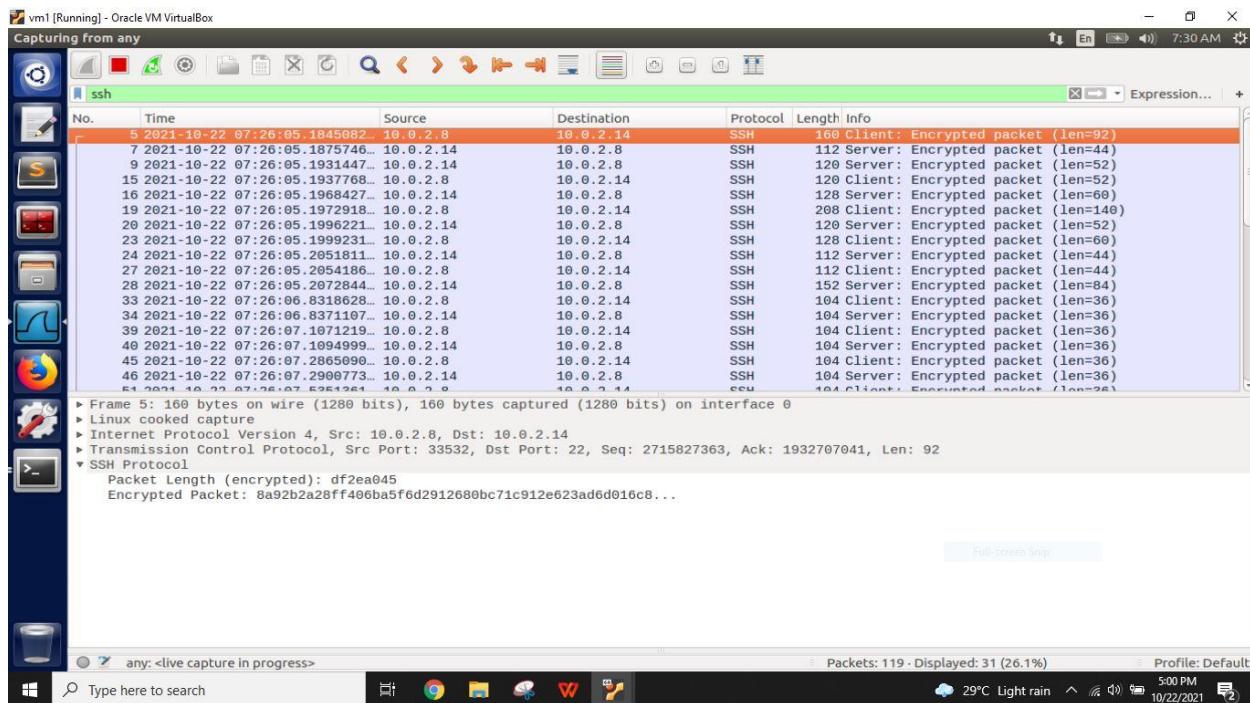
```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is ']'.
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Fri Oct 22 06:15:27 EDT 2021 from 10.0.2.8 on pts/4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

[10/22/21]seed@Nikhil_PES1UG20CS821:~$ █
```

Meanwhile we capture the packets from wireshark in all three vm's
In vm1 wireshark capture we can see that ssh connection is established
from vm1 to vm3



Capturing from any

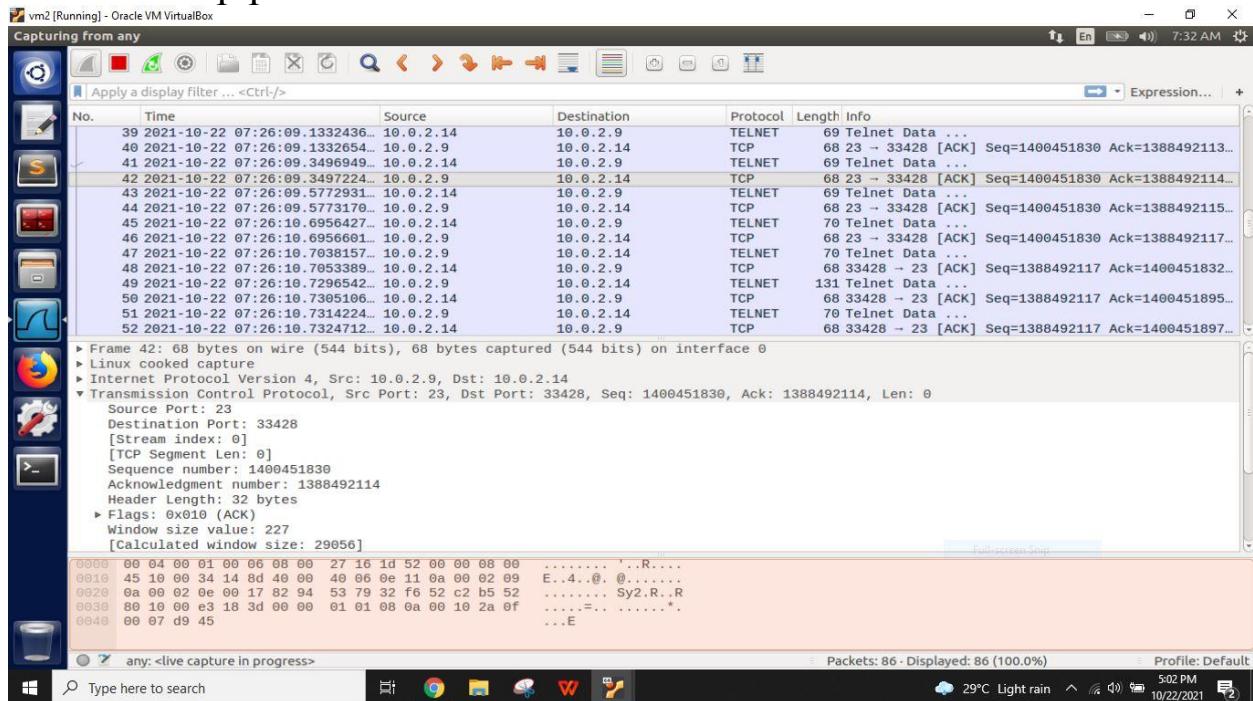
No.	Time	Source	Destination	Protocol	Length	Info
5	2021-10-22 07:26:05.1845082...	10.0.2.8	10.0.2.14	SSH	160	Client: Encrypted packet (len=92)
7	2021-10-22 07:26:05.1875746...	10.0.2.14	10.0.2.8	SSH	112	Server: Encrypted packet (len=44)
9	2021-10-22 07:26:05.1931447...	10.0.2.14	10.0.2.8	SSH	120	Client: Encrypted packet (len=52)
15	2021-10-22 07:26:05.1937768...	10.0.2.8	10.0.2.14	SSH	120	Server: Encrypted packet (len=52)
16	2021-10-22 07:26:05.1968427...	10.0.2.14	10.0.2.8	SSH	128	Client: Encrypted packet (len=60)
19	2021-10-22 07:26:05.1972918...	10.0.2.8	10.0.2.14	SSH	208	Server: Encrypted packet (len=148)
20	2021-10-22 07:26:05.1996221...	10.0.2.14	10.0.2.8	SSH	120	Client: Encrypted packet (len=52)
23	2021-10-22 07:26:05.1999231...	10.0.2.8	10.0.2.14	SSH	128	Server: Encrypted packet (len=60)
24	2021-10-22 07:26:05.2051811...	10.0.2.14	10.0.2.8	SSH	112	Client: Encrypted packet (len=44)
27	2021-10-22 07:26:05.2054186...	10.0.2.8	10.0.2.14	SSH	112	Server: Encrypted packet (len=44)
28	2021-10-22 07:26:05.2072844...	10.0.2.14	10.0.2.8	SSH	152	Client: Encrypted packet (len=84)
33	2021-10-22 07:26:06.8318628...	10.0.2.8	10.0.2.14	SSH	104	Server: Encrypted packet (len=36)
34	2021-10-22 07:26:06.8371107...	10.0.2.14	10.0.2.8	SSH	104	Client: Encrypted packet (len=36)
35	2021-10-22 07:26:07.1071219...	10.0.2.8	10.0.2.14	SSH	104	Server: Encrypted packet (len=36)
40	2021-10-22 07:26:07.1094999...	10.0.2.14	10.0.2.8	SSH	104	Client: Encrypted packet (len=36)
45	2021-10-22 07:26:07.2865090...	10.0.2.8	10.0.2.14	SSH	104	Server: Encrypted packet (len=36)
46	2021-10-22 07:26:07.2900773...	10.0.2.14	10.0.2.8	SSH	104	Client: Encrypted packet (len=36)
51	2021-10-22 07:26:07.5261361...	10.0.2.8	10.0.2.14	SSH	104	Server: Encrypted packet (len=36)

Frame 5: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
 ▶ Linux cooked capture
 ▶ Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.14
 ▶ Transmission Control Protocol, Src Port: 33532, Dst Port: 22, Seq: 2715827363, Ack: 1932707041, Len: 92
 ▶ SSH Protocol
 Packet Length (encrypted): df2ea045
 Encrypted Packet: 8a92b2a28ff406ba5f6d2912680bc71c912e623ad6d016c8...

