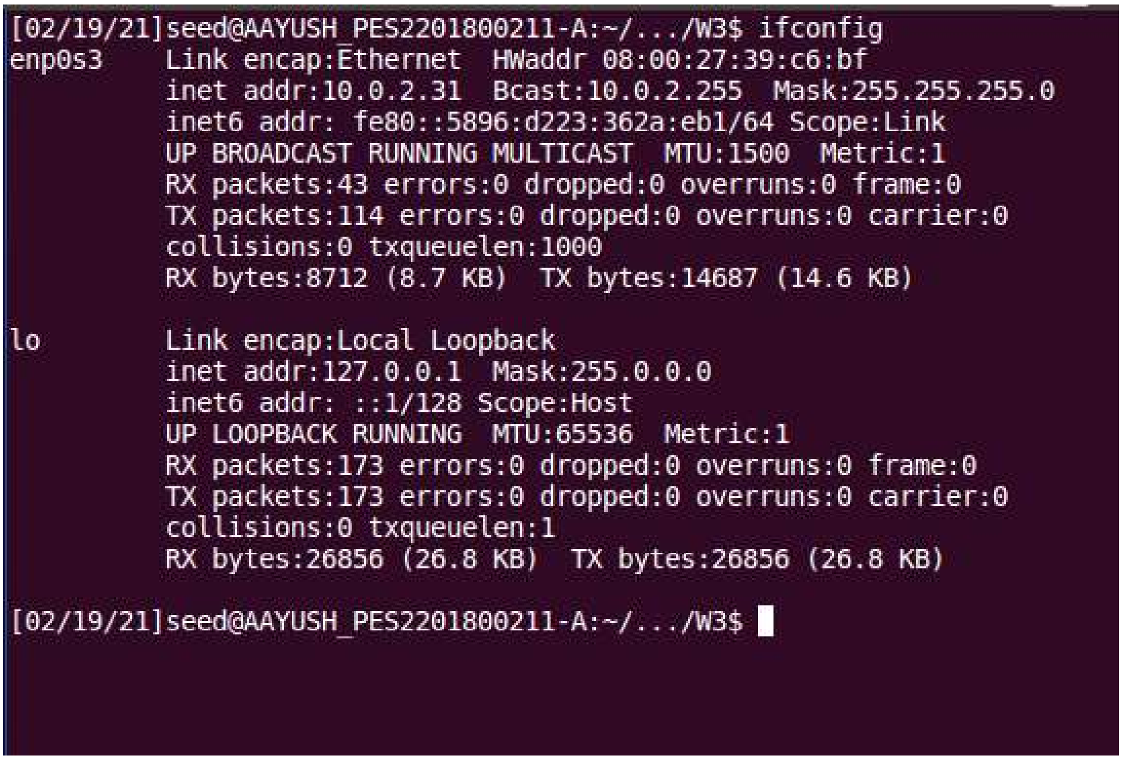
PES UNIVERSITY
INFORMATION SECURITY LAB
LAB 3 - FIREWALL

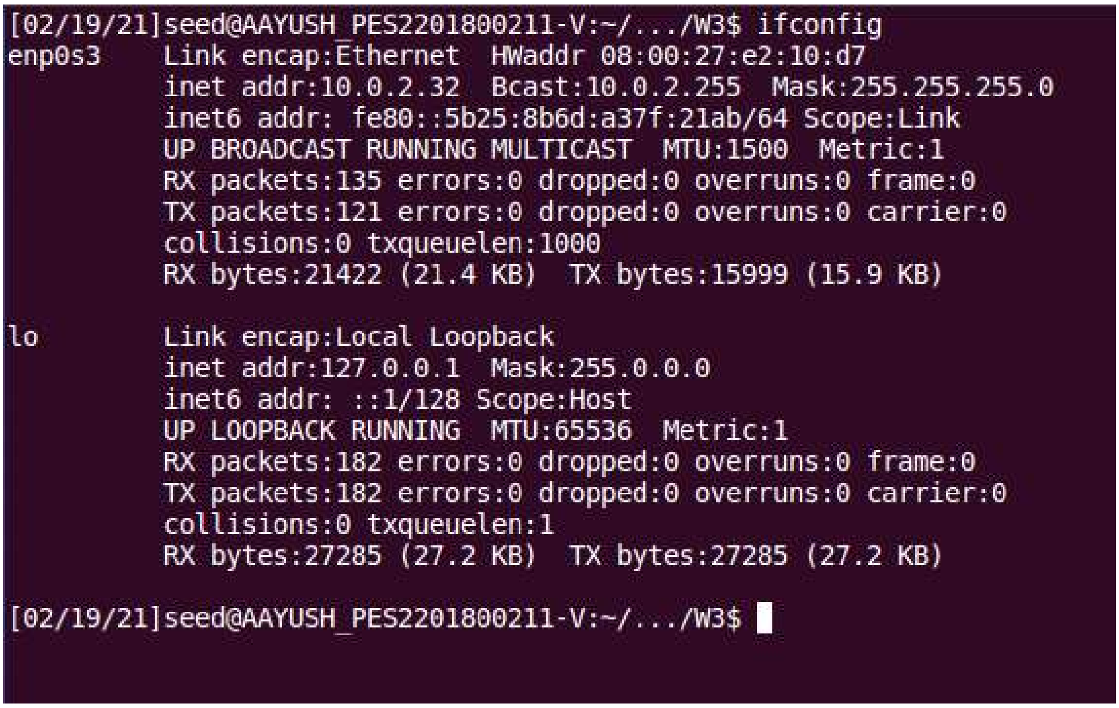
Aayush Kapoor PES2201800211

ATTACKER IP (VM 1)



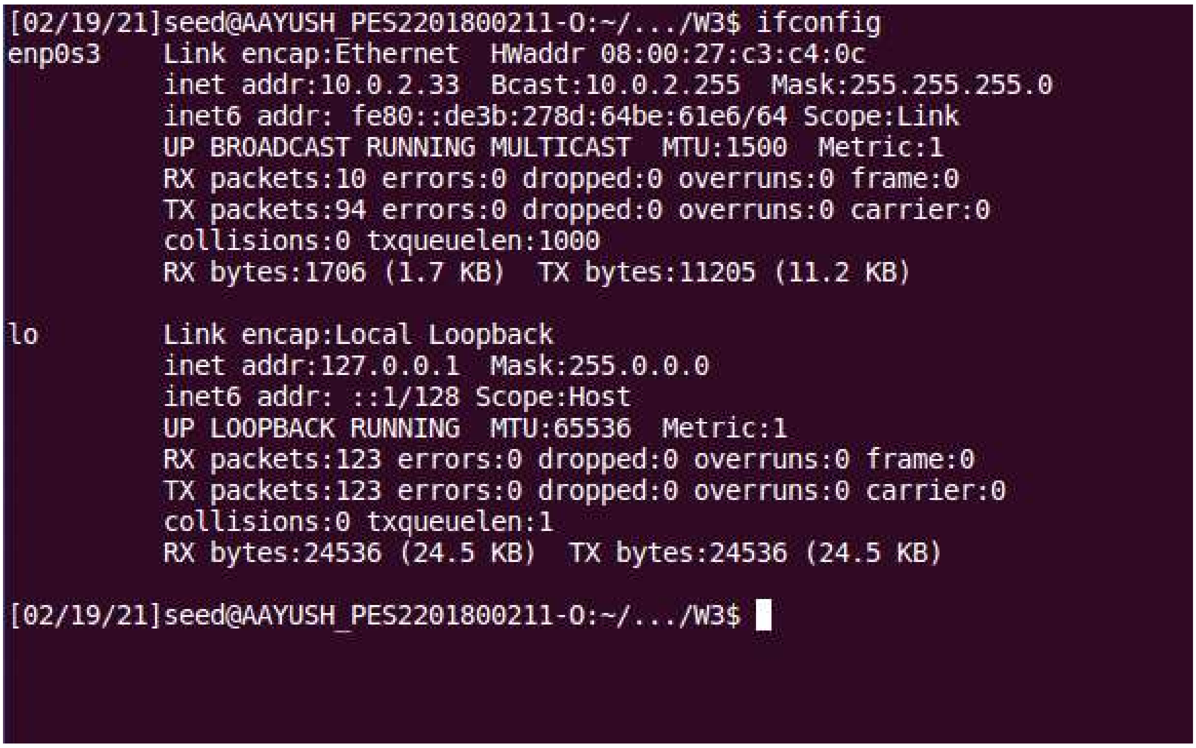
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:39:c6:bf
          inet addr:10.0.2.31  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::5896:d223:362a:eb1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8712 (8.7 KB)  TX bytes:14687 (14.6 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:173 errors:0 dropped:0 overruns:0 frame:0
          TX packets:173 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:26856 (26.8 KB)  TX bytes:26856 (26.8 KB)

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```

VICTIM IP (VM 2)



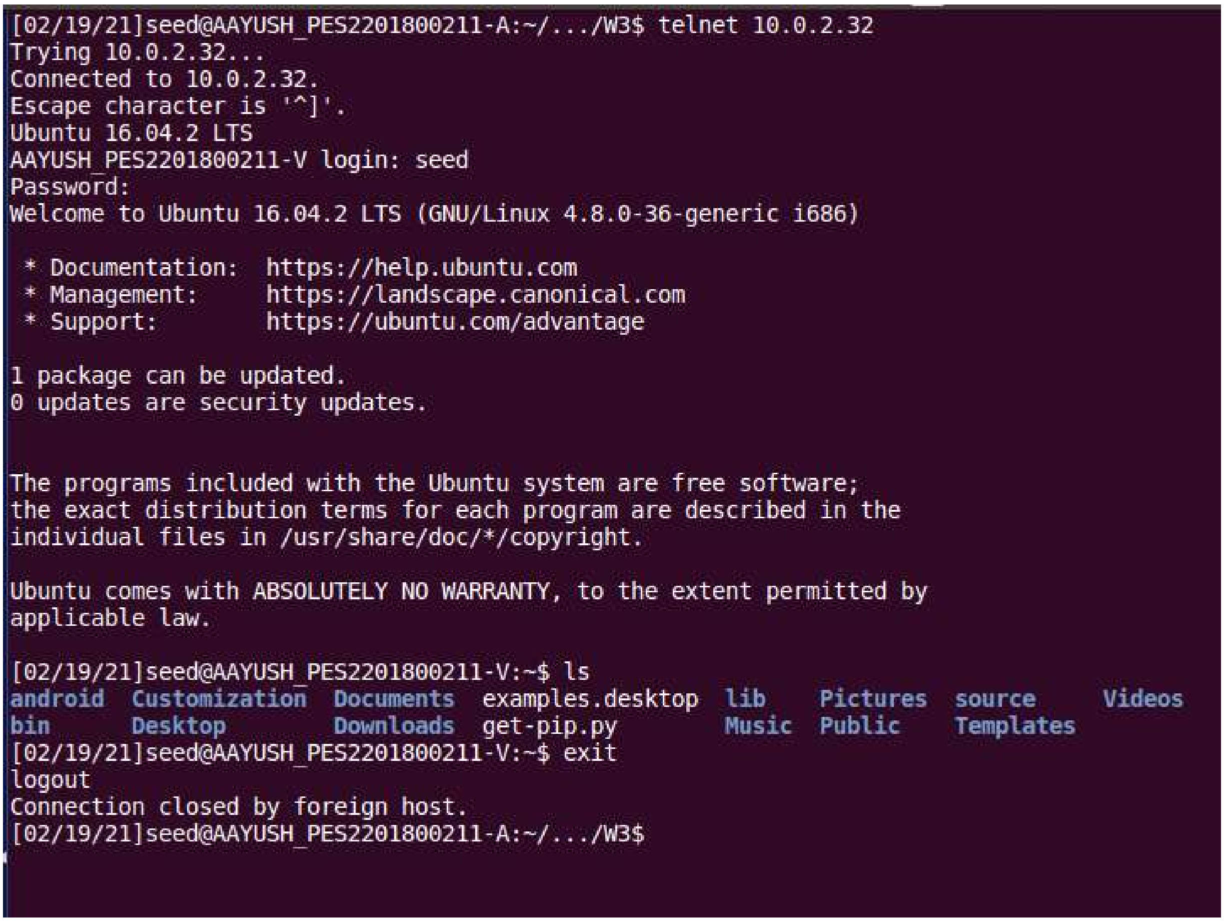
```
[02/19/21]seed@AAYUSH_PES2201800211-V:~/.../W3$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:e2:10:d7
          inet addr:10.0.2.32  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::5b25:8b6d:a37f:21ab/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21422 (21.4 KB)  TX bytes:15999 (15.9 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:182 errors:0 dropped:0 overruns:0 frame:0
          TX packets:182 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:27285 (27.2 KB)  TX bytes:27285 (27.2 KB)

[02/19/21]seed@AAYUSH_PES2201800211-V:~/.../W3$
```

OBSERVER IP (VM 3)



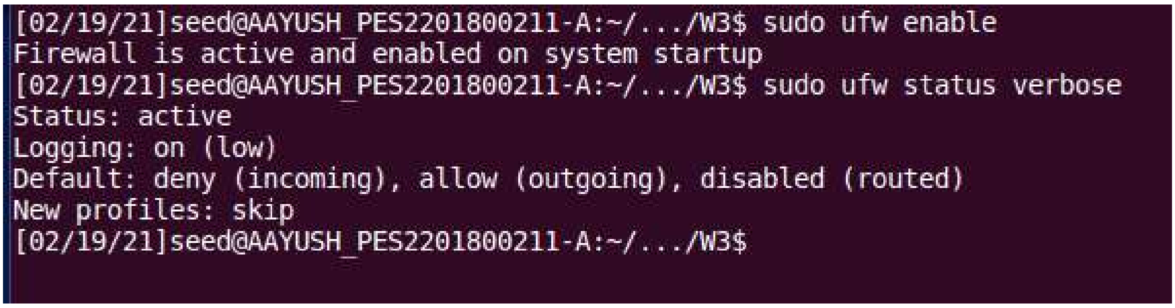
```
[02/19/21]seed@AAYUSH_PES2201800211-O:~/.../W3$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:c3:c4:0c
          inet addr:10.0.2.33  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::de3b:278d:64be:61e6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1706 (1.7 KB)  TX bytes:11205 (11.2 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:123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:24536 (24.5 KB)  TX bytes:24536 (24.5 KB)

[02/19/21]seed@AAYUSH_PES2201800211-O:~/.../W3$
```

TASK 1:



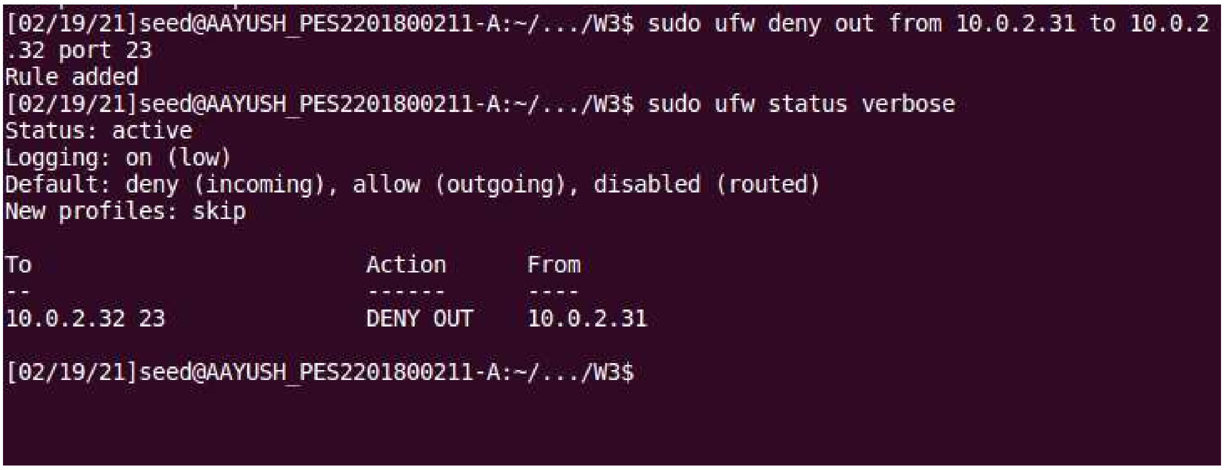
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ telnet 10.0.2.32
Trying 10.0.2.32...
Connected to 10.0.2.32.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
AAYUSH_PES2201800211-V login: seed
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[02/19/21]seed@AAYUSH_PES2201800211-V:~$ ls
android  Customization  Documents  examples.desktop  lib    Pictures  source     Videos
bin      Desktop        Downloads  get-pip.py        Music  Public    Templates
[02/19/21]seed@AAYUSH_PES2201800211-V:~$ exit
logout
Connection closed by foreign host.
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```

First we try to telnet from VM1 to VM2 - Successful connection.



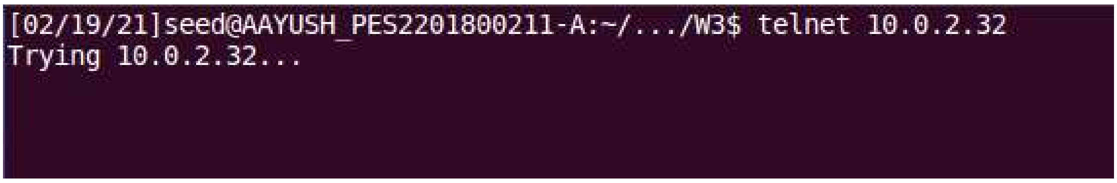
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw enable
Firewall is active and enabled on system startup
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```

Now, we enable UFW (Uncomplicated Firewall) and check the status of it.