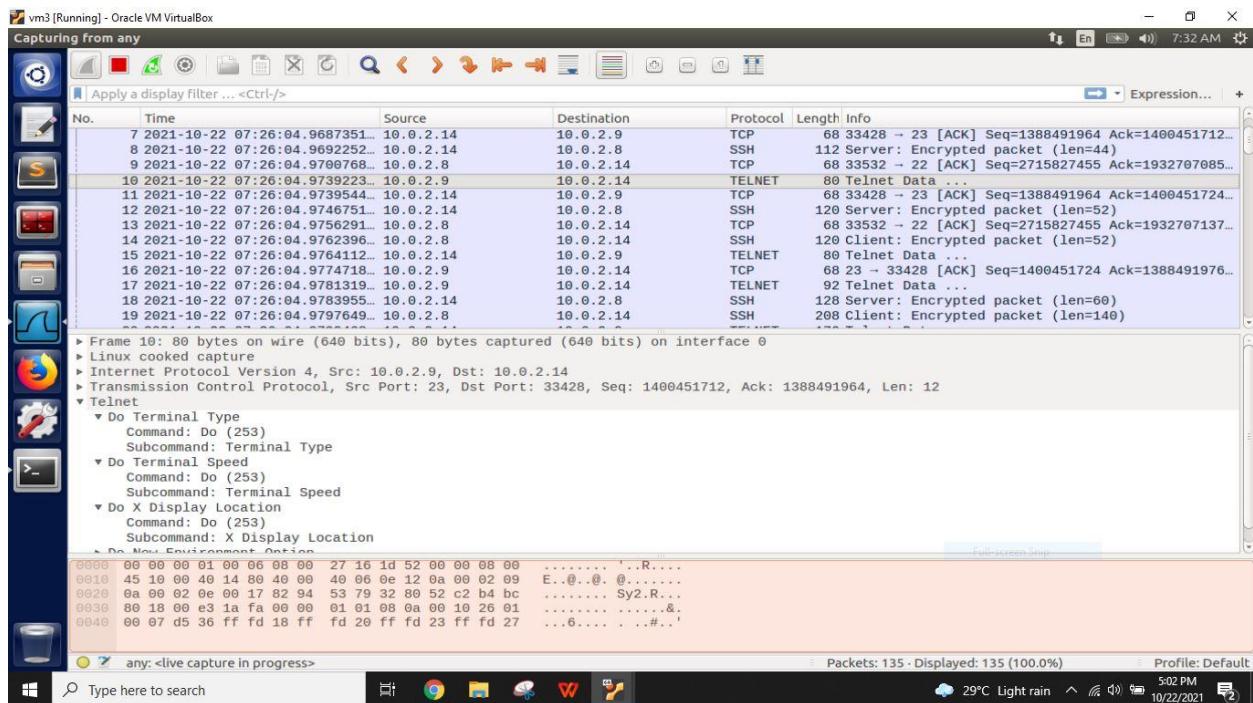
Packets: 119 - Displayed: 31 (26.1%) Profile: Default

457 PM 29°C Light rain 10/22/2021

In vm2 packets capture through wireshark we can observe that both telnet and tcp packets flow from vm2 to vm3

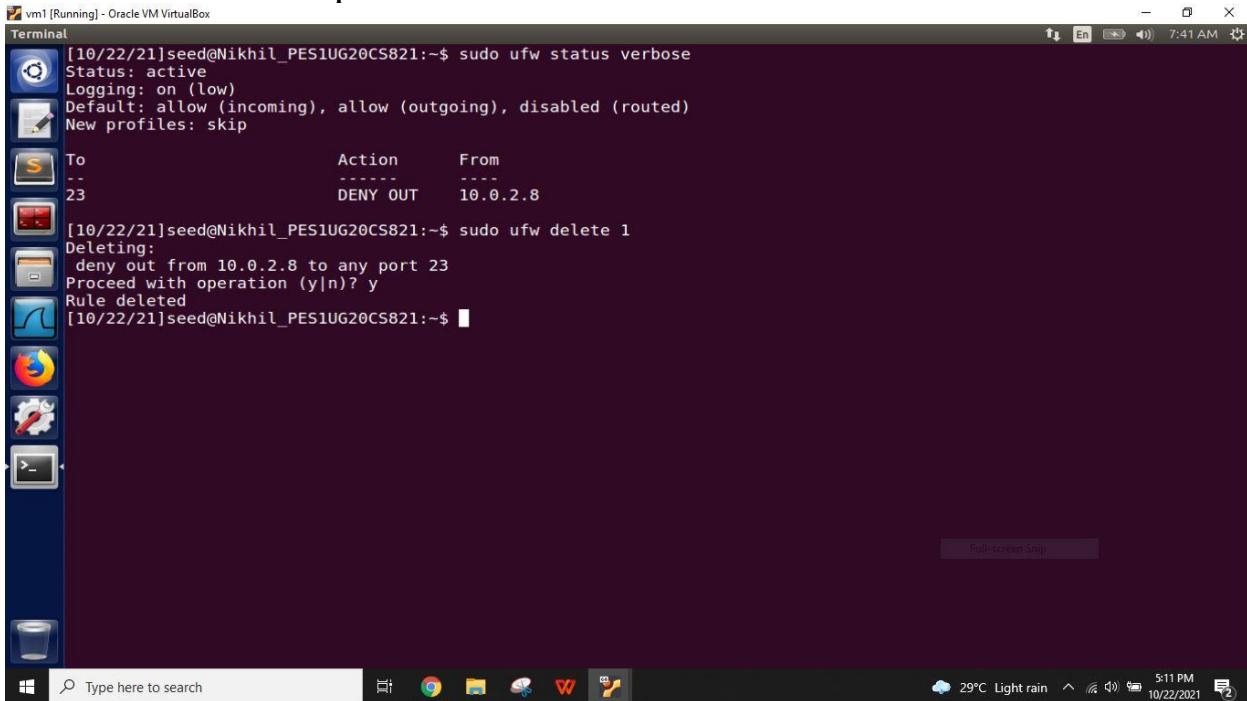


In vm3 wireshark obseravtion we can see telnet,tcp and ssh all three protocols are used.ssh is used by the vm1.tcp and telnet is used by the vm2



Task 3.b: Connecting to Google using SSH tunnel

first we delete the previous rules we added



vm1 [Running] - Oracle VM VirtualBox

```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

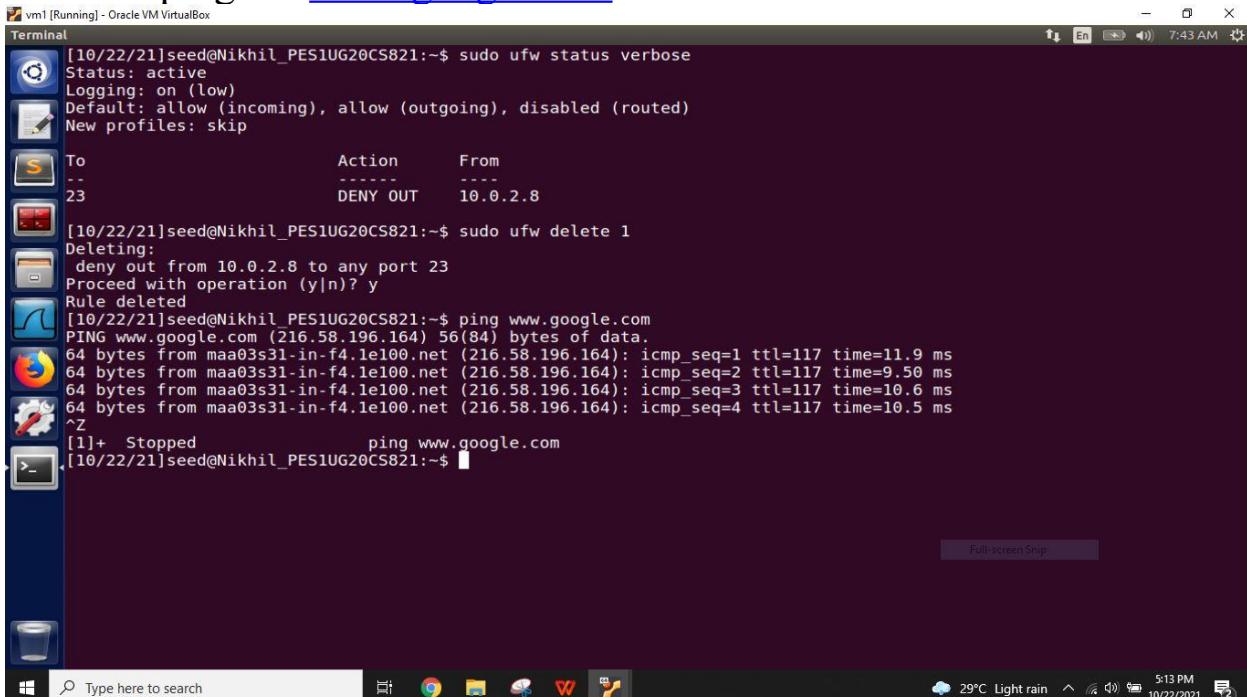
To           Action      From
--          ----      --
23          DENY OUT    10.0.2.8

[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw delete 1
Deleting:
  deny out from 10.0.2.8 to any port 23
Proceed with operation (y|n)? y
Rule deleted
[10/22/21]seed@Nikhil_PES1UG20CS821:~$
```

Full-screen Snip

Windows Taskbar: Type here to search, File, Internet Explorer, Chrome, File Explorer, File History, Task View, Taskbar icons, Weather (29°C Light rain), Date (5:11 PM 10/22/2021)

Now we ping the www.google.com to obtain the IP address of it



vm1 [Running] - Oracle VM VirtualBox

```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To           Action      From
--          ----      --
23          DENY OUT    10.0.2.8

[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw delete 1
Deleting:
  deny out from 10.0.2.8 to any port 23
Proceed with operation (y|n)? y
Rule deleted
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ ping www.google.com
PING www.google.com (216.58.196.164) 56(84) bytes of data.
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=1 ttl=117 time=11.9 ms
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=2 ttl=117 time=9.50 ms
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=3 ttl=117 time=10.6 ms
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=4 ttl=117 time=10.5 ms
^Z
[1]+  Stopped                  ping www.google.com
[10/22/21]seed@Nikhil_PES1UG20CS821:~$
```

Full-screen Snip

Windows Taskbar: Type here to search, File, Internet Explorer, Chrome, File Explorer, File History, Task View, Taskbar icons, Weather (29°C Light rain), Date (5:13 PM 10/22/2021)

After obtaining the ip address by pinging use to add rule so that we can block to visit that site.

```
vm1 [Running] - Oracle VM VirtualBox
Terminal
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To           Action     From
--          -----    ---
23          DENY OUT   10.0.2.8

[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw delete 1
Deleting:
  deny out from 10.0.2.8 to any port 23
Proceed with operation (y|n)? y
Rule deleted
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ ping www.google.com
PING www.google.com (216.58.196.164) 56(84) bytes of data.
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=1 ttl=117 time=11.9 ms
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=2 ttl=117 time=9.50 ms
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=3 ttl=117 time=10.6 ms
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=4 ttl=117 time=10.5 ms
^Z
[1]+  Stopped                  ping www.google.com
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny out to 216.58.196.164
Rule added
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To           Action     From
--          -----    ---
216.58.196.164        DENY OUT   Anywhere

[10/22/21]seed@Nikhil_PES1UG20CS821:~$ █
```

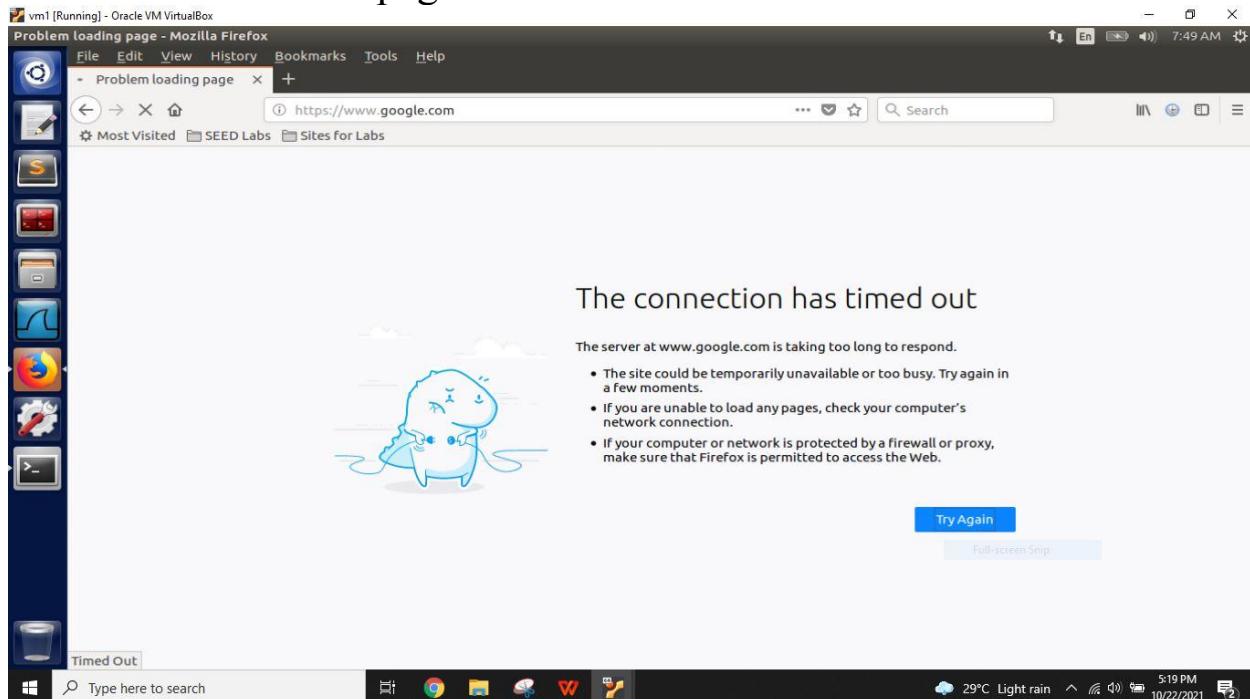
After adding the rule try to ping the same website and we will get operation not permitted as that site is being blocked

```
vm1 [Running] - Oracle VM VirtualBox
Terminal
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw delete 1
Deleting:
  deny out from 10.0.2.8 to any port 23
Proceed with operation (y|n)? y
Rule deleted
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ ping www.google.com
PING www.google.com (216.58.196.164) 56(84) bytes of data.
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=1 ttl=117 time=11.9 ms
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=2 ttl=117 time=9.50 ms
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=3 ttl=117 time=10.6 ms
64 bytes from maa03s31-in-f4.1e100.net (216.58.196.164): icmp_seq=4 ttl=117 time=10.5 ms
^Z
[1]+  Stopped                  ping www.google.com
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny out to 216.58.196.164
Rule added
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

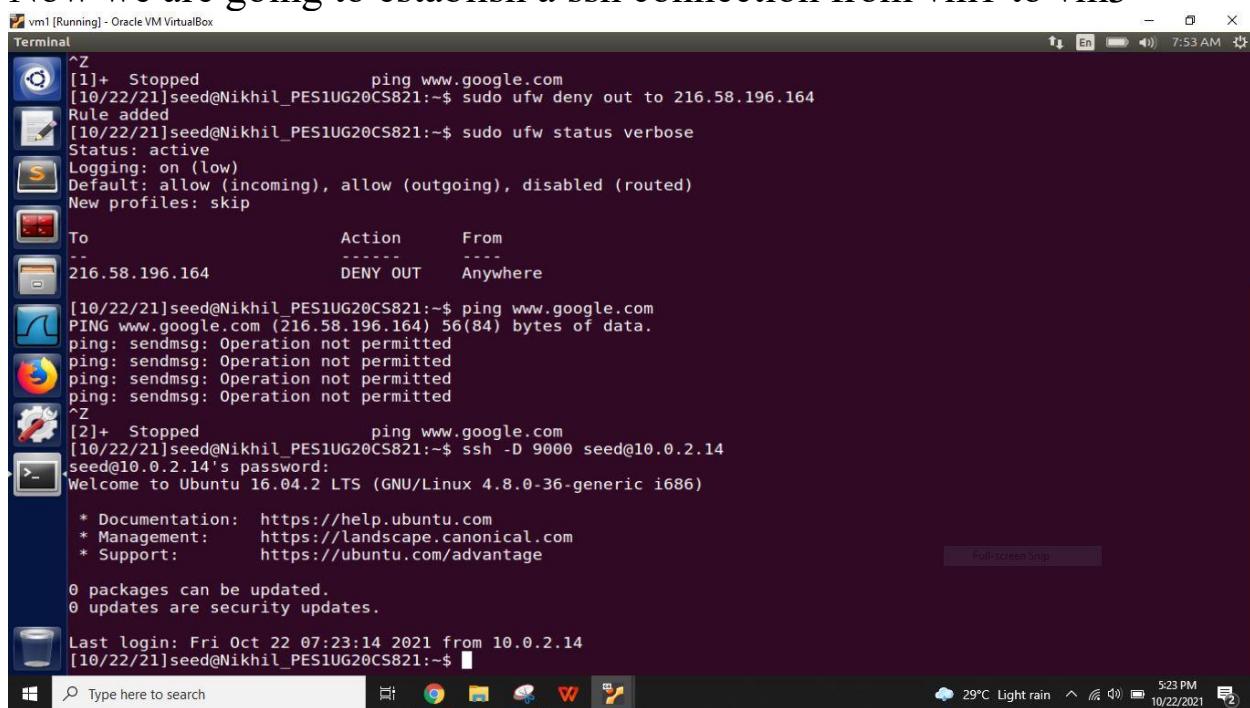
To           Action     From
--          -----    ---
216.58.196.164        DENY OUT   Anywhere

[10/22/21]seed@Nikhil_PES1UG20CS821:~$ ping www.google.com
PING www.google.com (216.58.196.164) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
^Z
[2]+  Stopped                  ping www.google.com
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ █
```