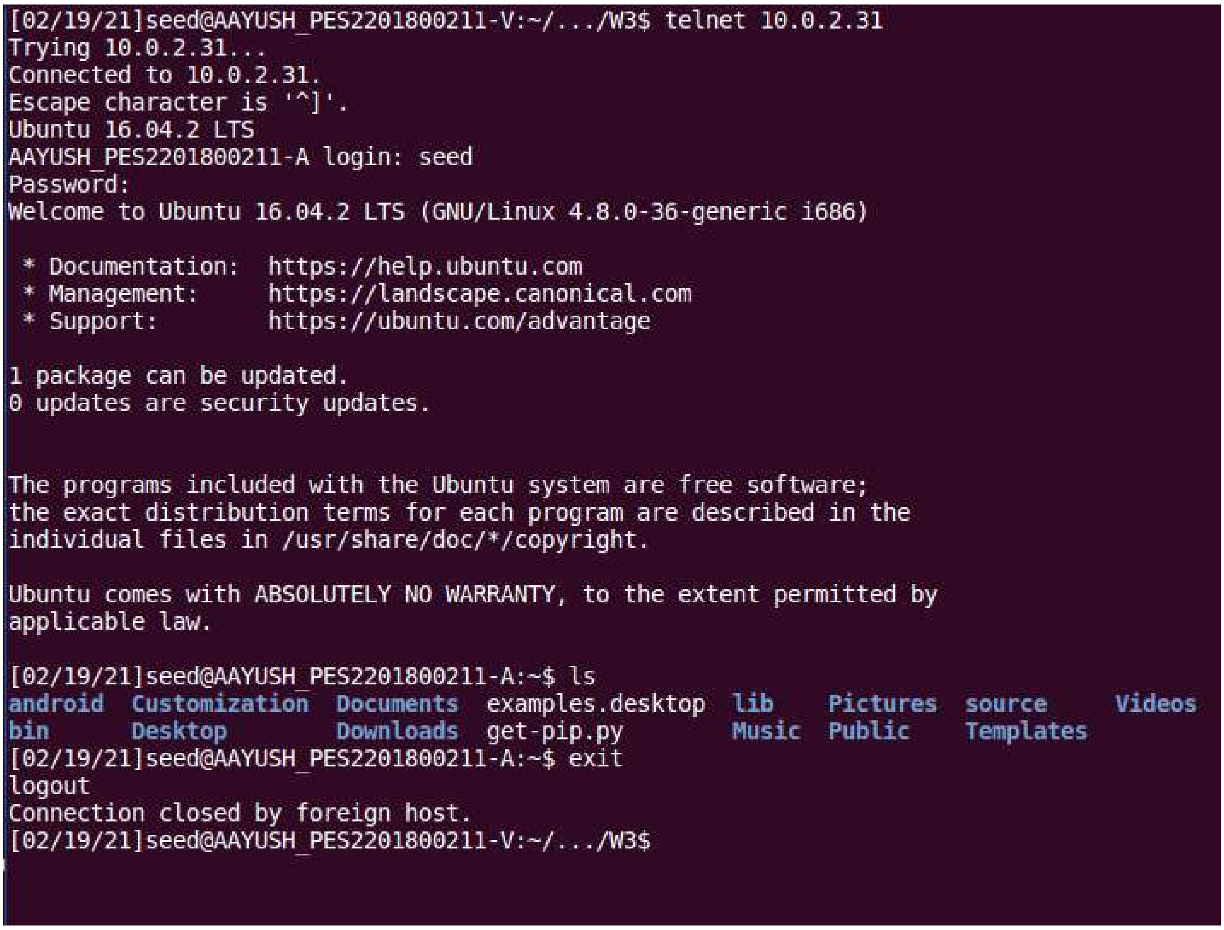
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw deny out from 10.0.2.31 to 10.0.2
.32 port 23
Rule added
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
10.0.2.32 23               DENY OUT    10.0.2.31

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```

Here, we setup firewall using UFW to prevent VM1 from telnetting to VM2.



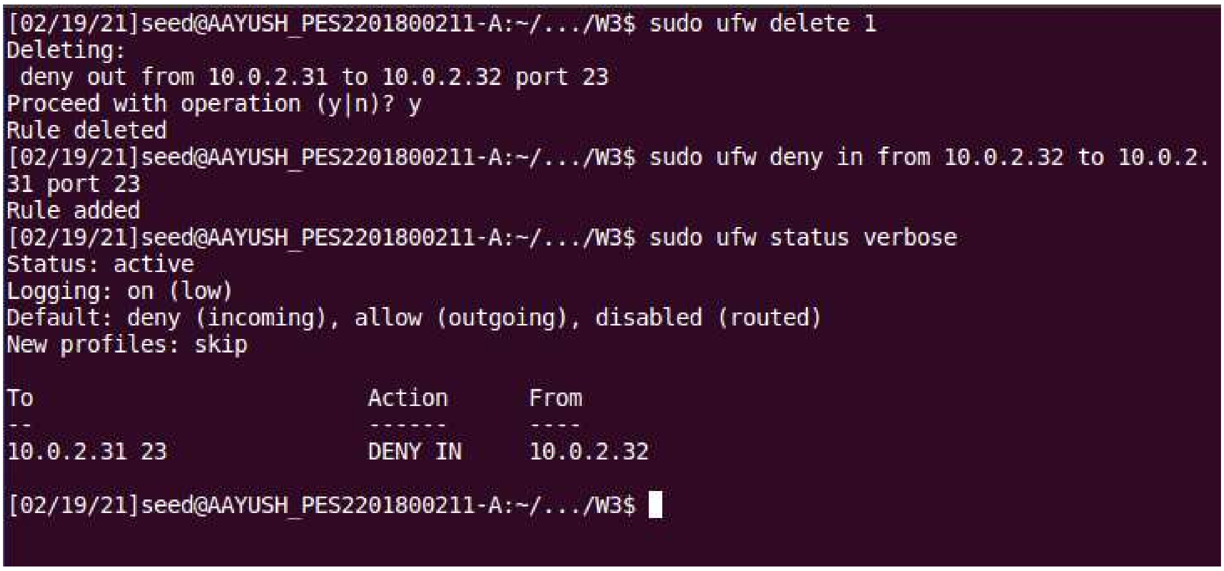
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ telnet 10.0.2.32
Trying 10.0.2.32...
```

On trying it, we see that the telnet was unsuccessful.



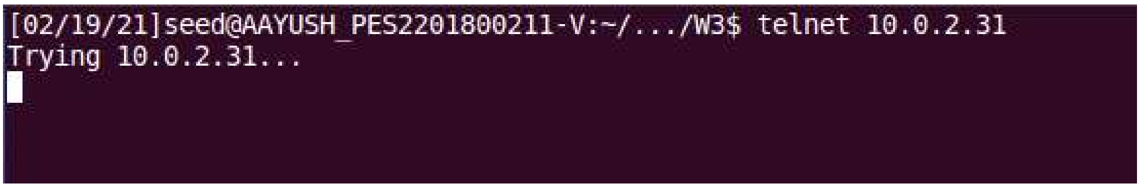
```
[02/19/21]seed@AAYUSH_PES2201800211-V:~/.../W3$ telnet 10.0.2.31
Trying 10.0.2.31...
Connected to 10.0.2.31.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
AAYUSH_PES2201800211-A login: seed
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[02/19/21]seed@AAYUSH_PES2201800211-A:~$ ls
android  Customization  Documents  examples.desktop  lib    Pictures  source     Videos
bin      Desktop        Downloads  get-pip.py        Music  Public    Templates
[02/19/21]seed@AAYUSH_PES2201800211-A:~$ exit
logout
Connection closed by foreign host.
[02/19/21]seed@AAYUSH_PES2201800211-V:~/.../W3$
```

Same as above, now we do it from VM2 to VM1 and see that it is possible as the rule was from VM1 to VM2 prevention.



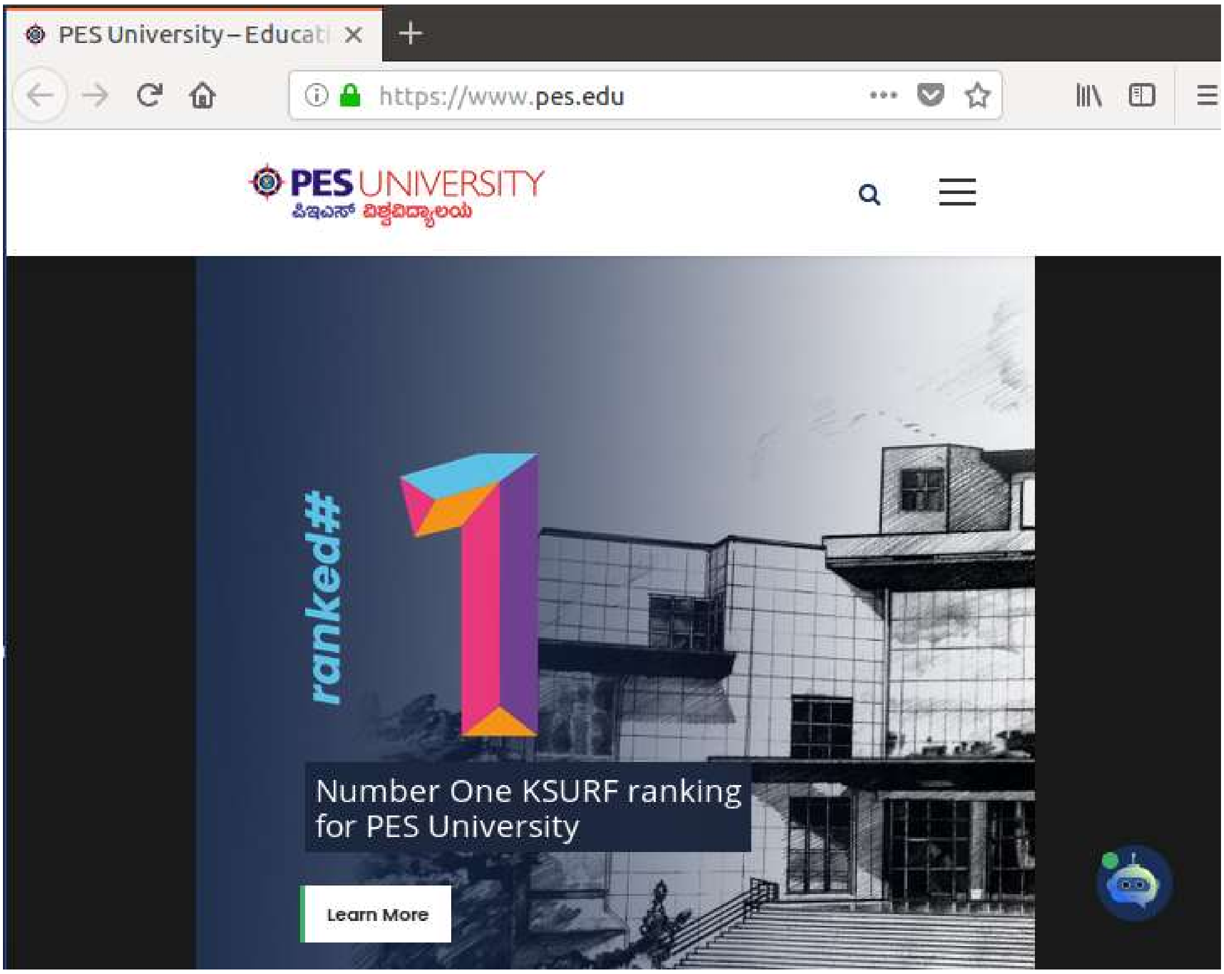
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw delete 1
Deleting:
 deny out from 10.0.2.31 to 10.0.2.32 port 23
Proceed with operation (y|n)? y
Rule deleted
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw deny in from 10.0.2.32 to 10.0.2.
31 port 23
Rule added
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
10.0.2.31 23               DENY IN     10.0.2.32

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ 
```

On deleting previous rule and adding rule to prevent it from VM2 to VM1.

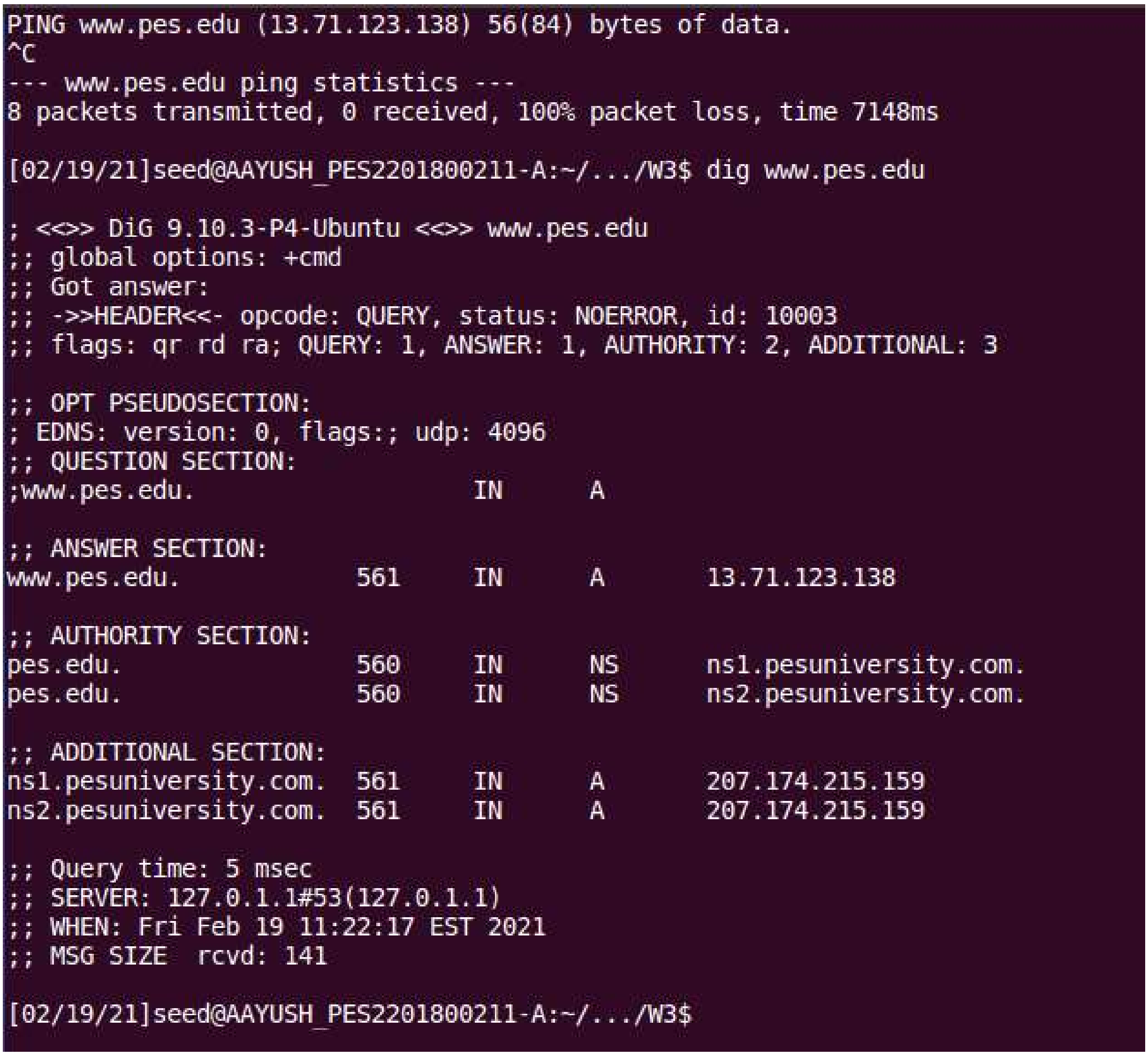


```
[02/19/21]seed@AAYUSH_PES2201800211-V:~/.../W3$ telnet 10.0.2.31
Trying 10.0.2.31...
```

Again on telnetting from VM2 to VM1, it was unsuccessful.

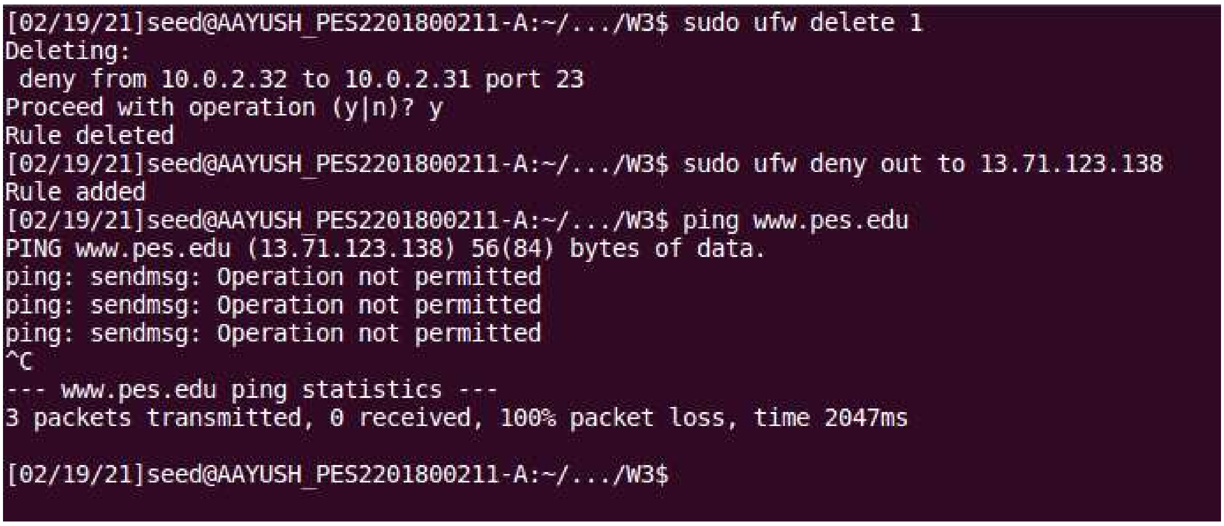


For task 1 part 3, we check whether we are able to reach the pes.edu web page. Above we see that we are able to load the site.