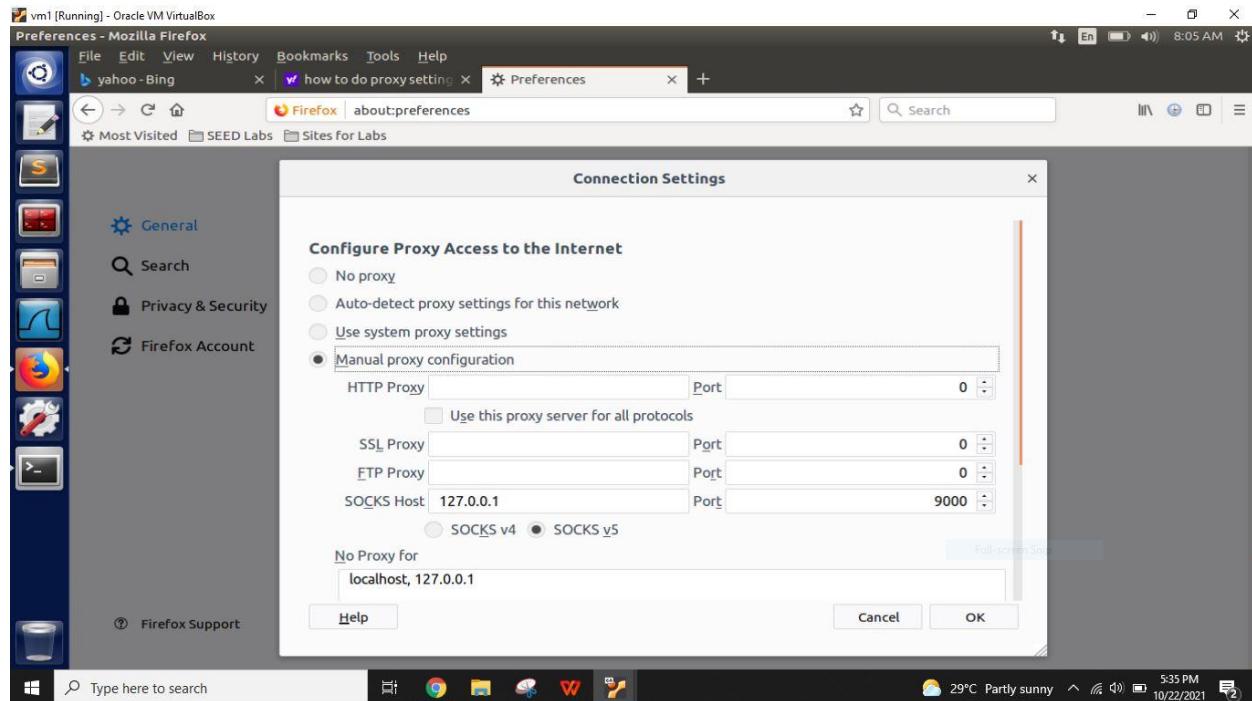
Later we visit the same site through browser and we can see the browser fails to load that web page



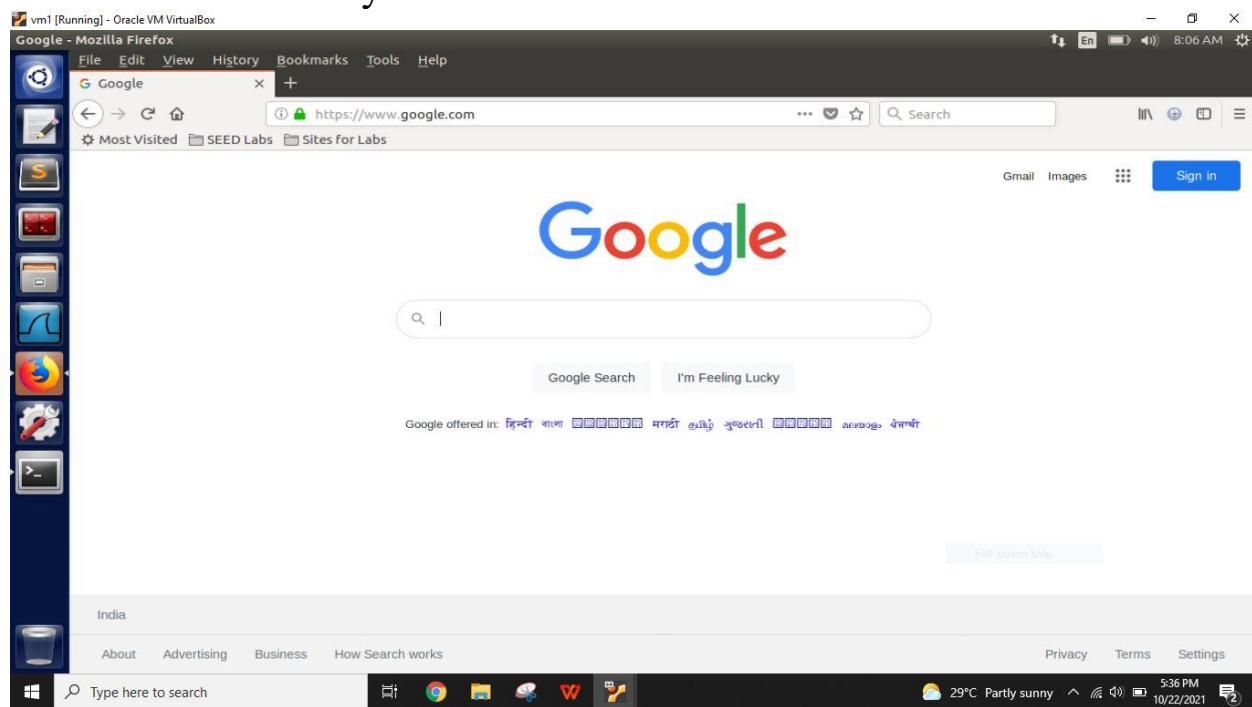
Now we are going to establish a ssh connection from vm1 to vm3



After successful ssh connection we are going to add manual proxy in the browser of vm1 as follows



After adding the proxy we can see that the web page [www.google..com](https://www.google.com) is loaded successfully



We can see the observation in vm1 wireshark which consists of tcp and ssh protocols with vm3

This screenshot shows a Wireshark capture from vm1. The packet list pane displays numerous TCP and SSH frames. A selected frame (Frame 10) is shown in the details, bytes, and hex panes. The details pane shows the following information for Frame 10:

- Source Port: 9000
- Destination Port: 44890
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence number: 3322084316
- Acknowledgment number: 3213428956
- Header Length: 32 bytes
- Flags: 0x10 (ACK)
- Window size value: 342
- [Calculated window size: 43776]
- [Window size scaling factor: 128]
- CHECKSUM: 0xfe28 [unverified]
- [Checksum Status: Unverified]

Same observation can be seen in vm3 with vm1

This screenshot shows a Wireshark capture from vm3. The packet list pane displays numerous TCP and SSH frames. A selected frame (Frame 14) is shown in the details, bytes, and hex panes. The details pane shows the following information for Frame 14:

- Source Port: 33600
- Destination Port: 22
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence number: 563009366
- Acknowledgment number: 1463198931
- Header Length: 32 bytes
- Flags: 0x10 (ACK)
- Window size value: 2085
- [Calculated window size: 2085]

After we gets disconnect from the ssh connection in the vm1

vm1 [Running] - Oracle VM VirtualBox

Terminal

```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ ssh -D 9000 seed@10.0.2.14
seed@10.0.2.14's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

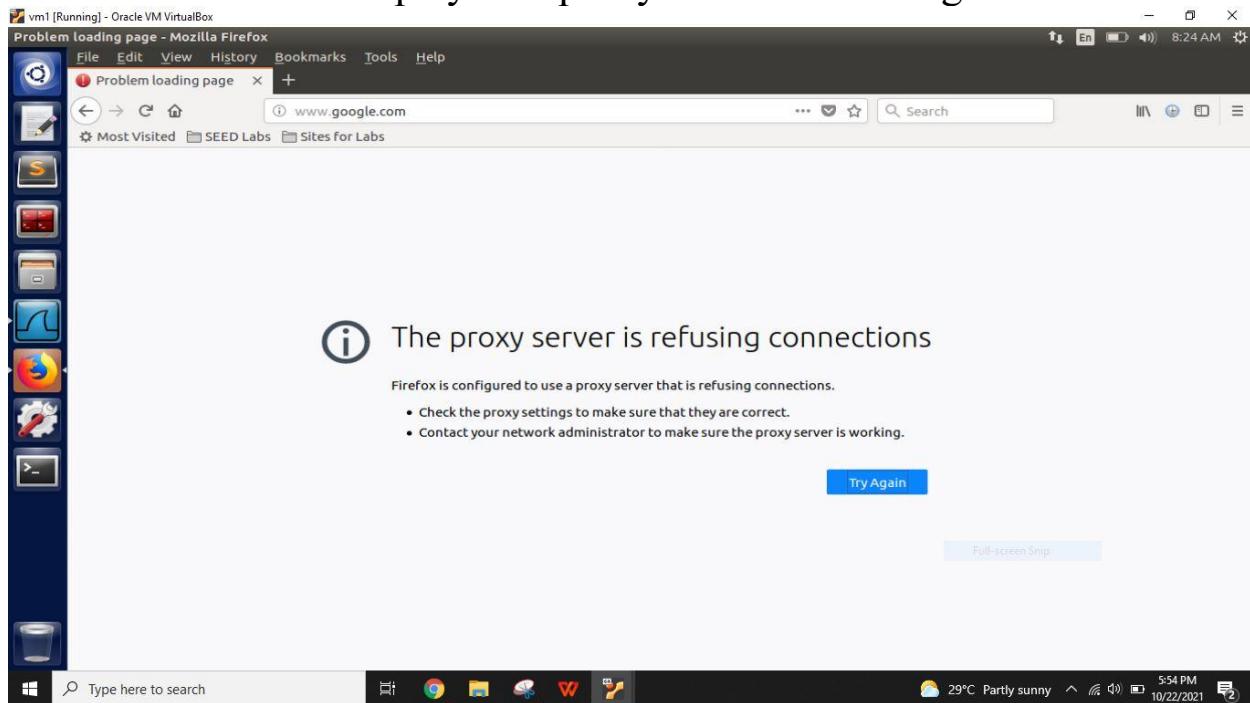
0 packages can be updated.
0 updates are security updates.

Last login: Fri Oct 22 07:52:22 2021 from 10.0.2.8
[10/22/21]seed@Nikhil_PES1UG20CS821:~$
```

Type here to search

29°C Partly sunny 5:43 PM 10/22/2021

After getting disconnected from the ssh connection we are going to load that webpage again in the browser by clearing the cache and history.we can observe that it displays the proxy server is refusing connections



Now again we establish the ssh connection

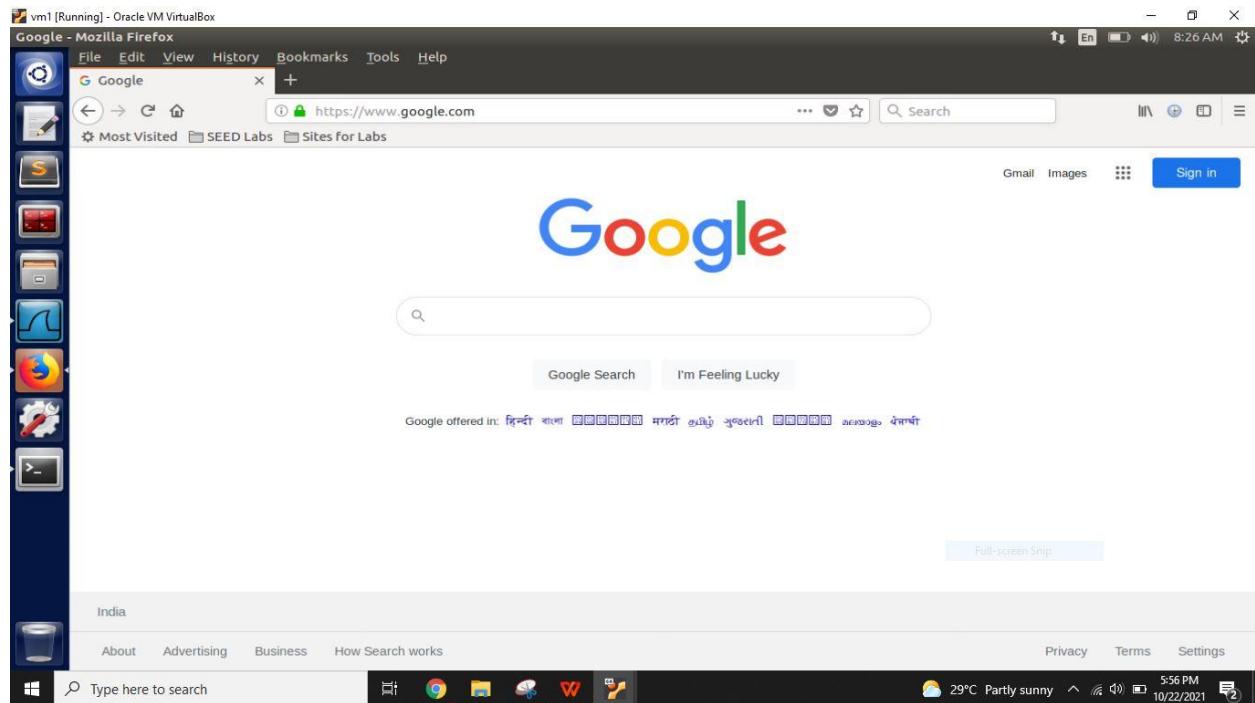
```
[10/22/21]seed@Nikhil_PES1UG20CS821:~$ ssh -D 9000 seed@10.0.2.14
seed@10.0.2.14's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Fri Oct 22 08:13:36 2021 from 10.0.2.8
[10/22/21]seed@Nikhil_PES1UG20CS821:~$
```

We reload the same page again and we can access the web page after the ssh connection



Task 4: Evade Ingress Filtering

Delete all the previous rules we added for the previous tasks

vm1 [Running] - Oracle VM VirtualBox
Terminal
[10/23/21]seed@Nikhil_PES1UG20CS821:~\$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To Action From

216.58.196.164 DENY OUT Anywhere
[10/23/21]seed@Nikhil_PES1UG20CS821:~\$ sudo ufw delete 1
Deleting:
deny out to 216.58.196.164
Proceed with operation (y|n)? y
Rule deleted
[10/23/21]seed@Nikhil_PES1UG20CS821:~\$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[10/23/21]seed@Nikhil_PES1UG20CS821:~\$ █

The screenshot shows a Linux desktop environment with a terminal window open in the background. The terminal window displays the command `sudo ufw status verbose` followed by the output of the UFW status. It then shows the command `sudo ufw delete 1` being run, which removes a rule deny out to 216.58.196.164. The desktop interface includes a taskbar with various icons and a system tray at the bottom.