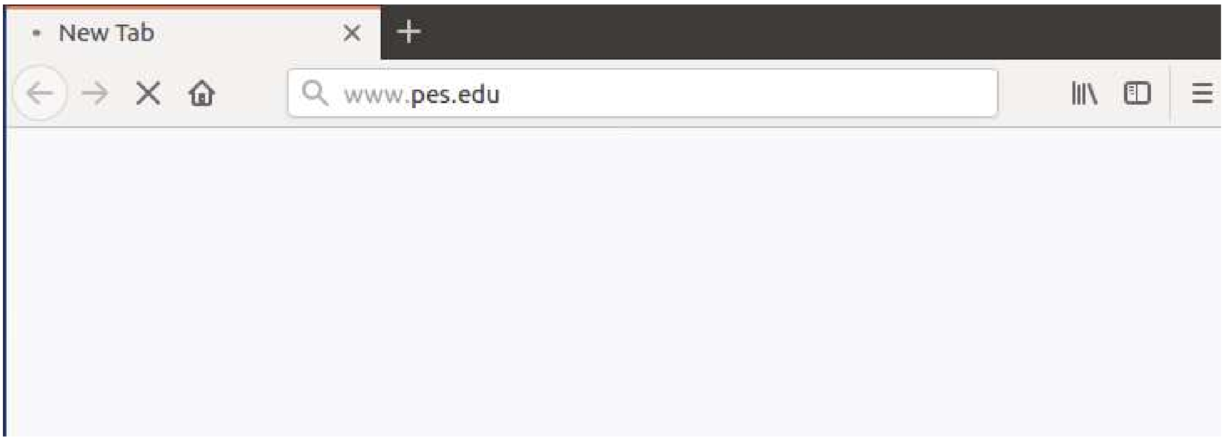


```
PING www.pes.edu (13.71.123.138) 56(84) bytes of data.
^C
--- www.pes.edu ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7148ms

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ dig www.pes.edu

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.pes.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10003
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.pes.edu.                   IN      A

;; ANSWER SECTION:
www.pes.edu.            561     IN      A       13.71.123.138

;; AUTHORITY SECTION:
pes.edu.                560     IN      NS      ns1.pesuniversity.com.
pes.edu.                560     IN      NS      ns2.pesuniversity.com.

;; ADDITIONAL SECTION:
ns1.pesuniversity.com.  561     IN      A       207.174.215.159
ns2.pesuniversity.com.  561     IN      A       207.174.215.159

;; Query time: 5 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Feb 19 11:22:17 EST 2021
;; MSG SIZE  rcvd: 141

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```

We are also able to ping www.pes.edu and later using dig command we get the IP of the site.



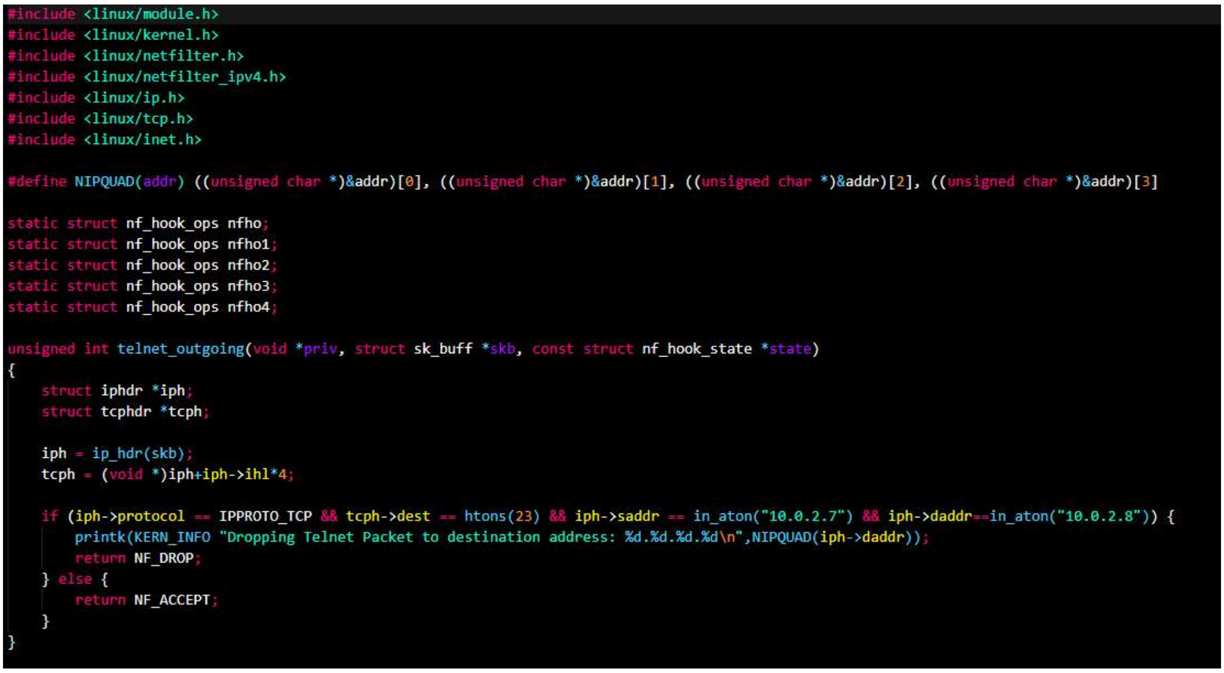
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw delete 1
Deleting:
 deny from 10.0.2.32 to 10.0.2.31 port 23
Proceed with operation (y|n)? y
Rule deleted
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw deny out to 13.71.123.138
Rule added
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ping www.pes.edu
PING www.pes.edu (13.71.123.138) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- www.pes.edu ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2047ms

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```



After adding a rule to prevent traffic going to the website IP address and also chose to block the entire IP and not just http/https traffic. On pinging again we get **“Operation not permitted”** message and also the browser is unable to reach the website after clearing the browser cache.

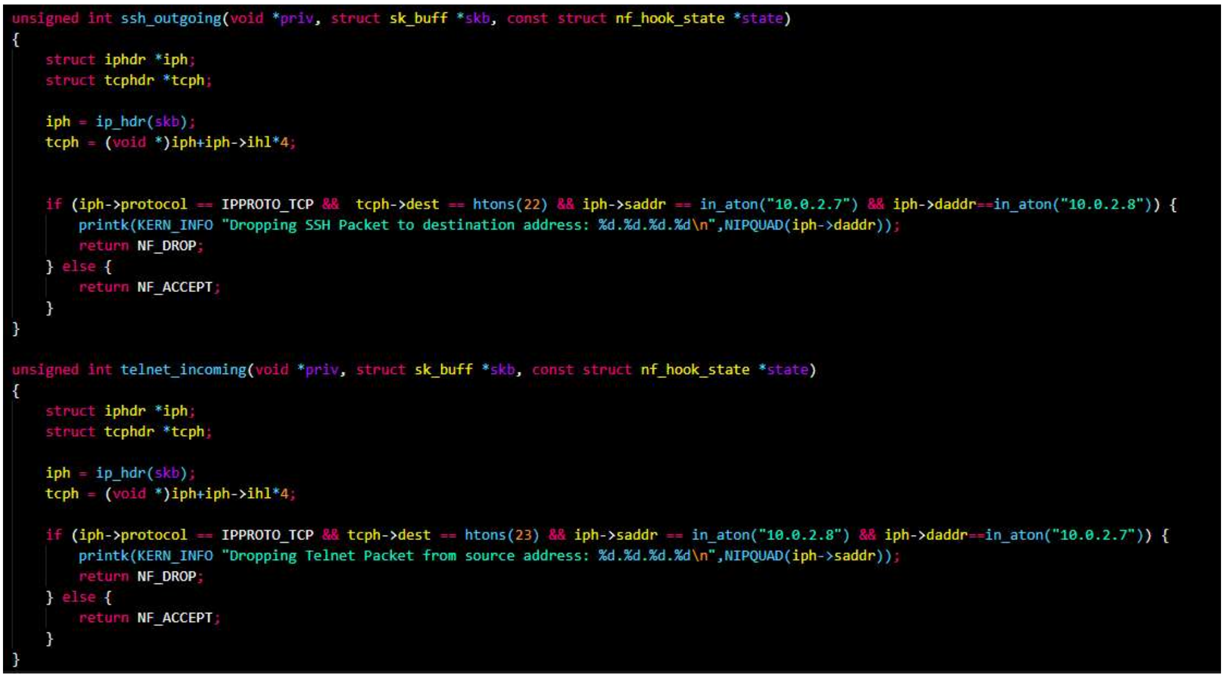
TASK 2:

CODE SNIPPETS



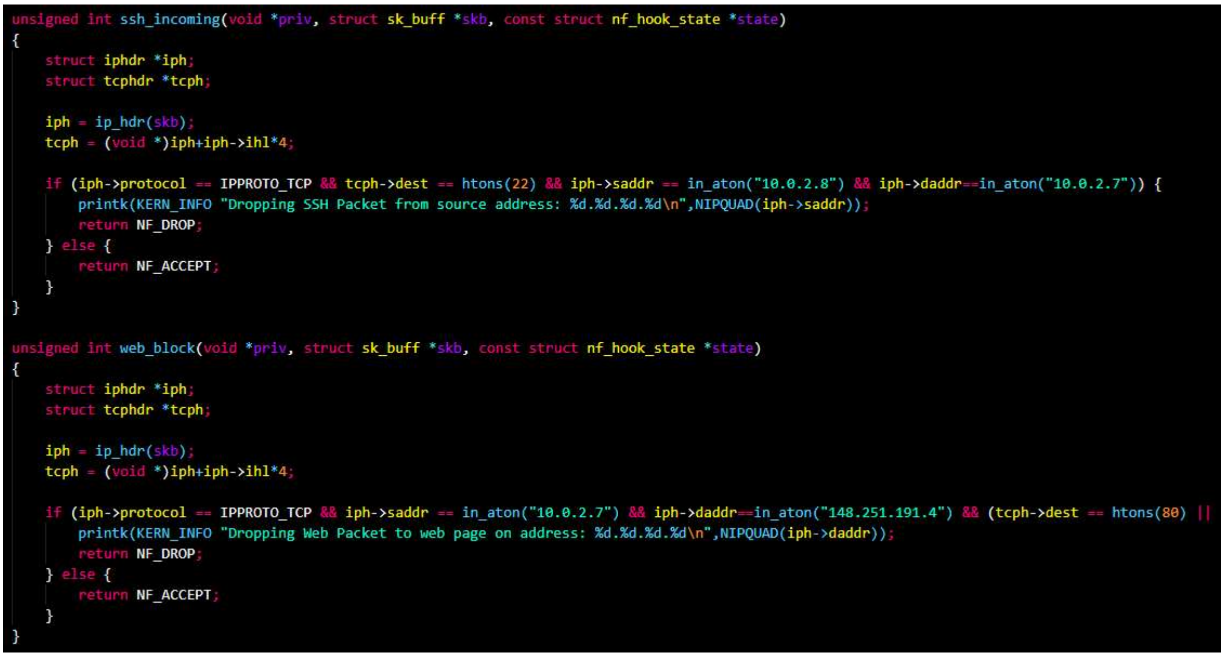
```
#include <linux/module.h>
#include <linux/kernel.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/inet.h>

#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("10.0.2.7") && iph->daddr==in_aton("10.0.2.8")) {
        printk(KERN_INFO "Dropping Telnet Packet to destination address: %d.%d.%d.%d\n",NIPQUAD(iph->daddr));
        return NF_DROP;
    } else {
        return NF_ACCEPT;
    }
}
```

Here we have created the structure and telnet_outgoing function from VM1 to VM2.



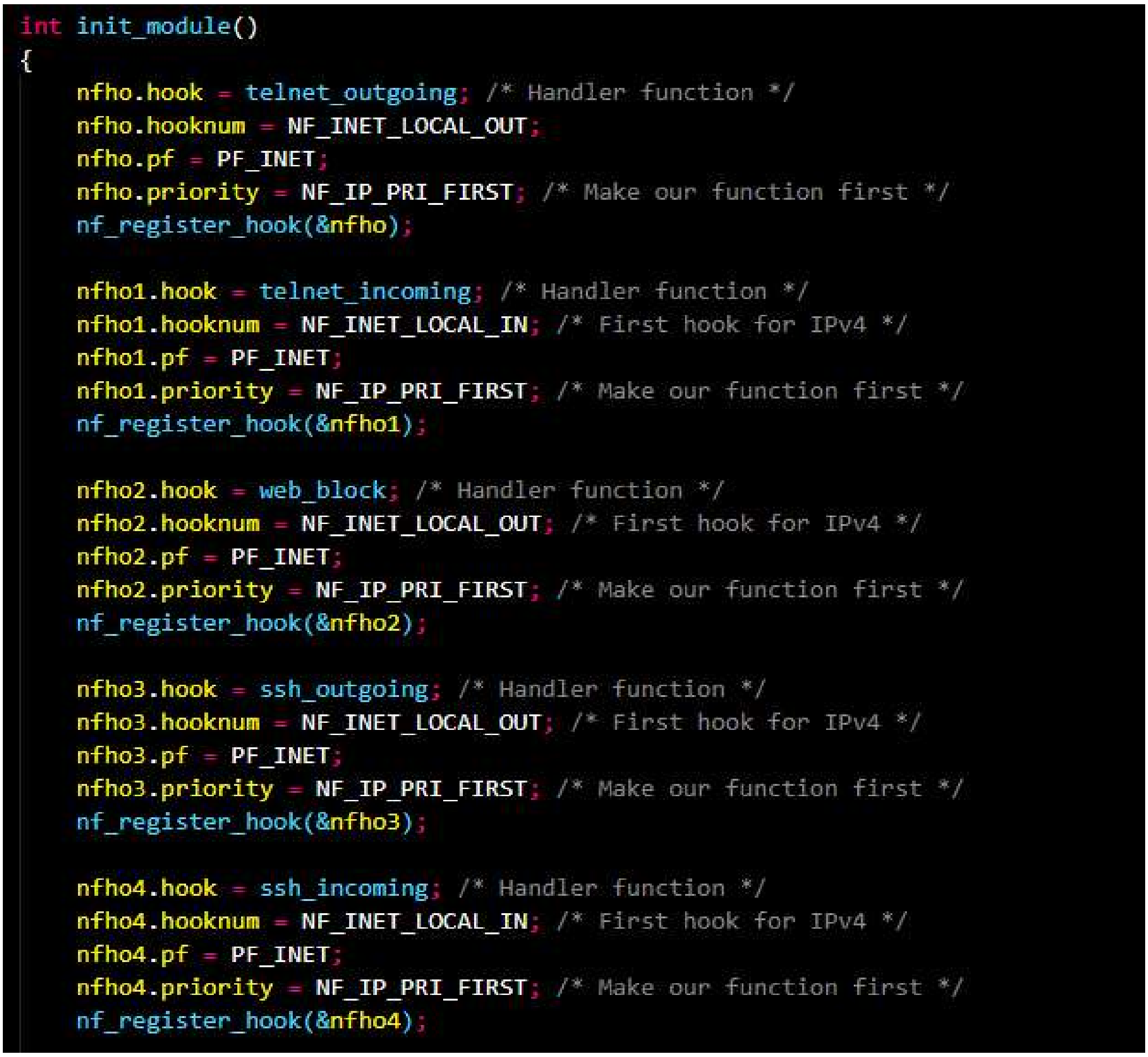
```
unsigned int ssh_outgoing(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
    struct iphdr *iph;
    struct tcphdr *tcph;

    iph = ip_hdr(skb);
    tcph = (void *)iph+iph->ihl*4;


    if (iph->protocol == IPPROTO_TCP &&  tcph->dest == htons(22) && iph->saddr == in_aton("10.0.2.7") && iph->daddr==in_aton("10.0.2.8")) {
        printk(KERN_INFO "Dropping SSH Packet to destination address: %d.%d.%d.%d\n",NIPQUAD(iph->daddr));
        return NF_DROP;
    } else {
        return NF_ACCEPT;
    }
}

unsigned int telnet_incoming(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("10.0.2.7")) {
        printk(KERN_INFO "Dropping Telnet Packet from source address: %d.%d.%d.%d\n",NIPQUAD(iph->saddr));
        return NF_DROP;
    } else {
        return NF_ACCEPT;
    }
}
```

Here we have ssh_outgoing and telnet_incoming function.



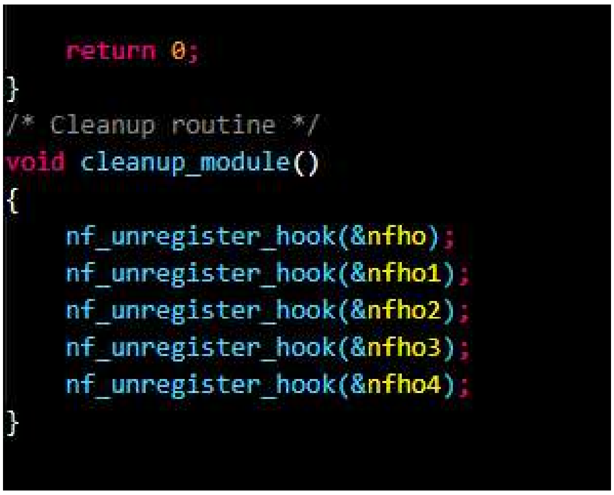
```
unsigned int ssh_incoming(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
    struct iphdr *iph;
    struct tcphdr *tcph;

    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("10.0.2.7")) {
        printk(KERN_INFO "Dropping SSH Packet from source address: %d.%d.%d.%d\n",NIPQUAD(iph->saddr));
        return NF_DROP;
    } else {
        return NF_ACCEPT;
    }
}

unsigned int web_block(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 && iph->saddr == in_aton("10.0.2.7") && iph->daddr==in_aton("148.251.191.4") && (tcph->dest == htons(80) ||
        printk(KERN_INFO "Dropping Web Packet to web page on address: %d.%d.%d.%d\n",NIPQUAD(iph->daddr));
        return NF_DROP;
    } else {
        return NF_ACCEPT;
    }
}
```

In this functions we are implementing web_block and ssh_incoming.

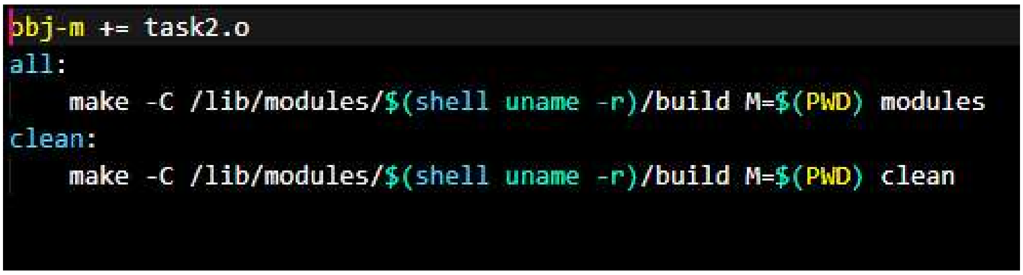


```
int init_module()
{
    nfho.hook = telnet_outgoing; /* Handler function */
    nfho.hooknum = NF_INET_LOCAL_OUT;
    nfho.pf = PF_INET;
    nfho.priority = NF_IP_PRI_FIRST; /* Make our function first */
    nf_register_hook(&nfho);

    nfho1.hook = telnet_incoming; /* Handler function */
    nfho1.hooknum = NF_INET_LOCAL_IN; /* First hook for IPv4 */
    nfho1.pf = PF_INET;
    nfho1.priority = NF_IP_PRI_FIRST; /* Make our function first */
    nf_register_hook(&nfho1);

    nfho2.hook = web_block; /* Handler function */
    nfho2.hooknum = NF_INET_LOCAL_OUT; /* First hook for IPv4 */
    nfho2.pf = PF_INET;
    nfho2.priority = NF_IP_PRI_FIRST; /* Make our function first */
    nf_register_hook(&nfho2);

    nfho3.hook = ssh_outgoing; /* Handler function */
    nfho3.hooknum = NF_INET_LOCAL_OUT; /* First hook for IPv4 */
    nfho3.pf = PF_INET;
    nfho3.priority = NF_IP_PRI_FIRST; /* Make our function first */
    nf_register_hook(&nfho3);

    nfho4.hook = ssh_incoming; /* Handler function */
    nfho4.hooknum = NF_INET_LOCAL_IN; /* First hook for IPv4 */
    nfho4.pf = PF_INET;
    nfho4.priority = NF_IP_PRI_FIRST; /* Make our function first */
    nf_register_hook(&nfho4);
```

Main module that initiates all the calling to various functions.

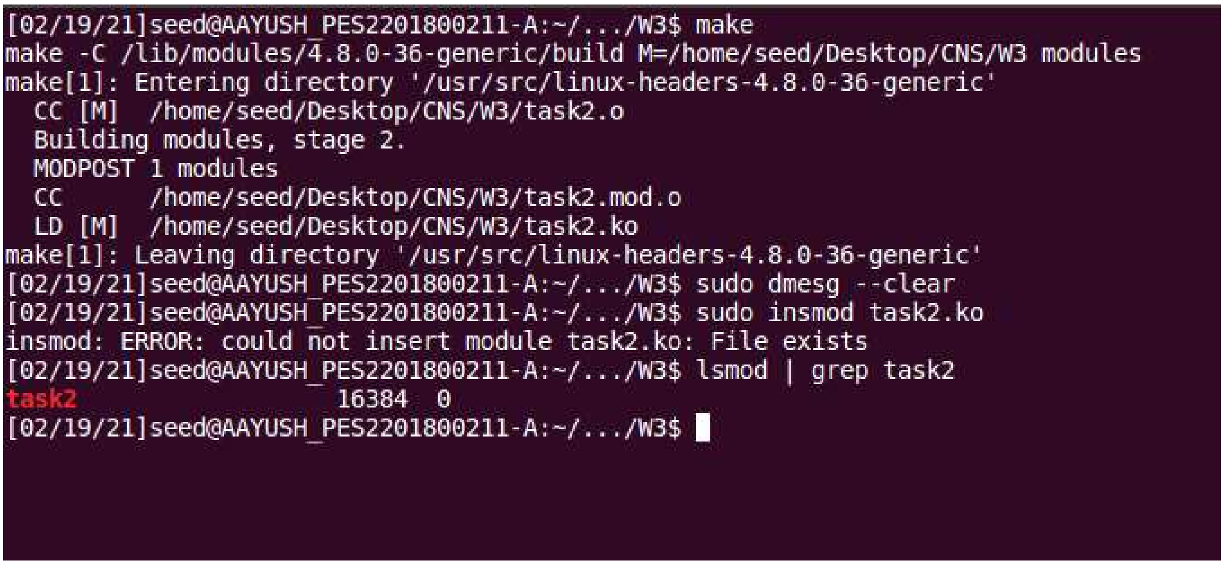