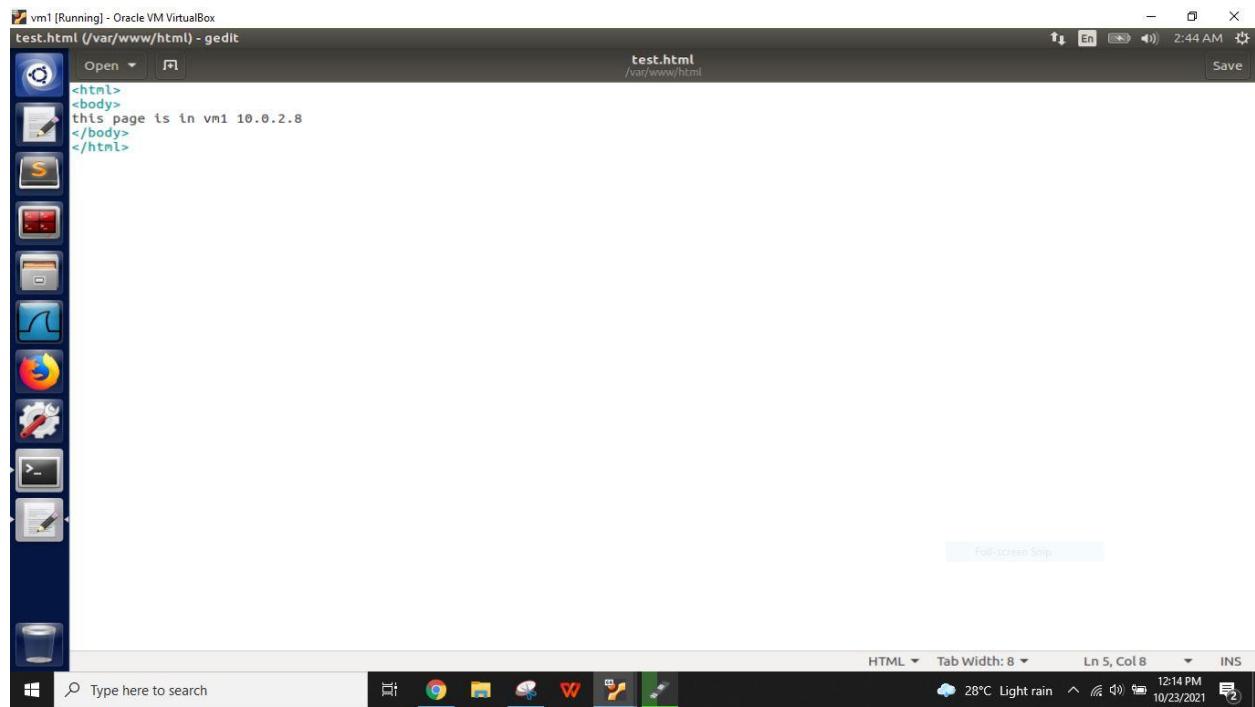
Create a new file named as test.html in the path var/www/html

vm1 [Running] - Oracle VM VirtualBox
Terminal
[10/23/21]seed@Nikhil_PES1UG20CS821:~\$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To Action From

216.58.196.164 DENY OUT Anywhere
[10/23/21]seed@Nikhil_PES1UG20CS821:~\$ sudo ufw delete 1
Deleting:
deny out to 216.58.196.164
Proceed with operation (y|n)? y
Rule deleted
[10/23/21]seed@Nikhil_PES1UG20CS821:~\$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[10/23/21]seed@Nikhil_PES1UG20CS821:~\$ cd /var/www/html/
[10/23/21]seed@Nikhil_PES1UG20CS821:~/html\$ ls
index.html
[10/23/21]seed@Nikhil_PES1UG20CS821:~/html\$ sudo gedit test.html
(gedit:3092): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3092): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3092): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3092): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/23/21]seed@Nikhil_PES1UG20CS821:~/html\$

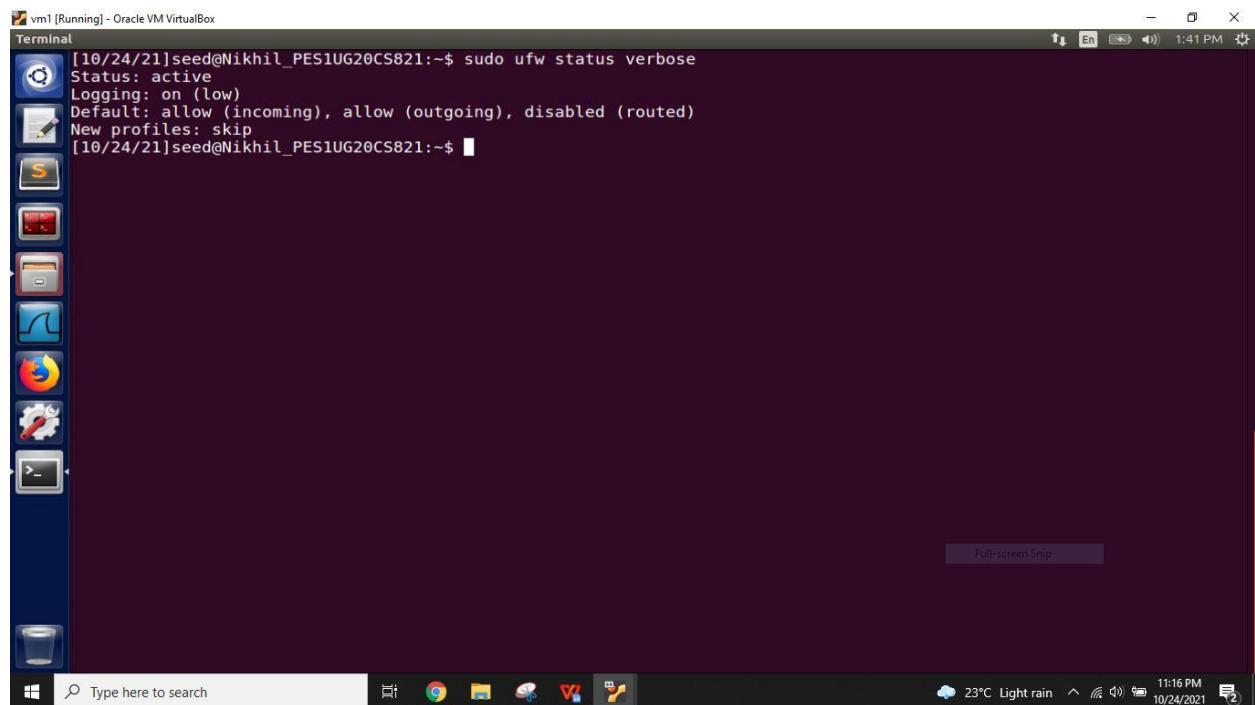
The screenshot shows a Linux desktop environment with a terminal window open in the background. The terminal window displays the command `sudo ufw status verbose` followed by the output of the UFW status. It then shows the command `cd /var/www/html/` being run, followed by `ls` which lists the file `index.html`. Finally, the command `sudo gedit test.html` is run, opening a new file named `test.html` in the Gedit text editor. The desktop interface includes a taskbar with various icons and a system tray at the bottom.

The content of the file test.html is as shown below



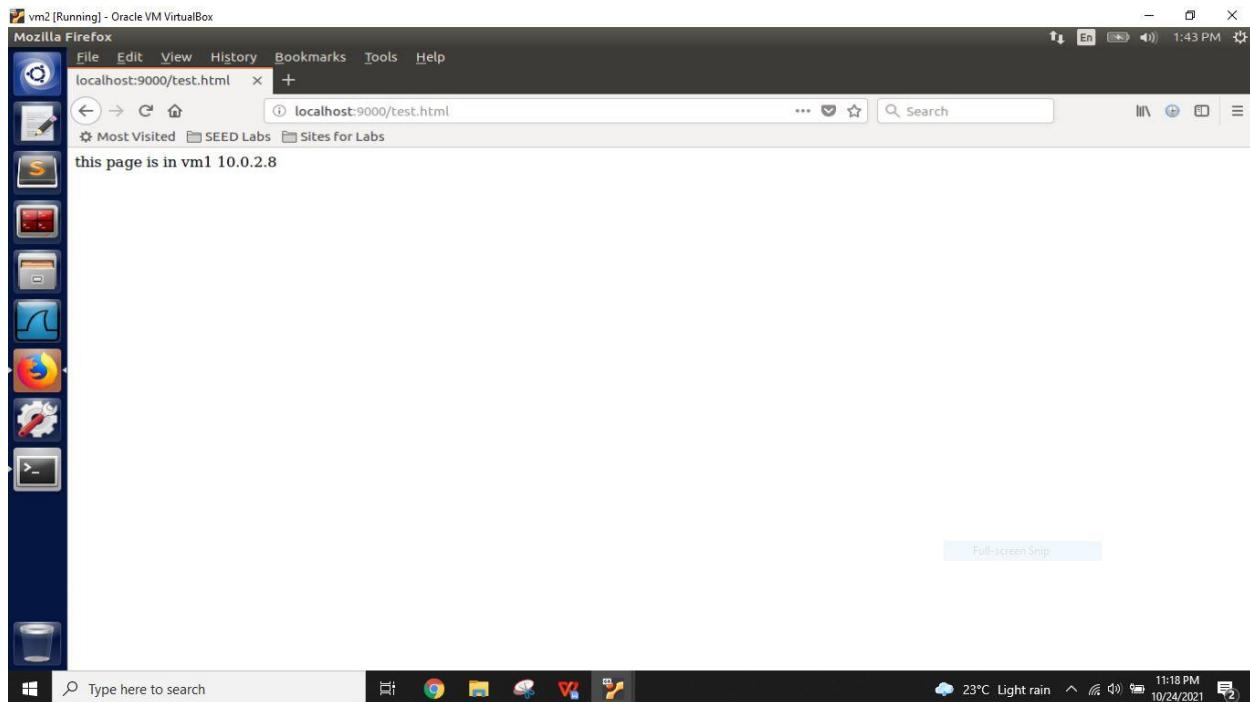
```
<html>
<body>
this page is in vm1 10.0.2.8
</body>
</html>
```

Now there is no firewall rules in the vm1

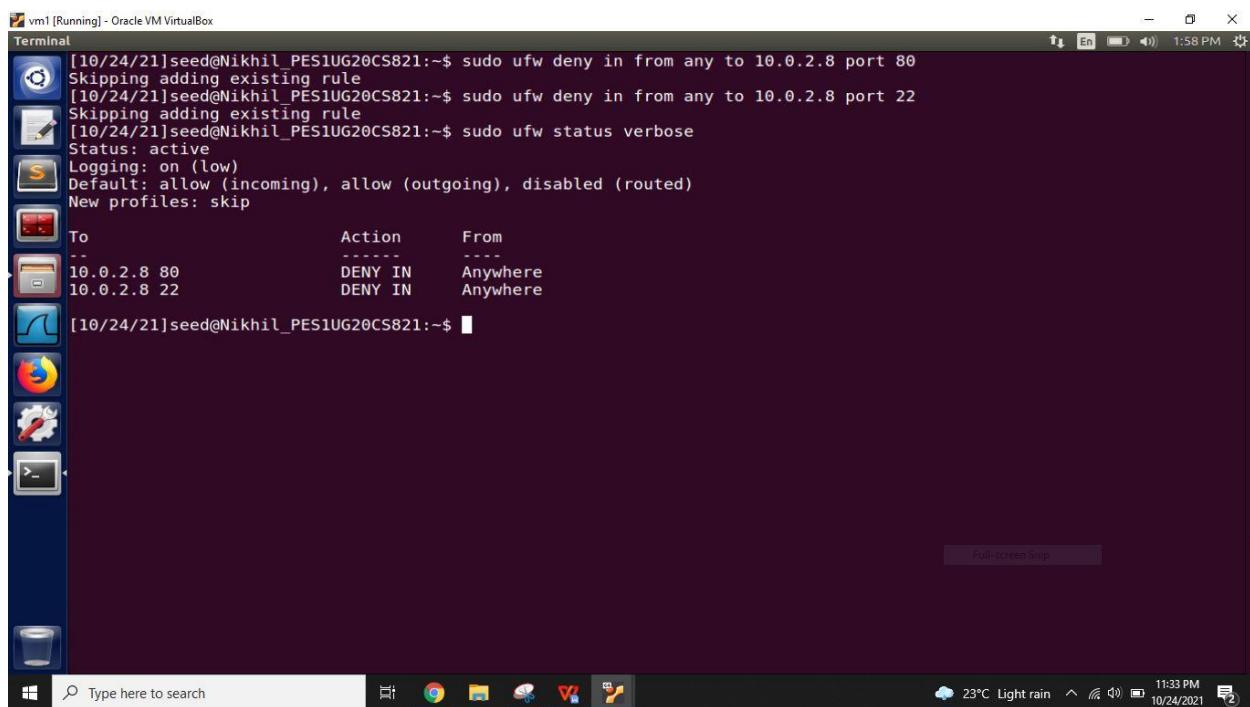


```
[10/24/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[10/24/21]seed@Nikhil_PES1UG20CS821:~$
```

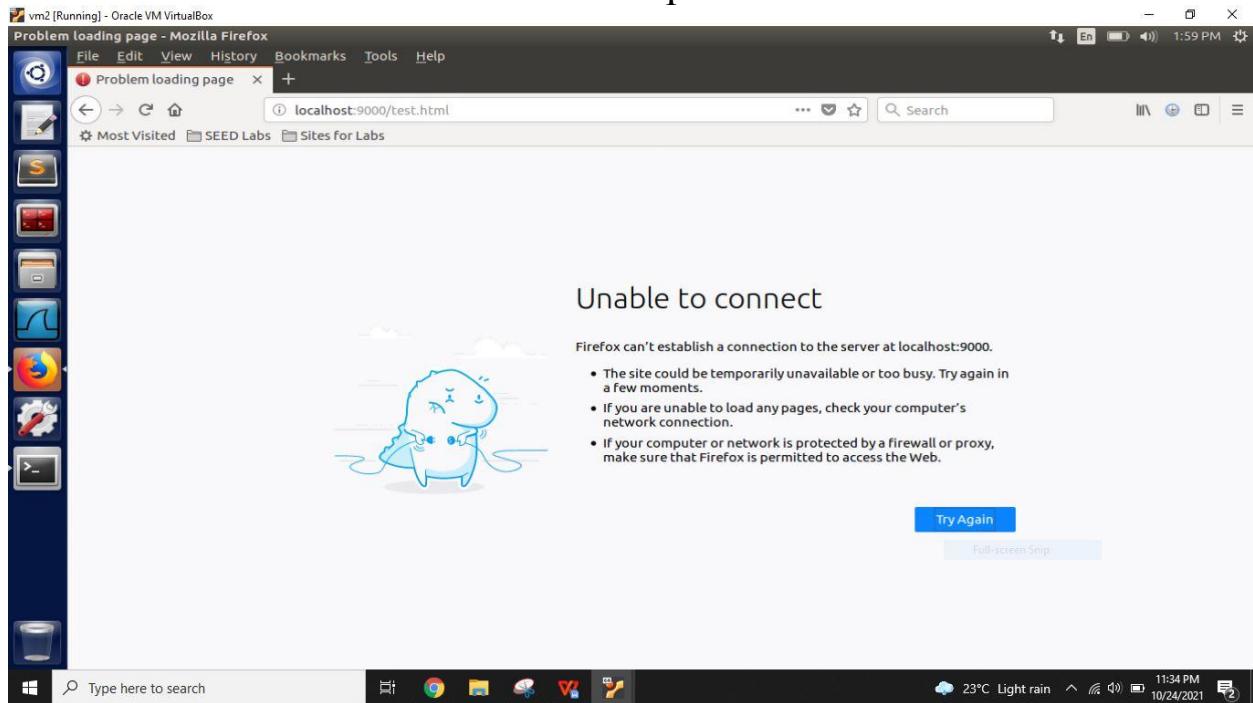
Because of there is no rules in the vm1 we can access the web page that is present in the vm1 from vm2 through the browser