```
    return 0;
}
/* Cleanup routine */
void cleanup_module()
{
    nf_unregister_hook(&nfho);
    nf_unregister_hook(&nfho1);
    nf_unregister_hook(&nfho2);
    nf_unregister_hook(&nfho3);
    nf_unregister_hook(&nfho4);
}
```



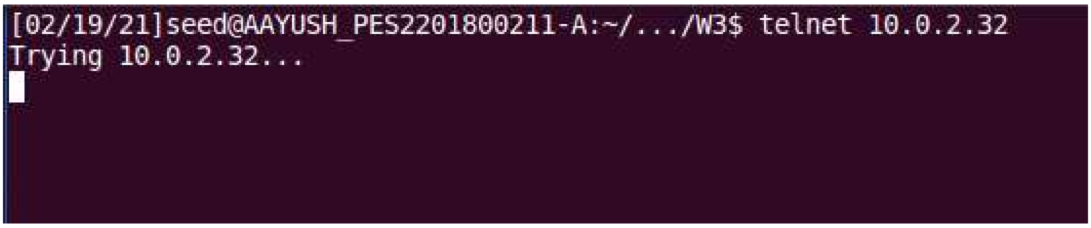
```
obj-m += task2.o
all:
    make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules
clean:
    make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean
```

MAKEFILE SNIPPET.



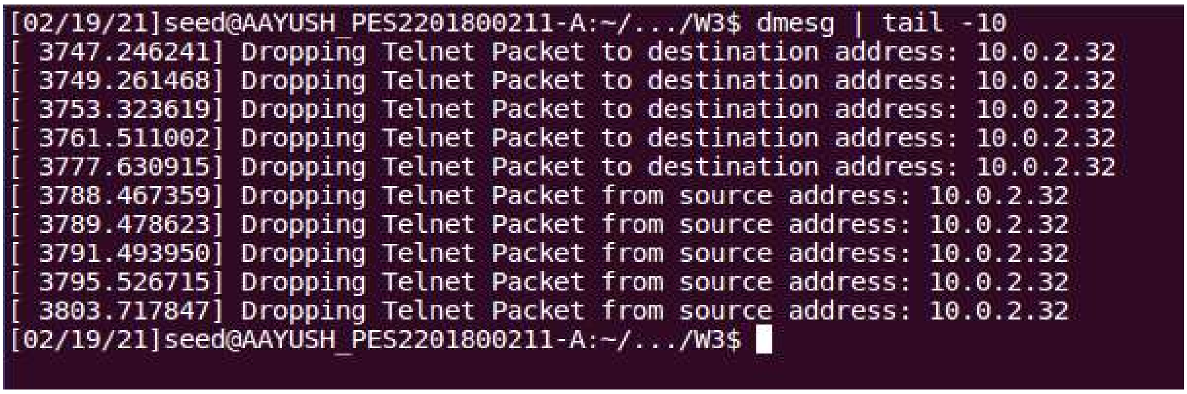
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed/Desktop/CNS/W3 modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  CC [M]  /home/seed/Desktop/CNS/W3/task2.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/Desktop/CNS/W3/task2.mod.o
  LD [M]  /home/seed/Desktop/CNS/W3/task2.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo dmesg --clear
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo insmod task2.ko
insmod: ERROR: could not insert module task2.ko: File exists
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ lsmod | grep task2
task2                  16384  0
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ 
```

For task 2, we will perform the same as task 1 using the task2.c program written to prevent telnet, ssh traffics to other VM and traffic to pes.edu website. We also have a makefile that helps to make the compilation easy. We store the makefile and task2.c in a folder and execute make command.

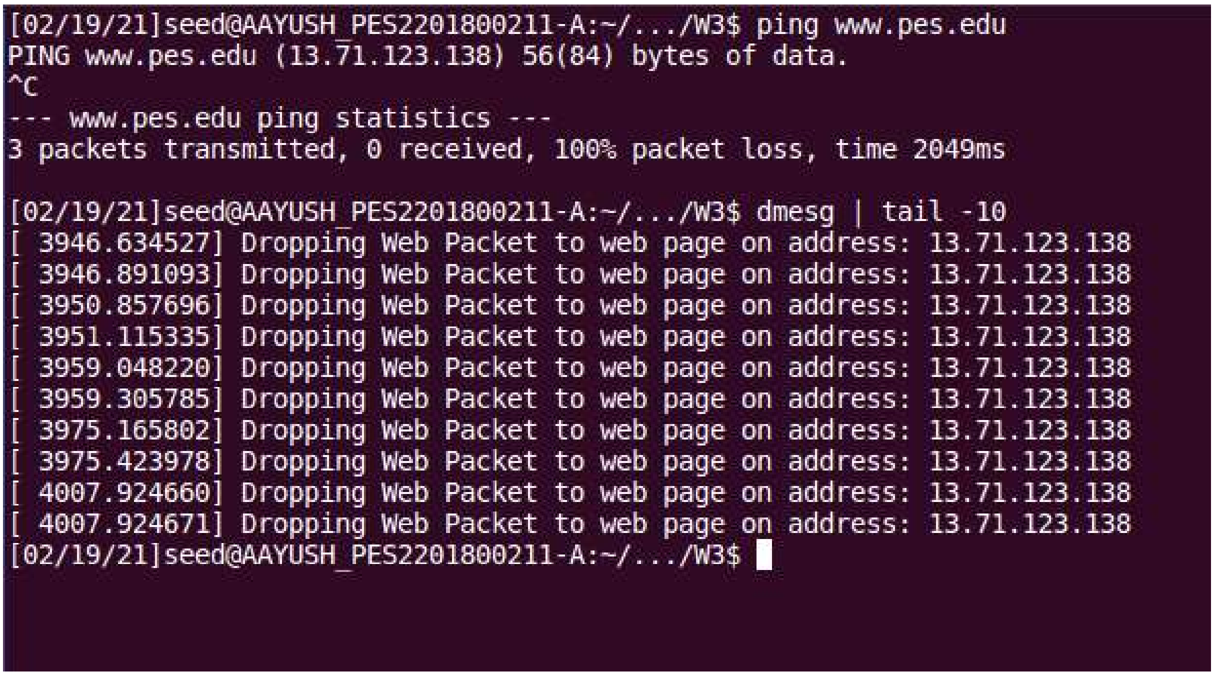


```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ telnet 10.0.2.32
Trying 10.0.2.32...
```

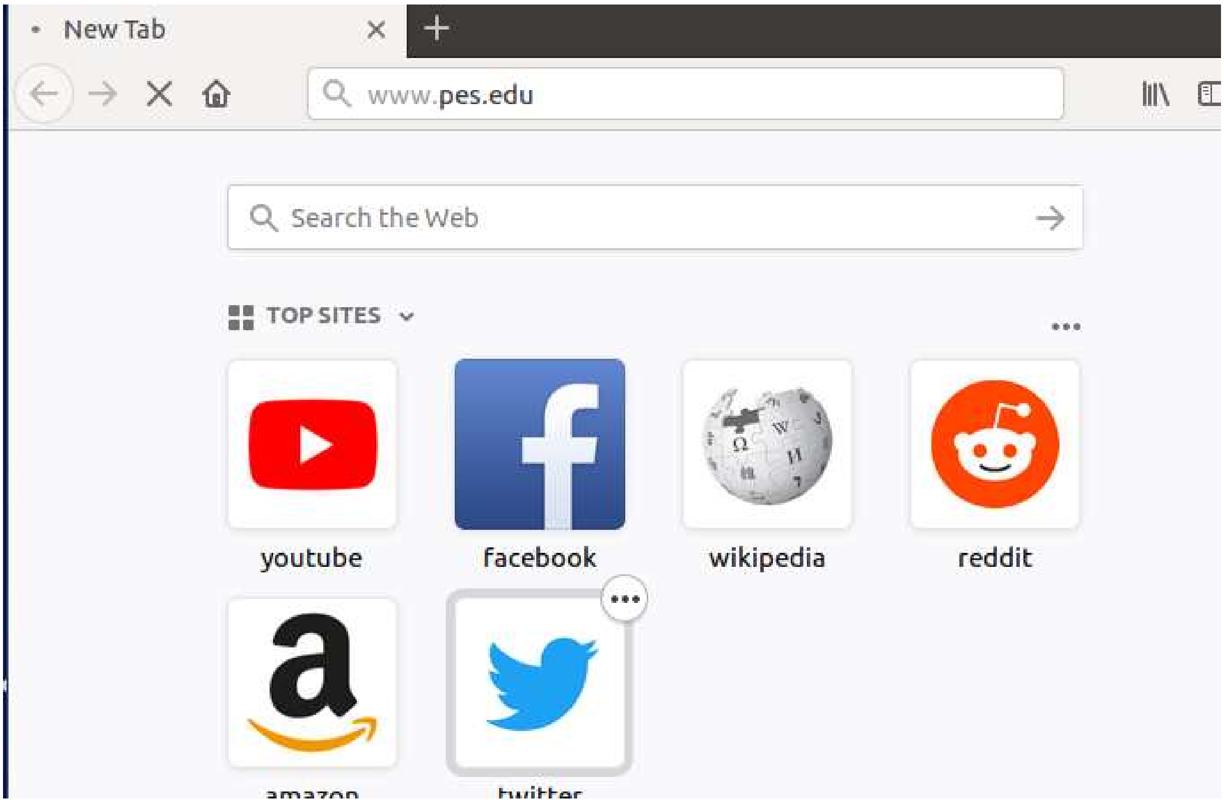
On telnetting to VM2 from VM1, we see that we are not successful performing telnet. Below we display the dropping packet from source and destination IP.



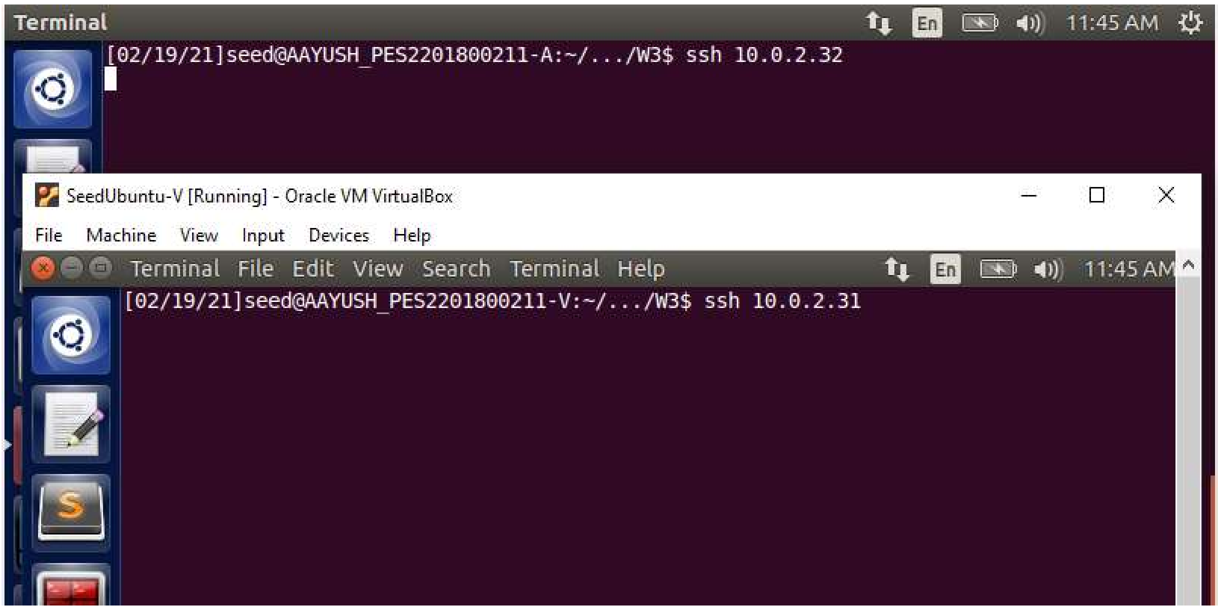
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ dmesg | tail -10
[ 3747.246241] Dropping Telnet Packet to destination address: 10.0.2.32
[ 3749.261468] Dropping Telnet Packet to destination address: 10.0.2.32
[ 3753.323619] Dropping Telnet Packet to destination address: 10.0.2.32
[ 3761.511002] Dropping Telnet Packet to destination address: 10.0.2.32
[ 3777.630915] Dropping Telnet Packet to destination address: 10.0.2.32
[ 3788.467359] Dropping Telnet Packet from source address: 10.0.2.32
[ 3789.478623] Dropping Telnet Packet from source address: 10.0.2.32
[ 3791.493950] Dropping Telnet Packet from source address: 10.0.2.32
[ 3795.526715] Dropping Telnet Packet from source address: 10.0.2.32
[ 3803.717847] Dropping Telnet Packet from source address: 10.0.2.32
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```



```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ping www.pes.edu
PING www.pes.edu (13.71.123.138) 56(84) bytes of data.
^C
--- www.pes.edu ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2049ms

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ dmesg | tail -10
[ 3946.634527] Dropping Web Packet to web page on address: 13.71.123.138
[ 3946.891093] Dropping Web Packet to web page on address: 13.71.123.138
[ 3950.857696] Dropping Web Packet to web page on address: 13.71.123.138
[ 3951.115335] Dropping Web Packet to web page on address: 13.71.123.138
[ 3959.048220] Dropping Web Packet to web page on address: 13.71.123.138
[ 3959.305785] Dropping Web Packet to web page on address: 13.71.123.138
[ 3975.165802] Dropping Web Packet to web page on address: 13.71.123.138
[ 3975.423978] Dropping Web Packet to web page on address: 13.71.123.138
[ 4007.924660] Dropping Web Packet to web page on address: 13.71.123.138
[ 4007.924671] Dropping Web Packet to web page on address: 13.71.123.138
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```



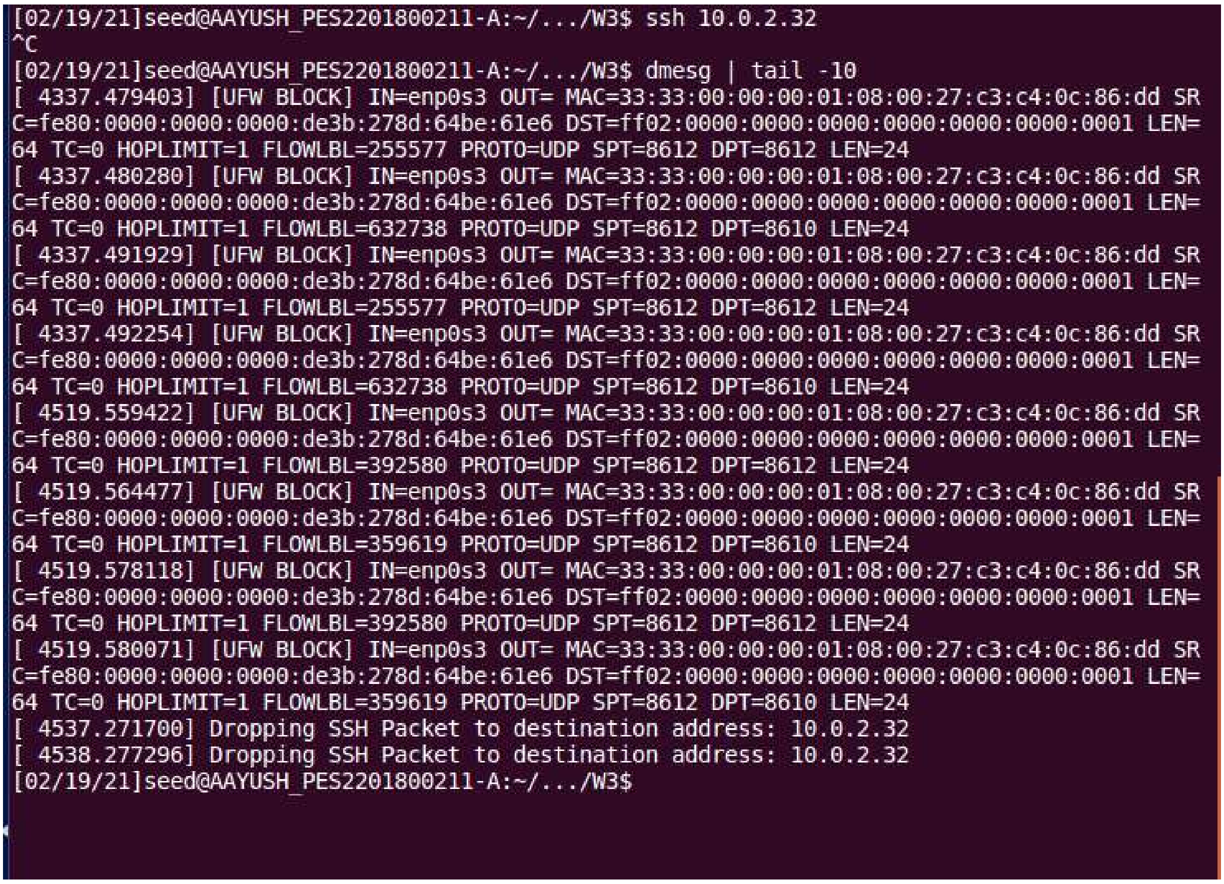
Here we do it for website traffic and see that we are not able to ping websites and same thing on browser after clearing cache. Also display the dropping website traffic to pes.edu webpage on it's IP address.



Terminal
En
11:45 AM
SeedUbuntu-V [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
En
11:45 AM

```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ssh 10.0.2.32
```

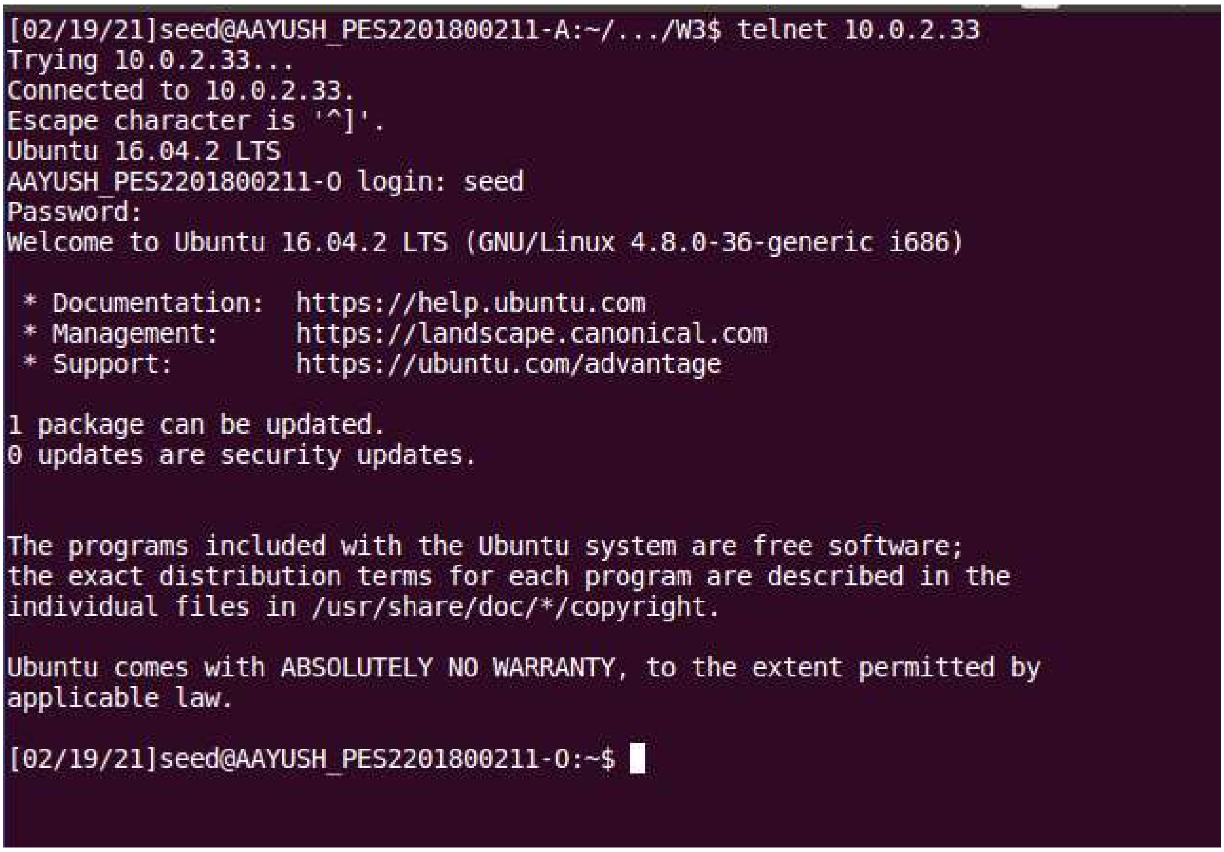
```
[02/19/21]seed@AAYUSH_PES2201800211-V:~/.../W3$ ssh 10.0.2.31
```



```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ssh 10.0.2.32
^C
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ dmesg | tail -10
[ 4337.479403] [UFW BLOCK] IN=enp0s3 OUT= MAC=33:33:00:00:00:01:08:00:27:c3:c4:0c:86:dd SR
C=fe80:0000:0000:0000:de3b:278d:64be:61e6 DST=ff02:0000:0000:0000:0000:0000:0000:0001 LEN=
64 TC=0 HOPLIMIT=1 FLOWLBL=255577 PROTO=UDP SPT=8612 DPT=8612 LEN=24
[ 4337.480280] [UFW BLOCK] IN=enp0s3 OUT= MAC=33:33:00:00:00:01:08:00:27:c3:c4:0c:86:dd SR
C=fe80:0000:0000:0000:de3b:278d:64be:61e6 DST=ff02:0000:0000:0000:0000:0000:0000:0001 LEN=
64 TC=0 HOPLIMIT=1 FLOWLBL=632738 PROTO=UDP SPT=8612 DPT=8610 LEN=24
[ 4337.491929] [UFW BLOCK] IN=enp0s3 OUT= MAC=33:33:00:00:00:01:08:00:27:c3:c4:0c:86:dd SR
C=fe80:0000:0000:0000:de3b:278d:64be:61e6 DST=ff02:0000:0000:0000:0000:0000:0000:0001 LEN=
64 TC=0 HOPLIMIT=1 FLOWLBL=255577 PROTO=UDP SPT=8612 DPT=8612 LEN=24
[ 4337.492254] [UFW BLOCK] IN=enp0s3 OUT= MAC=33:33:00:00:00:01:08:00:27:c3:c4:0c:86:dd SR
C=fe80:0000:0000:0000:de3b:278d:64be:61e6 DST=ff02:0000:0000:0000:0000:0000:0000:0001 LEN=
64 TC=0 HOPLIMIT=1 FLOWLBL=632738 PROTO=UDP SPT=8612 DPT=8610 LEN=24
[ 4519.559422] [UFW BLOCK] IN=enp0s3 OUT= MAC=33:33:00:00:00:01:08:00:27:c3:c4:0c:86:dd SR
C=fe80:0000:0000:0000:de3b:278d:64be:61e6 DST=ff02:0000:0000:0000:0000:0000:0000:0001 LEN=
64 TC=0 HOPLIMIT=1 FLOWLBL=392580 PROTO=UDP SPT=8612 DPT=8612 LEN=24
[ 4519.564477] [UFW BLOCK] IN=enp0s3 OUT= MAC=33:33:00:00:00:01:08:00:27:c3:c4:0c:86:dd SR
C=fe80:0000:0000:0000:de3b:278d:64be:61e6 DST=ff02:0000:0000:0000:0000:0000:0000:0001 LEN=
64 TC=0 HOPLIMIT=1 FLOWLBL=359619 PROTO=UDP SPT=8612 DPT=8610 LEN=24
[ 4519.578118] [UFW BLOCK] IN=enp0s3 OUT= MAC=33:33:00:00:00:01:08:00:27:c3:c4:0c:86:dd SR
C=fe80:0000:0000:0000:de3b:278d:64be:61e6 DST=ff02:0000:0000:0000:0000:0000:0000:0001 LEN=
64 TC=0 HOPLIMIT=1 FLOWLBL=392580 PROTO=UDP SPT=8612 DPT=8612 LEN=24
[ 4519.580071] [UFW BLOCK] IN=enp0s3 OUT= MAC=33:33:00:00:00:01:08:00:27:c3:c4:0c:86:dd SR
C=fe80:0000:0000:0000:de3b:278d:64be:61e6 DST=ff02:0000:0000:0000:0000:0000:0000:0001 LEN=
64 TC=0 HOPLIMIT=1 FLOWLBL=359619 PROTO=UDP SPT=8612 DPT=8610 LEN=24
[ 4537.271700] Dropping SSH Packet to destination address: 10.0.2.32
[ 4538.277296] Dropping SSH Packet to destination address: 10.0.2.32
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```

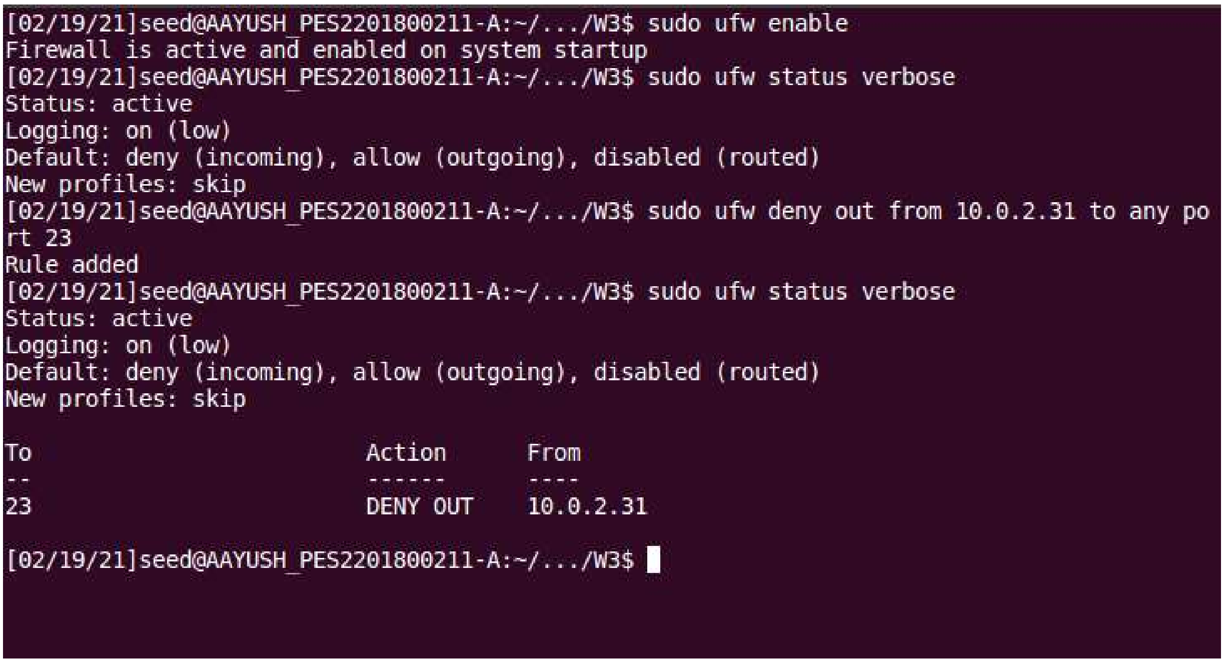
Here we perform ssh connection and see that we see that it was unsuccessful and also the dropping ssh packet from destination IP address. [The garbled message is due to a lost connection as I took it after ctrl+c command].

TASK 3a:



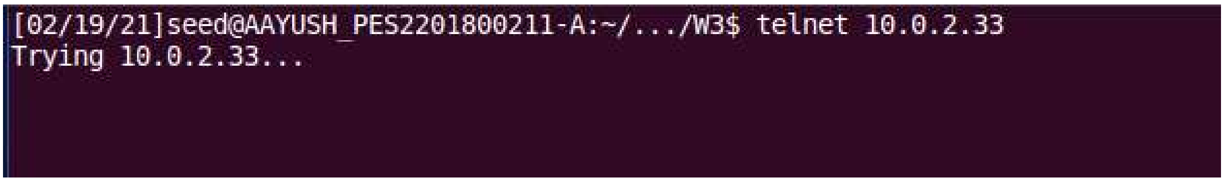
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ telnet 10.0.2.33
Trying 10.0.2.33...
Connected to 10.0.2.33.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
AAYUSH_PES2201800211-O login: seed
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[02/19/21]seed@AAYUSH_PES2201800211-O:~$ 
```

We are able to telnet from VM1 to VM3(observer IP).



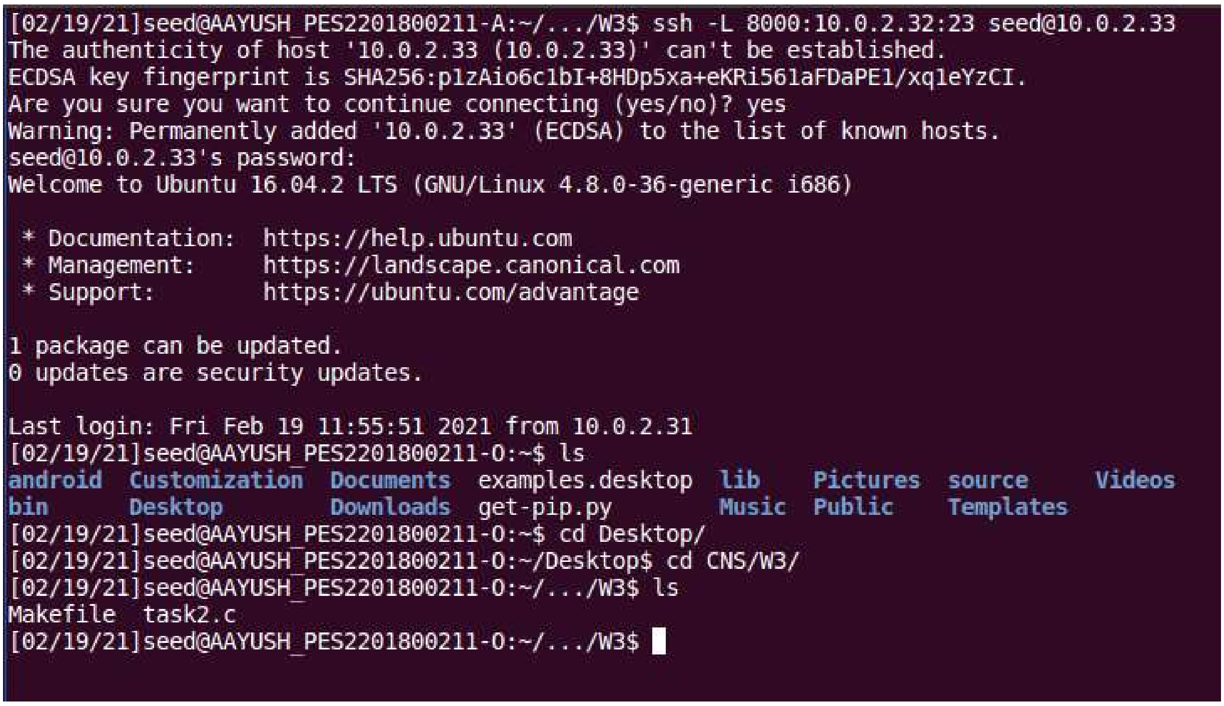
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw enable
Firewall is active and enabled on system startup
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw deny out from 10.0.2.31 to any po
rt 23
Rule added
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
23                         DENY OUT    10.0.2.31

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ 
```

We delete the previous rule and add rule to deny any outgoing telnet connection from VM1.



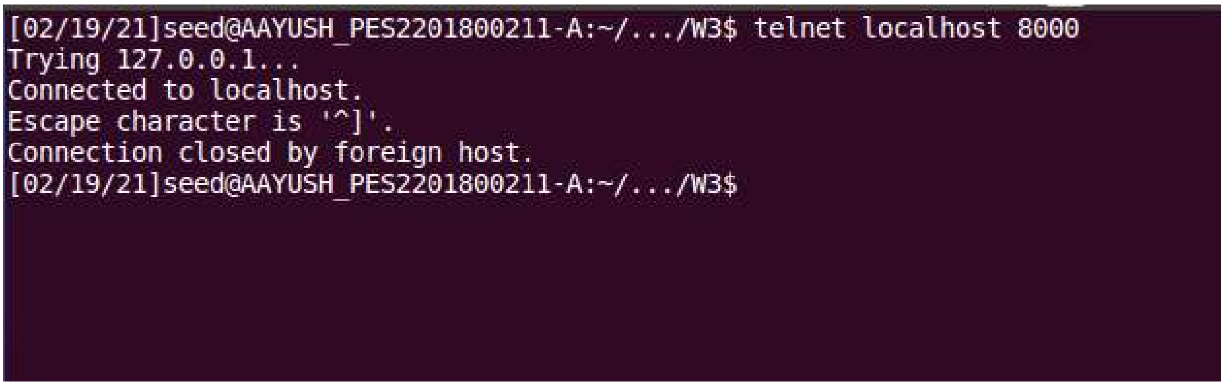
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ telnet 10.0.2.33
Trying 10.0.2.33...
```

On performing again telnet from VM1 to VM3, it displays the Trying message i.e the connection was unsuccessful.

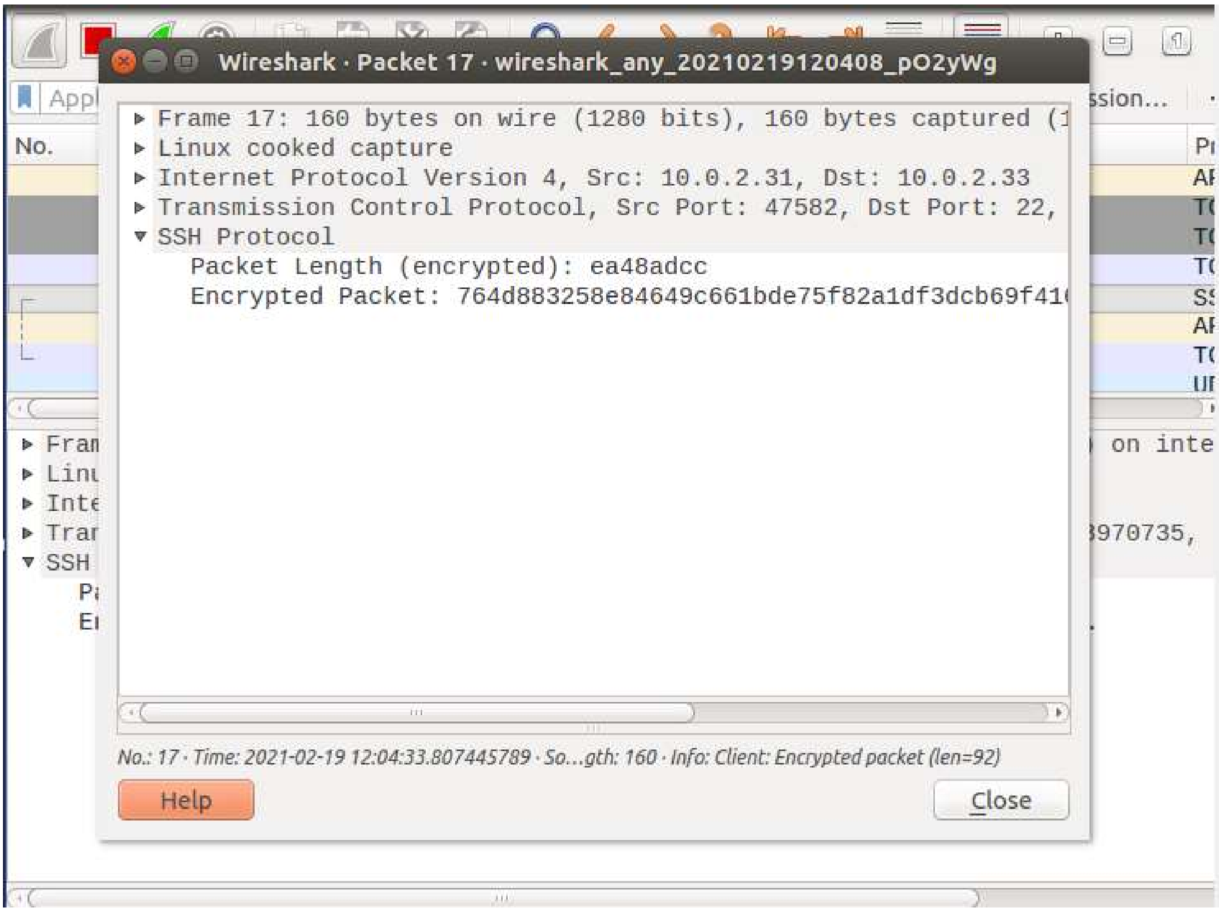


```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ssh -L 8000:10.0.2.32:23 seed@10.0.2.33
The authenticity of host '10.0.2.33 (10.0.2.33)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.33' (ECDSA) to the list of known hosts.
seed@10.0.2.33'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

1 package can be updated.
0 updates are security updates.