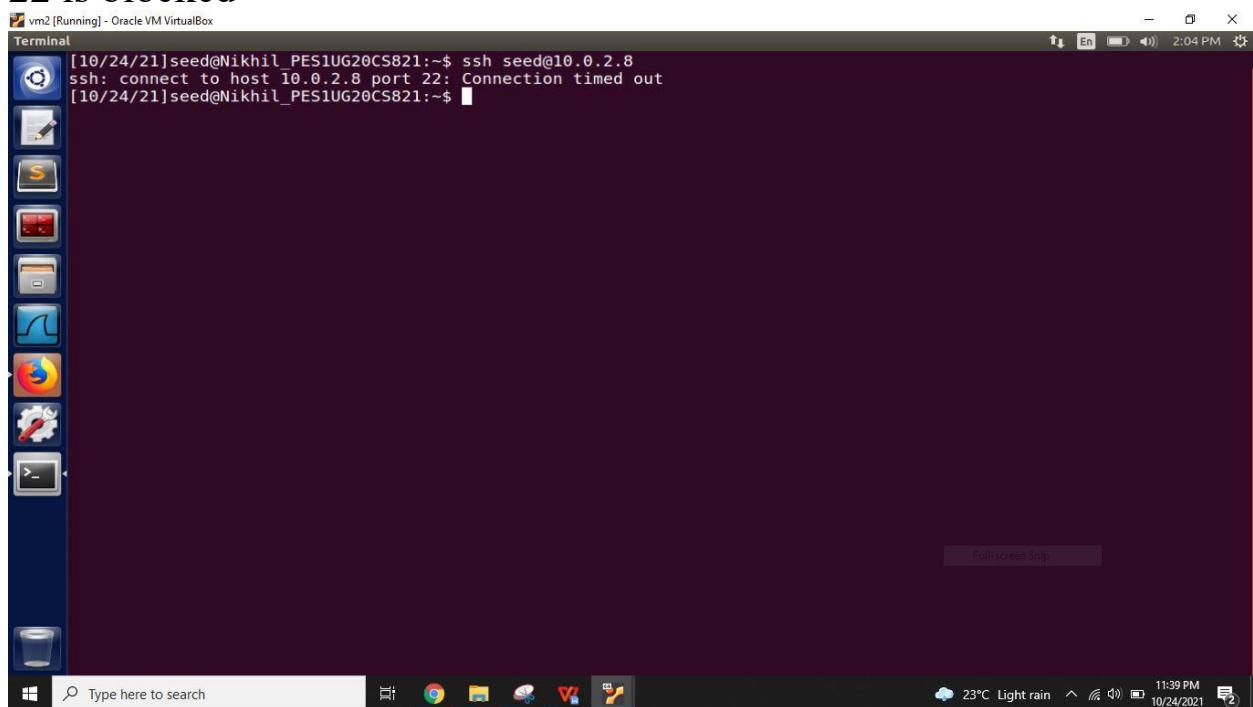
Now we add rules in the vm1 firewall to block the port 80 and 22



After adding the rules we go back to the vm2 and access the same file which is not able to access now as the port 80 from vm1 is blocked



Also we cannot establish a ssh connection to vm1 from vm2 as the port 22 is blocked



Now we perform reverse ssh from the vm1 to establish a reverse tunnel

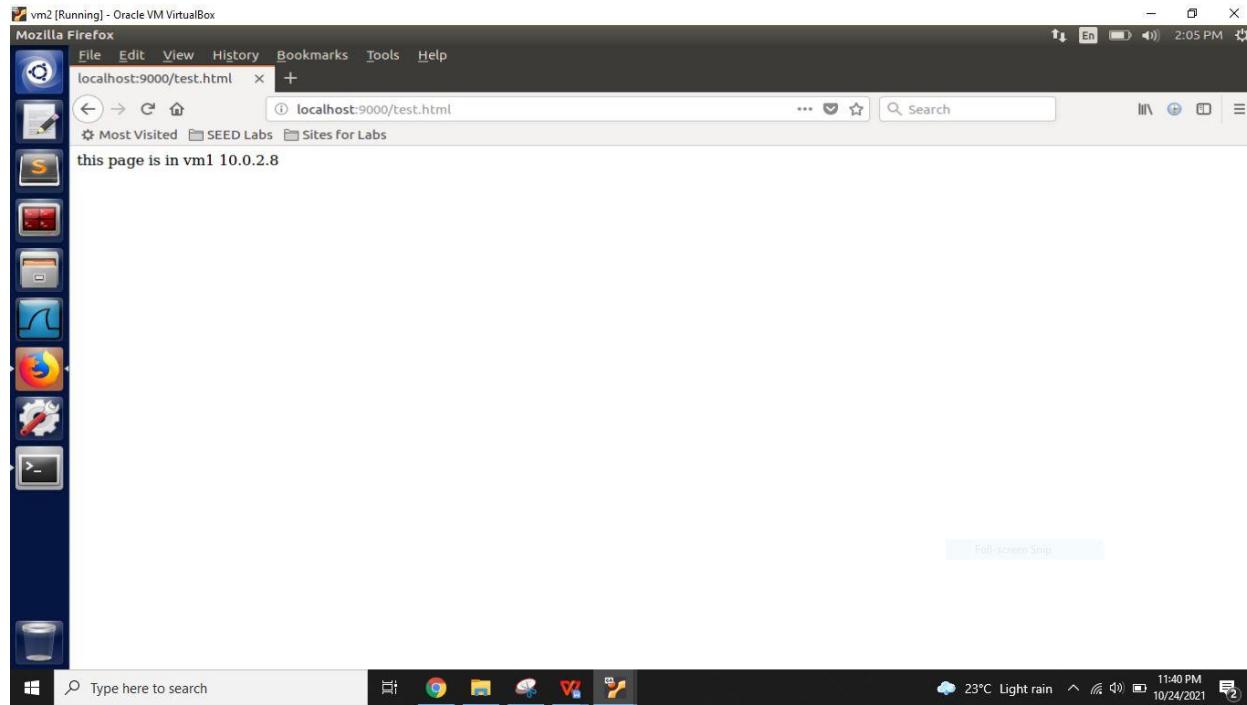
```
[10/24/21]seed@Nikhil_PESIUG20CS821:~$ sudo ufw deny in from any to 10.0.2.8 port 80
Skipping adding existing rule
[10/24/21]seed@Nikhil_PESIUG20CS821:~$ sudo ufw deny in from any to 10.0.2.8 port 22
Skipping adding existing rule
[10/24/21]seed@Nikhil_PESIUG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To Action From
-- ----
10.0.2.8 80 DENY IN Anywhere
10.0.2.8 22 DENY IN Anywhere
[10/24/21]seed@Nikhil_PESIUG20CS821:~$ ssh -R 9000:10.0.2.8:80 10.0.2.9
seed@10.0.2.9's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Sun Oct 24 13:56:03 2021 from 10.0.2.8
[10/24/21]seed@Nikhil_PESIUG20CS821:~$
```

With the tunnel connection we can access the webpage from the vm2 browser



Now we break the tunnel from vm1 to check whether we can access the file again from the vm2 browser

```
vm1 [Running] - Oracle VM VirtualBox
Terminal
[10/24/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny in from any to 10.0.2.8 port 80
Skipping adding existing rule
[10/24/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny in from any to 10.0.2.8 port 22
Skipping adding existing rule
[10/24/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To           Action      From
--          ----      ---
10.0.2.8 80    DENY IN    Anywhere
10.0.2.8 22    DENY IN    Anywhere
[10/24/21]seed@Nikhil_PES1UG20CS821:~$ ssh -R 9000:10.0.2.8:80 10.0.2.9
seed@10.0.2.9's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation: https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Sun Oct 24 13:56:03 2021 from 10.0.2.8
[10/24/21]seed@Nikhil_PES1UG20CS821:~$ exit
logout
Connection to 10.0.2.9 closed.
[10/24/21]seed@Nikhil_PES1UG20CS821:~$
```

We can see again we cannot access the web page from the from the vm2 browser after the tunnel is broken.