Last login: Fri Feb 19 11:55:51 2021 from 10.0.2.31
[02/19/21]seed@AAYUSH_PES2201800211-O:~$ ls
android  Customization  Documents  examples.desktop  lib    Pictures  source     Videos
bin      Desktop        Downloads  get-pip.py        Music  Public    Templates
[02/19/21]seed@AAYUSH_PES2201800211-O:~$ cd Desktop/
[02/19/21]seed@AAYUSH_PES2201800211-O:~/Desktop$ cd CNS/W3/
[02/19/21]seed@AAYUSH_PES2201800211-O:~/.../W3$ ls
Makefile  task2.c
[02/19/21]seed@AAYUSH_PES2201800211-O:~/.../W3$ 
```

To get the connection from VM1 to VM3 after adding the firewall rule, we create a tunnel from VM1 to VM2 via port 8000 and then telnet (port 23) from VM2 to VM3. On executing it we see that the connection was successful and on another terminal telnet to the VM3 via port 8000 as shown in below pic.



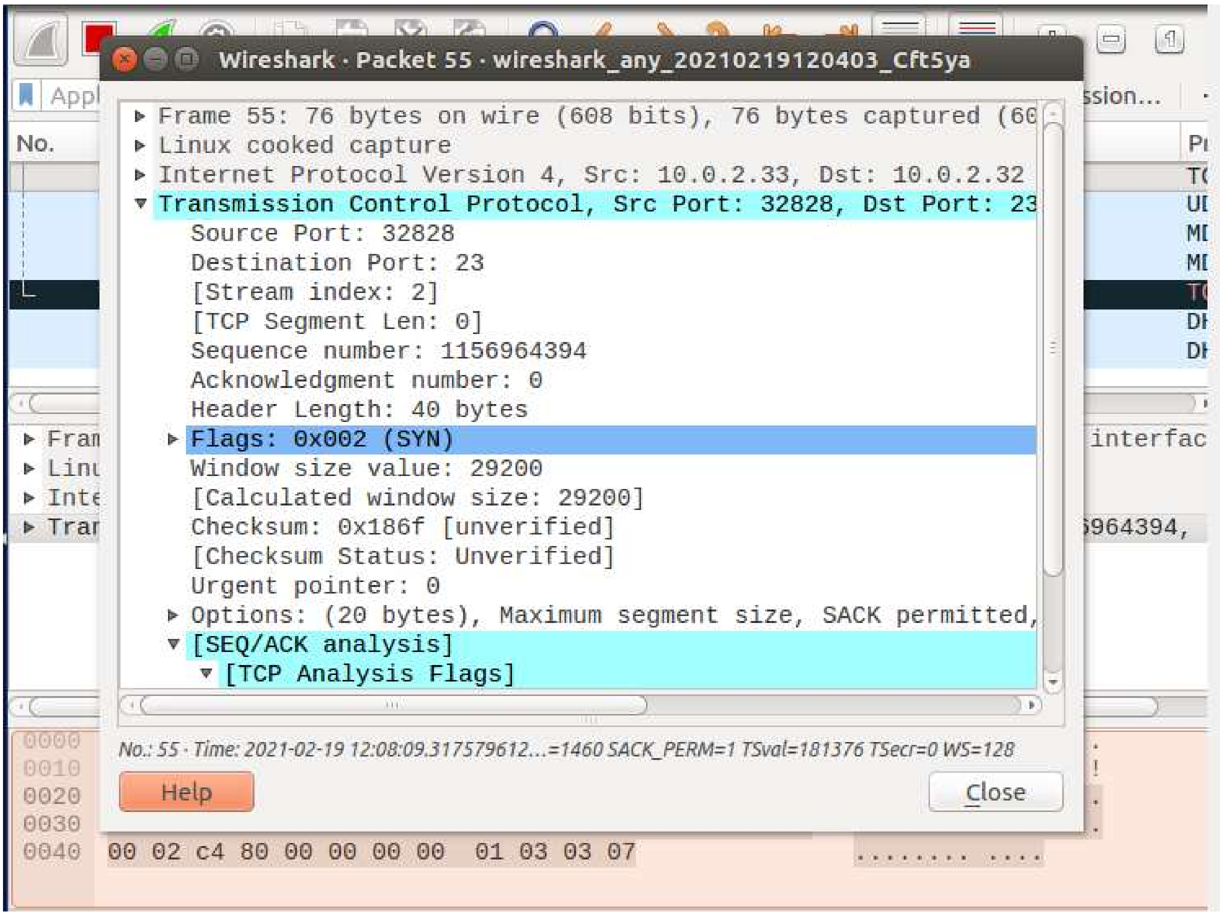
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Connection closed by foreign host.
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```



Wireshark · Packet 17 · wireshark_any_20210219120408_pO2yWg

```
▸ Frame 17: 160 bytes on wire (1280 bits), 160 bytes captured (1
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.31, Dst: 10.0.2.33
▸ Transmission Control Protocol, Src Port: 47582, Dst Port: 22,
▾ SSH Protocol
    Packet Length (encrypted): ea48adcc
    Encrypted Packet: 764d883258e84649c661bde75f82a1df3dcb69f41
```

No.: 17 · Time: 2021-02-19 12:04:33.807445789 · So...gth: 160 · Info: Client: Encrypted packet (len=92)



Wireshark · Packet 55 · wireshark_any_20210219120403_Cft5ya

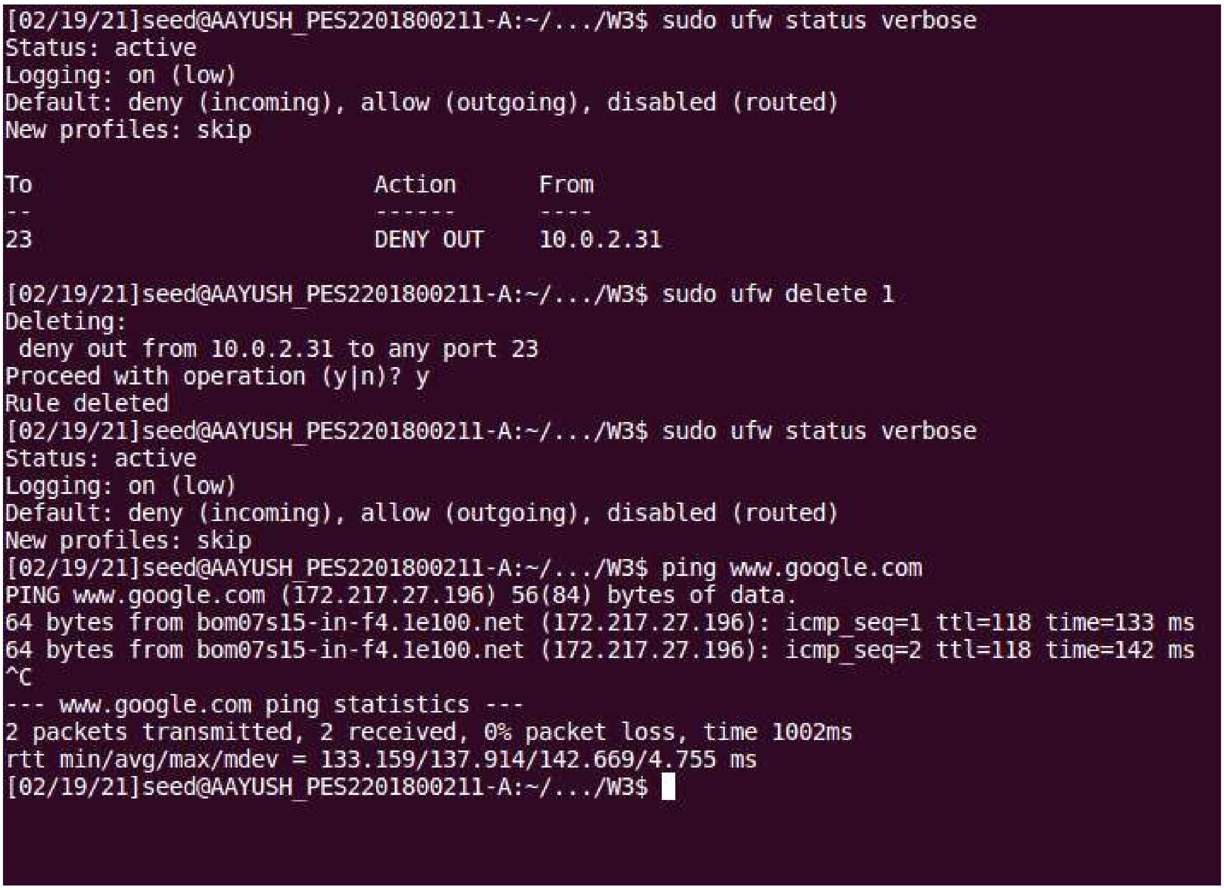
```
▸ Frame 55: 76 bytes on wire (608 bits), 76 bytes captured (60
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.33, Dst: 10.0.2.32
▾ Transmission Control Protocol, Src Port: 32828, Dst Port: 23
    Source Port: 32828
    Destination Port: 23
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 1156964394
    Acknowledgment number: 0
    Header Length: 40 bytes
  ▸ Flags: 0x002 (SYN)
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0x186f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted,
  ▾ [SEQ/ACK analysis]
    ▾ [TCP Analysis Flags]
```

No.: 55 · Time: 2021-02-19 12:08:09.317579612...=1460 SACK_PERM=1 TSval=181376 TSecr=0 WS=128

```
0000
0010
0020
0030
0040  00 02 c4 80 00 00 00 00  01 03 03 07     ........ ....
```

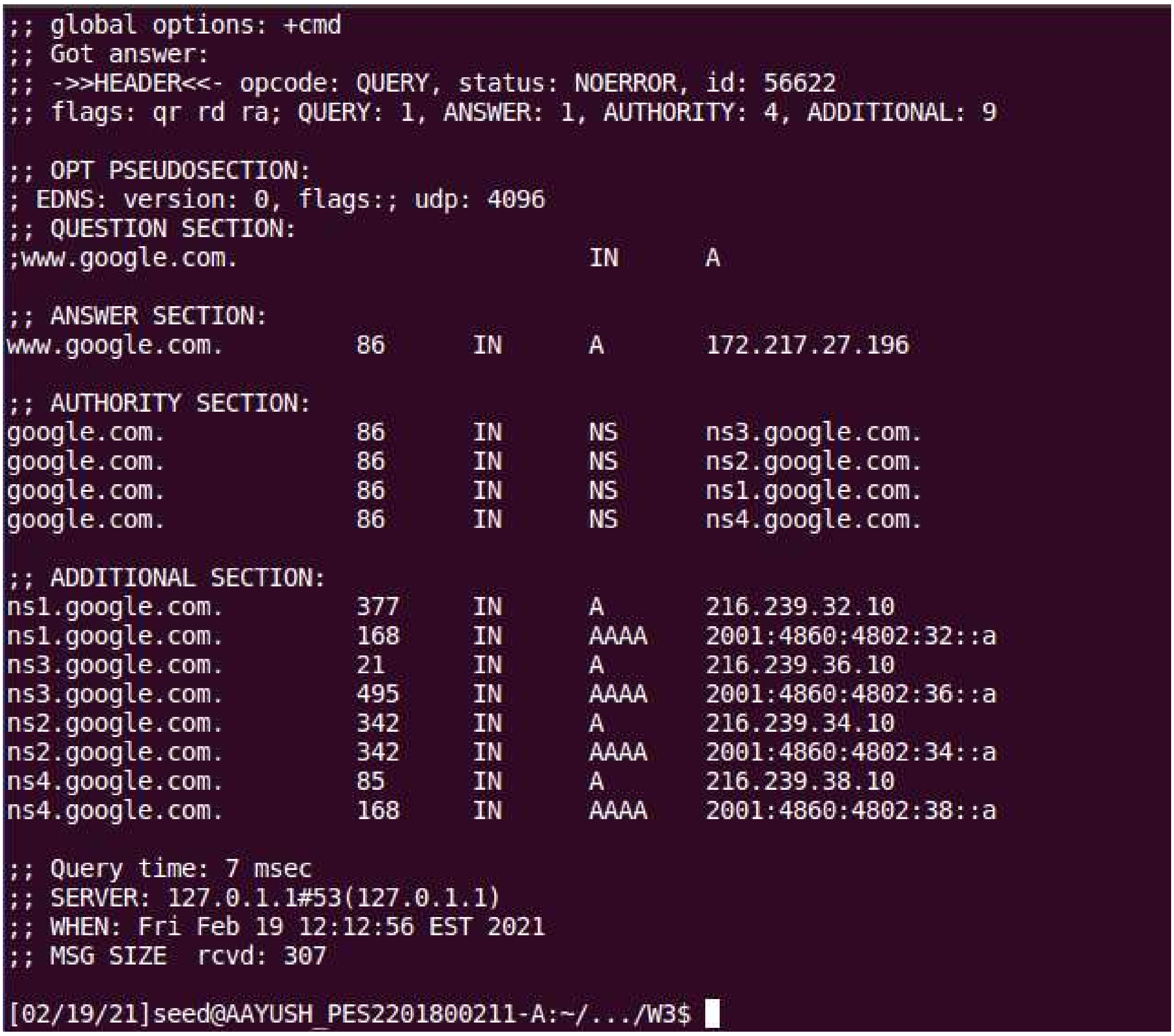
Above are the wireshark capture from source VM1 to destination VM3 (ssh protocol details are captured) and SYN packet traffic connection from VM3 to VM2.

TASK 3b:



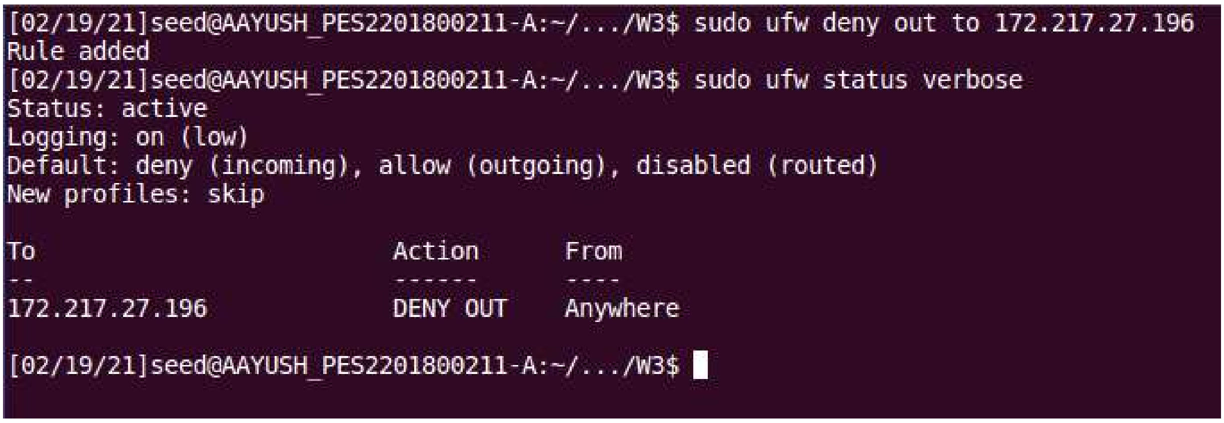
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
23                         DENY OUT    10.0.2.31

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw delete 1
Deleting:
 deny out from 10.0.2.31 to any port 23
Proceed with operation (y|n)? y
Rule deleted
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ping www.google.com
PING www.google.com (172.217.27.196) 56(84) bytes of data.
64 bytes from bom07s15-in-f4.1e100.net (172.217.27.196): icmp_seq=1 ttl=118 time=133 ms
64 bytes from bom07s15-in-f4.1e100.net (172.217.27.196): icmp_seq=2 ttl=118 time=142 ms
^C
--- www.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 133.159/137.914/142.669/4.755 ms
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ 
```

We delete previous firewall rules and ping google.com. In this task we will prevent VM1 to capture traffic from google therefore create a tunnel to VM2 and then send traffic to google.com.



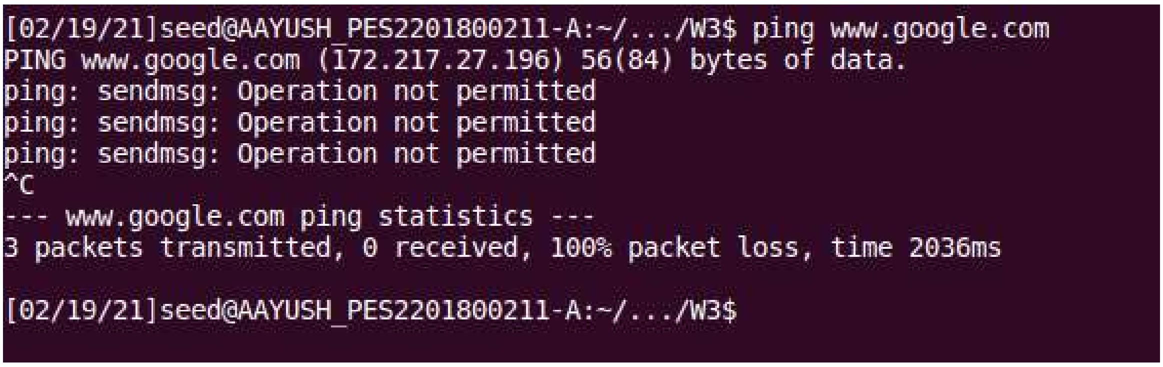
```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56622
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         86      IN      A       172.217.27.196

;; AUTHORITY SECTION:
google.com.             86      IN      NS      ns3.google.com.
google.com.             86      IN      NS      ns2.google.com.
google.com.             86      IN      NS      ns1.google.com.
google.com.             86      IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         377     IN      A       216.239.32.10
ns1.google.com.         168     IN      AAAA    2001:4860:4802:32::a
ns3.google.com.         21      IN      A       216.239.36.10
ns3.google.com.         495     IN      AAAA    2001:4860:4802:36::a
ns2.google.com.         342     IN      A       216.239.34.10
ns2.google.com.         342     IN      AAAA    2001:4860:4802:34::a
ns4.google.com.         85      IN      A       216.239.38.10
ns4.google.com.         168     IN      AAAA    2001:4860:4802:38::a

;; Query time: 7 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Feb 19 12:12:56 EST 2021
;; MSG SIZE  rcvd: 307

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ 
```

IP of google -> 172.217.27.196

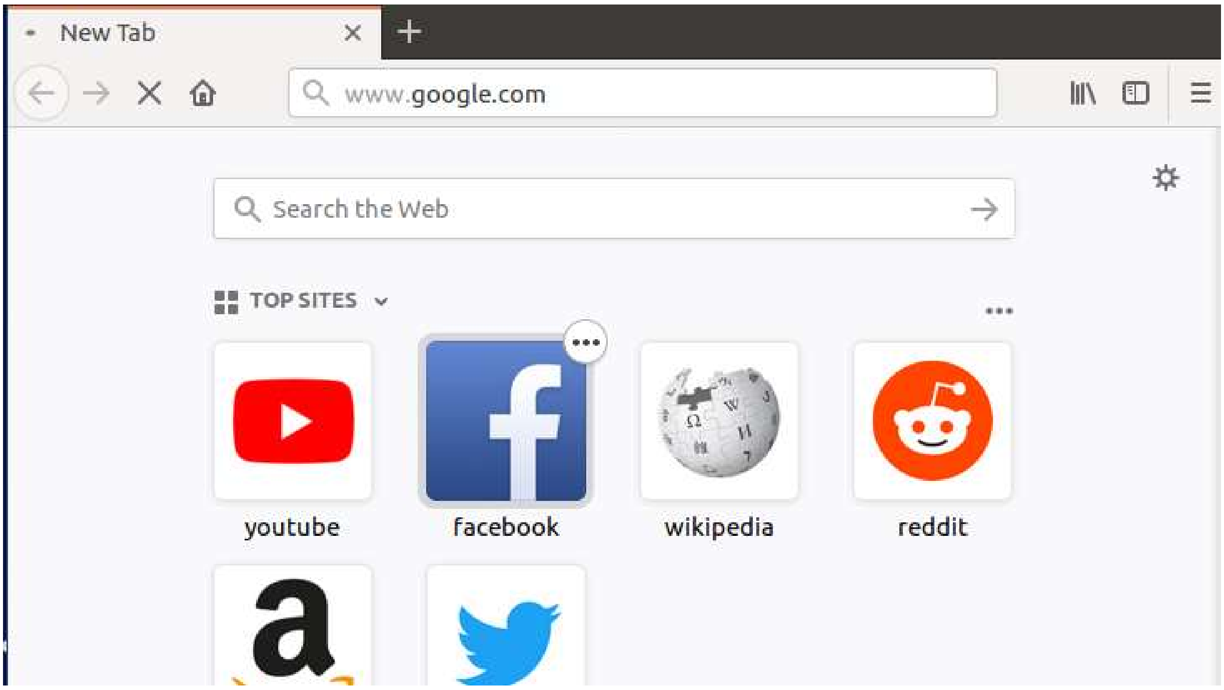


```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw deny out to 172.217.27.196
Rule added
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
172.217.27.196             DENY OUT    Anywhere

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ 
```

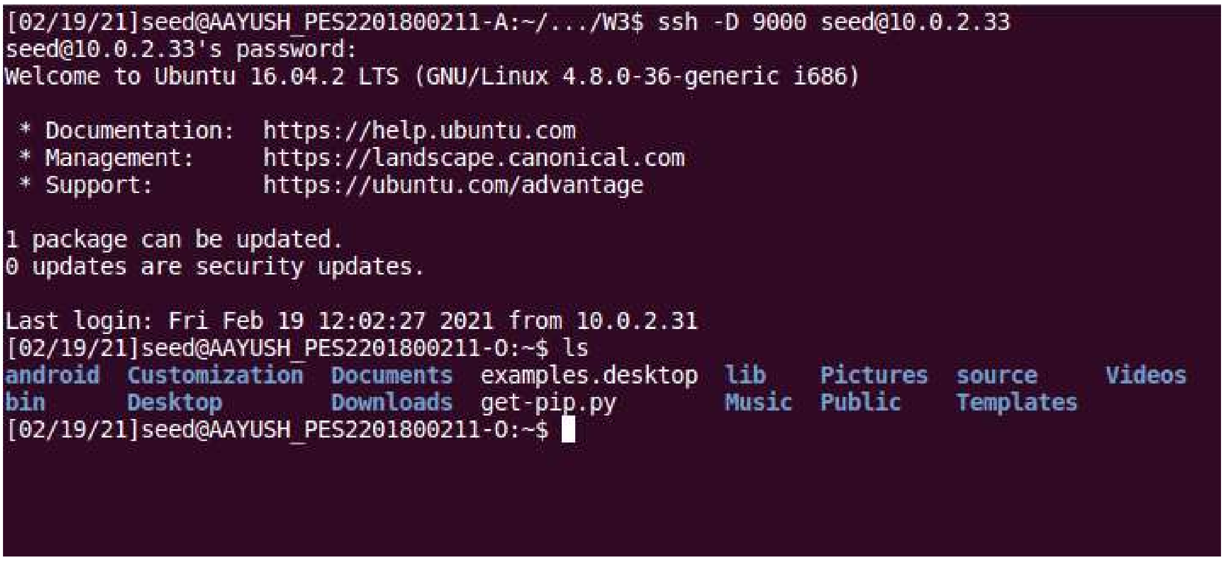
We add a rule to deny traffic from IP 172.217.27.196.



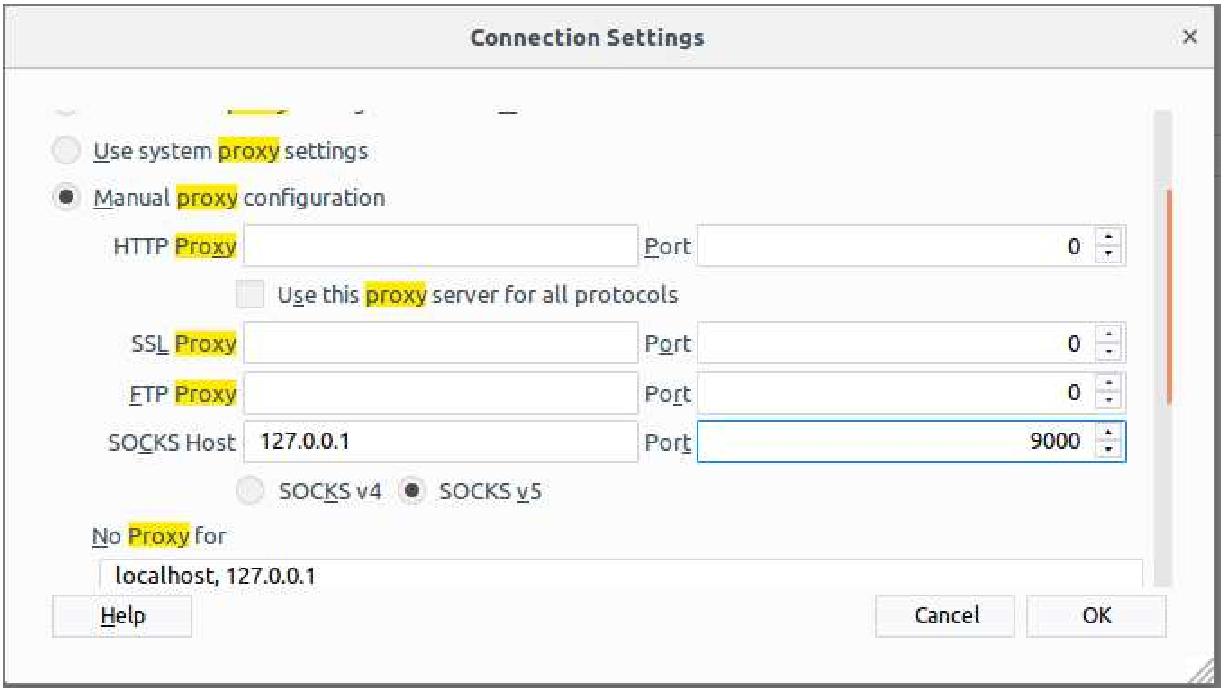
```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ping www.google.com
PING www.google.com (172.217.27.196) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- www.google.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2036ms

[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$
```



On pinging from VM1 to google.com we get the **“Operation not permitted”** message and on trying on browser after clearing cache, it does not get loaded. Hence the attack was successful for not allowing the traffic.



```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ssh -D 9000 seed@10.0.2.33
seed@10.0.2.33'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

1 package can be updated.
0 updates are security updates.

Last login: Fri Feb 19 12:02:27 2021 from 10.0.2.31
[02/19/21]seed@AAYUSH_PES2201800211-O:~$ ls
android  Customization  Documents  examples.desktop  lib    Pictures  source     Videos
bin      Desktop        Downloads  get-pip.py        Music  Public    Templates
[02/19/21]seed@AAYUSH_PES2201800211-O:~$ 
```



Connection Settings

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy: ____ Port: 0

□ Use this proxy server for all protocols

SSL Proxy: ____ Port: 0

FTP Proxy: ____ Port: 0

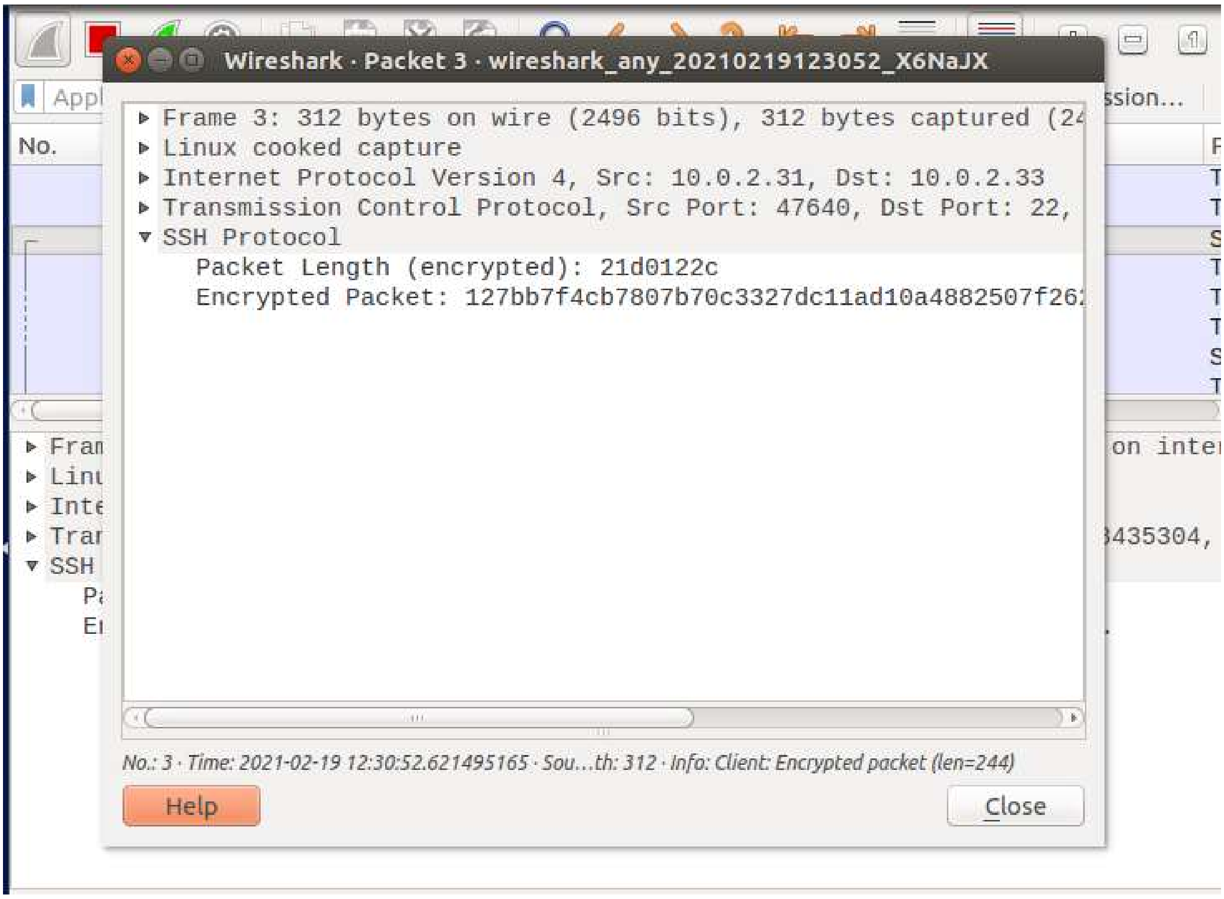
SOCKS Host: 127.0.0.1 Port: 9000

○ SOCKS v4 ● SOCKS v5

No Proxy for

localhost, 127.0.0.1

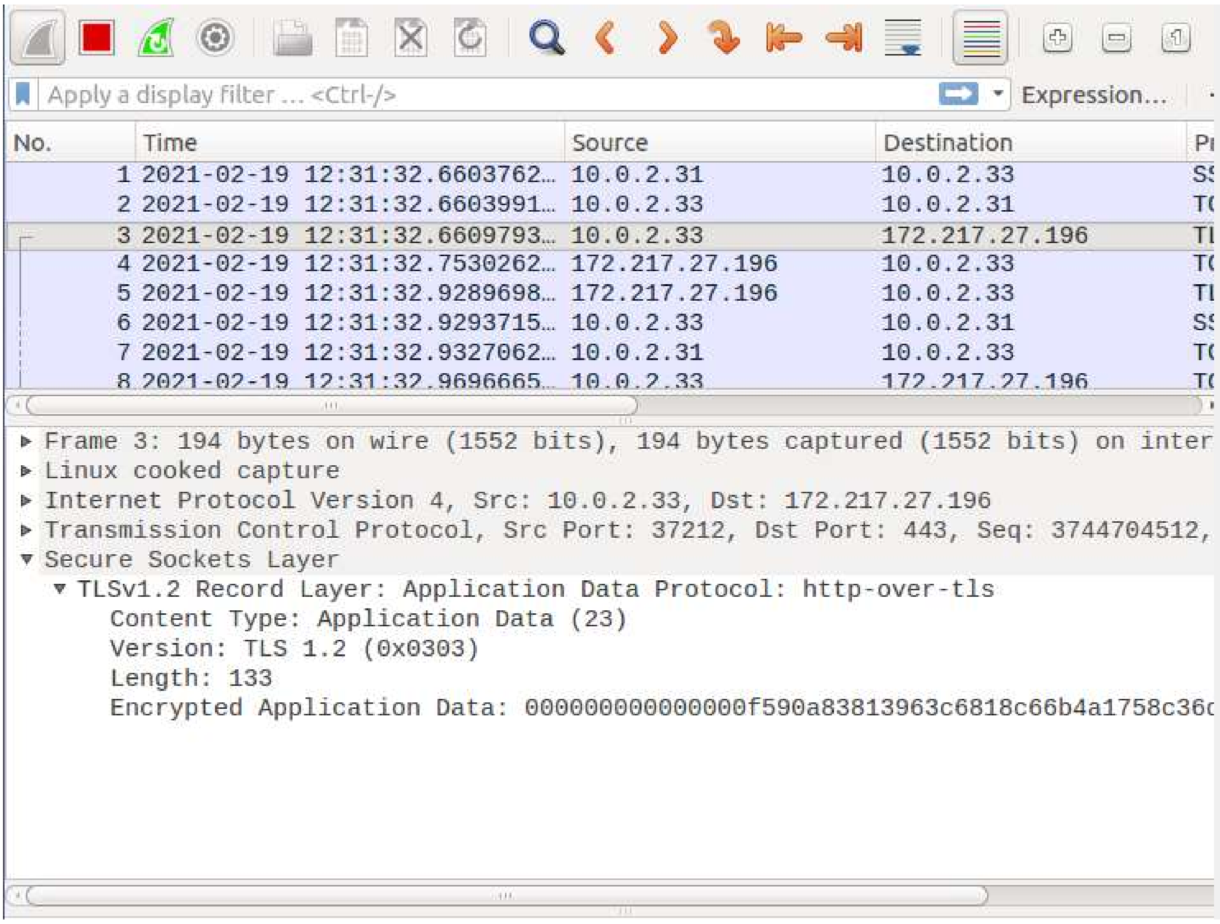
Above we create a ssh tunnel from VM1 to VM3 on port 9000 and then modify the proxy setting to manual and localhost on port 9000.



Wireshark · Packet 3 · wireshark_any_20210219123052_X6NaJX

```
▶ Frame 3: 312 bytes on wire (2496 bits), 312 bytes captured (24
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.0.2.31, Dst: 10.0.2.33
▶ Transmission Control Protocol, Src Port: 47640, Dst Port: 22,
▼ SSH Protocol
    Packet Length (encrypted): 21d0122c
    Encrypted Packet: 127bb7f4cb7807b70c3327dc11ad10a4882507f26
```

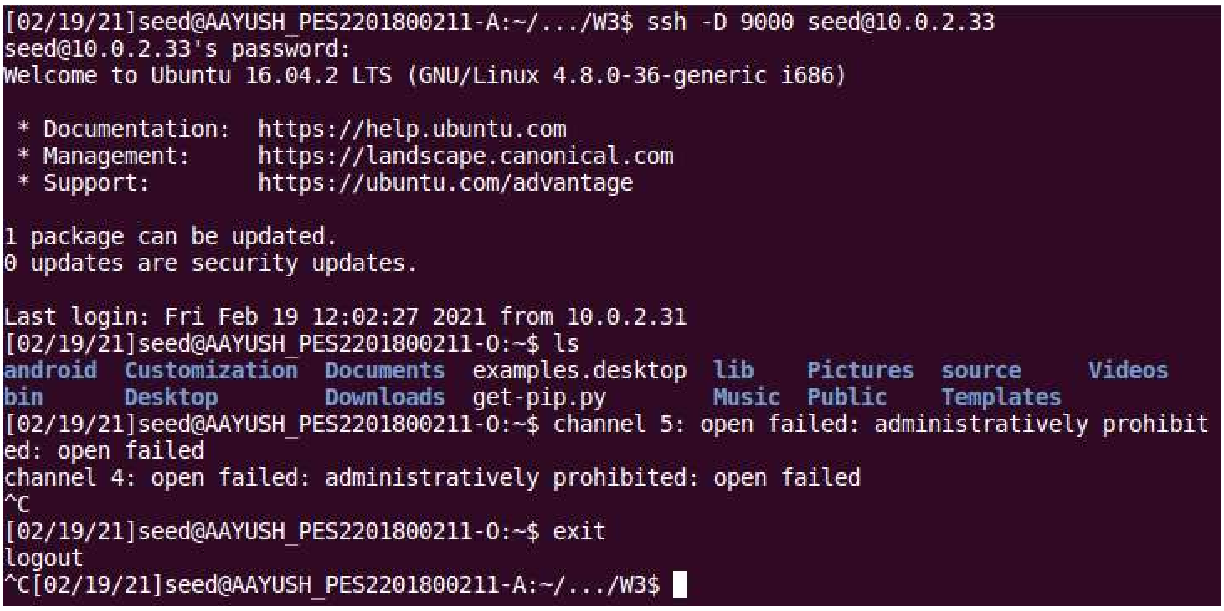
No.: 3 · Time: 2021-02-19 12:30:52.621495165 · Sou…th: 312 · Info: Client: Encrypted packet (len=244)



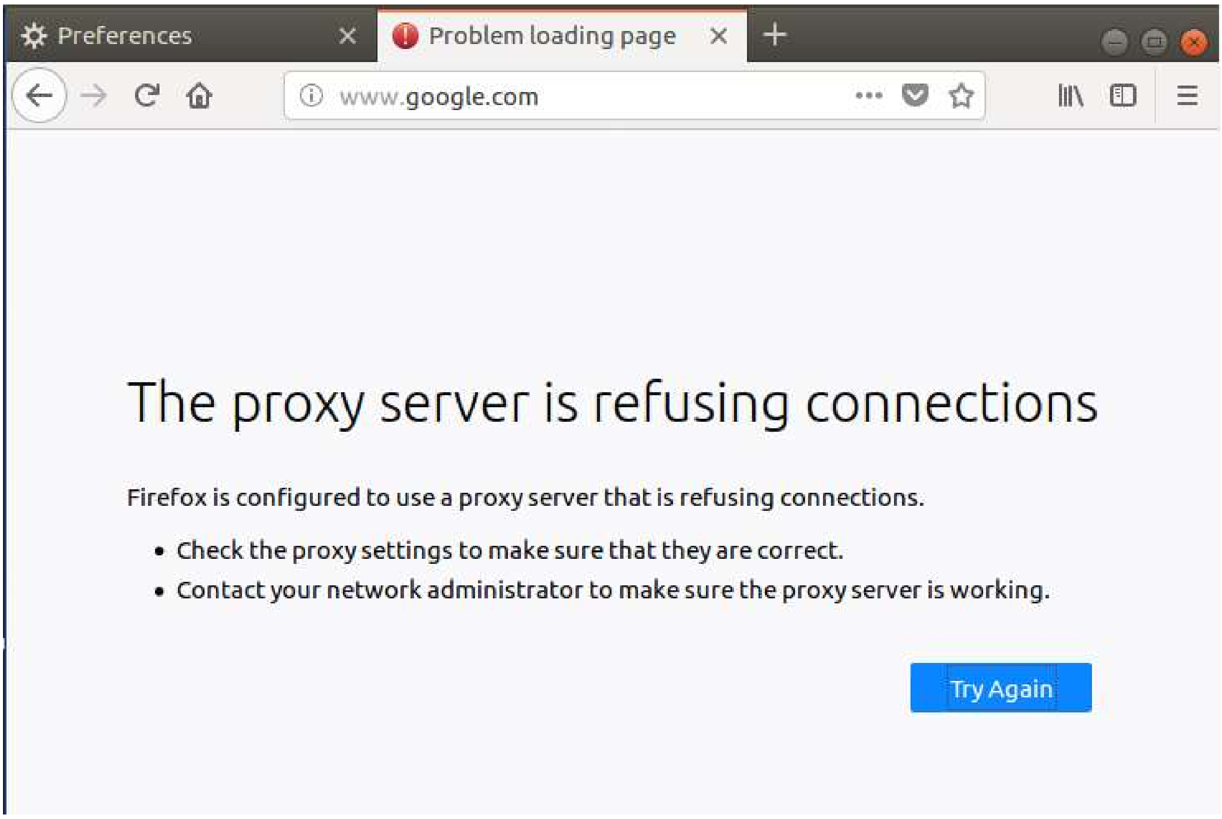
```
No.   Time                              Source           Destination      Pr
    1 2021-02-19 12:31:32.6603762…  10.0.2.31        10.0.2.33        SS
    2 2021-02-19 12:31:32.6603991…  10.0.2.33        10.0.2.31        TC
    3 2021-02-19 12:31:32.6609793…  10.0.2.33        172.217.27.196   TL
    4 2021-02-19 12:31:32.7530262…  172.217.27.196   10.0.2.33        TC
    5 2021-02-19 12:31:32.9289698…  172.217.27.196   10.0.2.33        TL
    6 2021-02-19 12:31:32.9293715…  10.0.2.33        10.0.2.31        SS
    7 2021-02-19 12:31:32.9327062…  10.0.2.31        10.0.2.33        TC
    8 2021-02-19 12:31:32.9696665…  10.0.2.33        172.217.27.196   TC
```

```
▶ Frame 3: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on inter
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.0.2.33, Dst: 172.217.27.196
▶ Transmission Control Protocol, Src Port: 37212, Dst Port: 443, Seq: 3744704512,
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 133
      Encrypted Application Data: 000000000000000f590a83813963c6818c66b4a1758c36c
```

1st capture we see the packet from VM1 to VM3 and then in this pic we capture from VM3 to google.com IP.



```
[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ ssh -D 9000 seed@10.0.2.33
seed@10.0.2.33'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

1 package can be updated.
0 updates are security updates.

Last login: Fri Feb 19 12:02:27 2021 from 10.0.2.31
[02/19/21]seed@AAYUSH_PES2201800211-O:~$ ls
android  Customization  Documents  examples.desktop  lib    Pictures  source     Videos
bin      Desktop        Downloads  get-pip.py        Music  Public    Templates
[02/19/21]seed@AAYUSH_PES2201800211-O:~$ channel 5: open failed: administratively prohibit
ed: open failed
channel 4: open failed: administratively prohibited: open failed
^C
[02/19/21]seed@AAYUSH_PES2201800211-O:~$ exit
logout
^C[02/19/21]seed@AAYUSH_PES2201800211-A:~/.../W3$ 
```



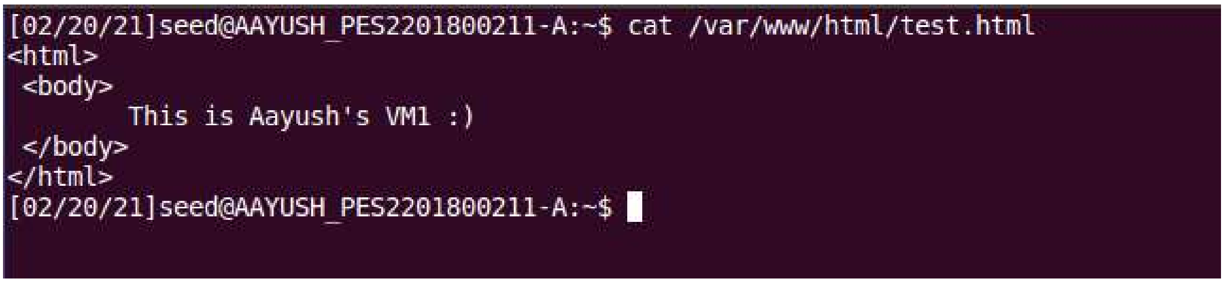
The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

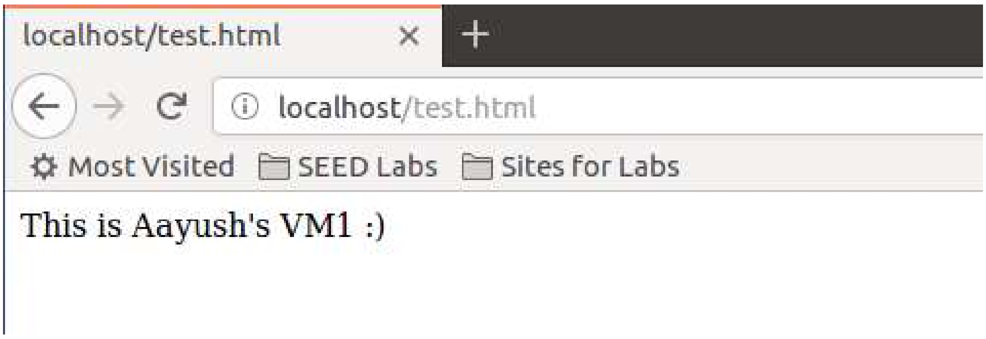
On destroying the tunnel as seen above i.e on exiting and deleting browser cache we are not able to reach the google site and the proxy server is refusing connections.

TASK 4:



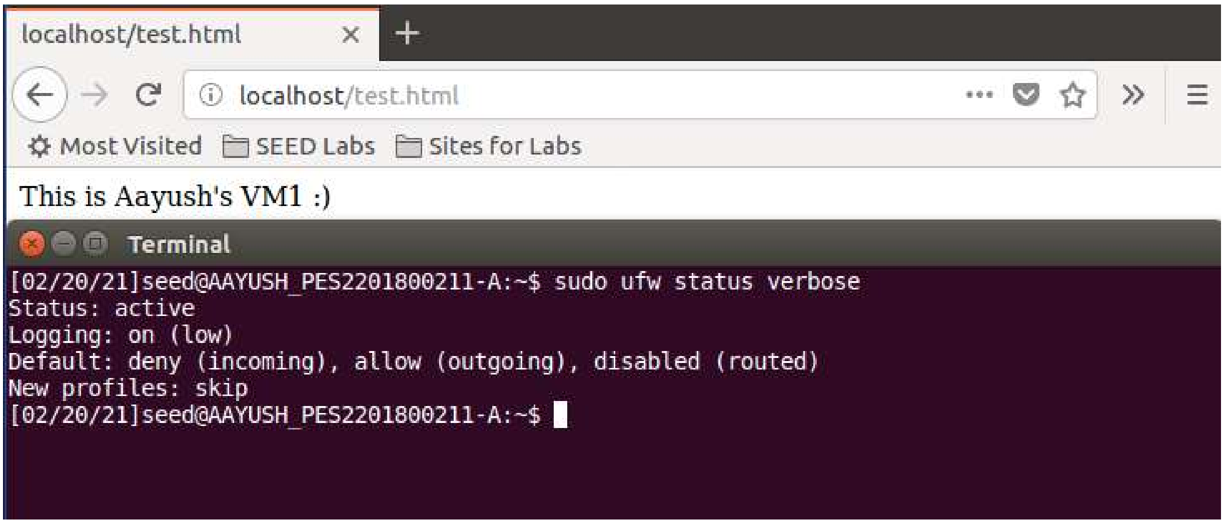
```
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ cat /var/www/html/test.html
<html>
 <body>
        This is Aayush's VM1 :)
 </body>
</html>
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ 
```

The test.html code.



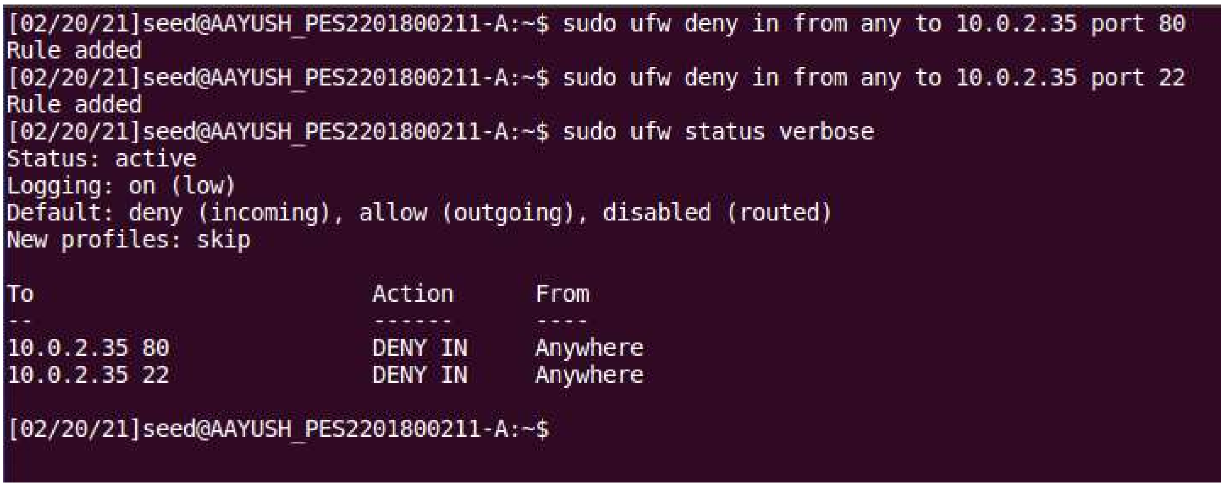
This is Aayush's VM1 :)

We are able to reach the test.html stored on VM1 from VM2.



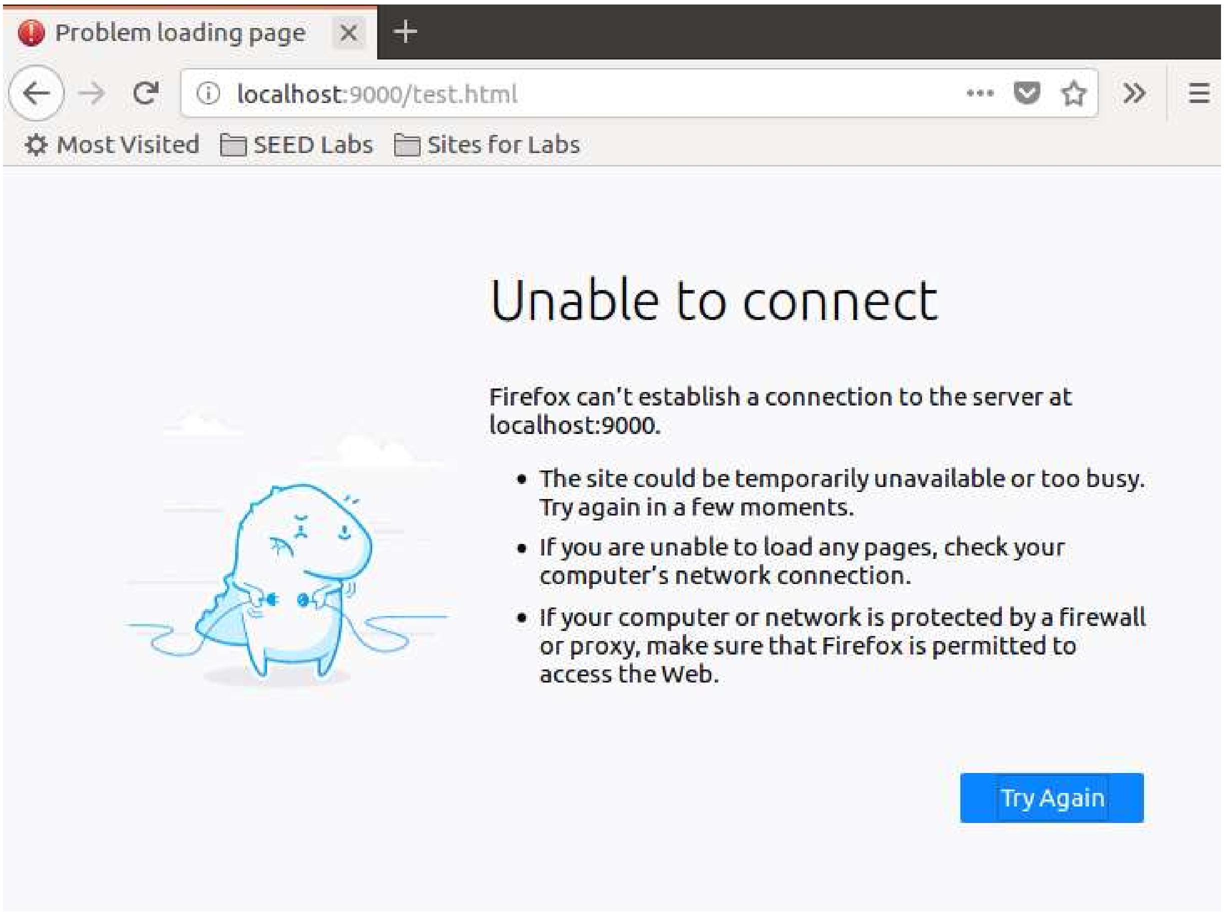
This is Aayush's VM1 :)

```
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ 
```



```
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ sudo ufw deny in from any to 10.0.2.35 port 80
Rule added
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ sudo ufw deny in from any to 10.0.2.35 port 22
Rule added
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
10.0.2.35 80               DENY IN     Anywhere
10.0.2.35 22               DENY IN     Anywhere

[02/20/21]seed@AAYUSH_PES2201800211-A:~$
```

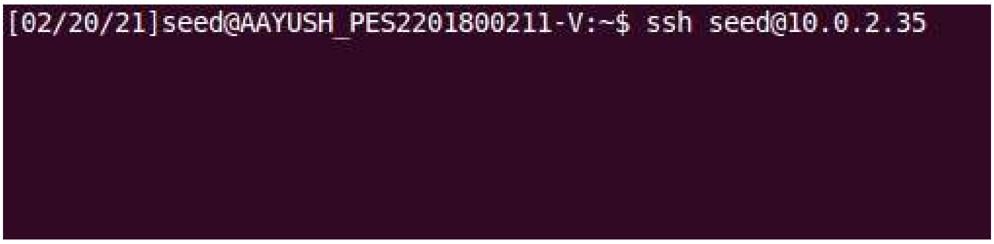
Now, on adding rules to prevent the traffic to VM1 and on port 80 i.e http and ssh port 22. We are unable to reach the webpage as shown below.



Unable to connect

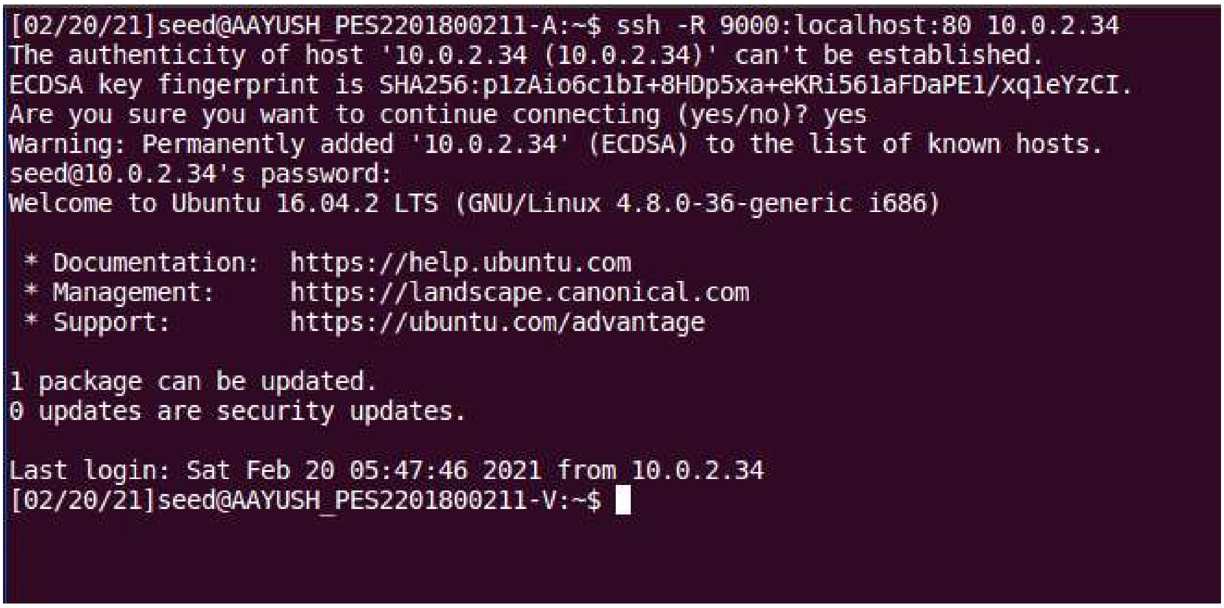
Firefox can't establish a connection to the server at localhost:9000.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.



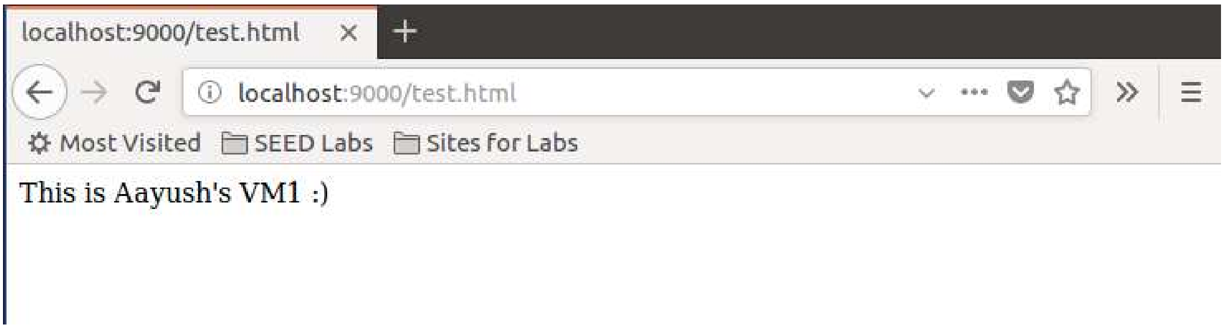
```
[02/20/21]seed@AAYUSH_PES2201800211-V:~$ ssh seed@10.0.2.35
```

We also try to ssh to other VM1 and the connection was unsuccessful.

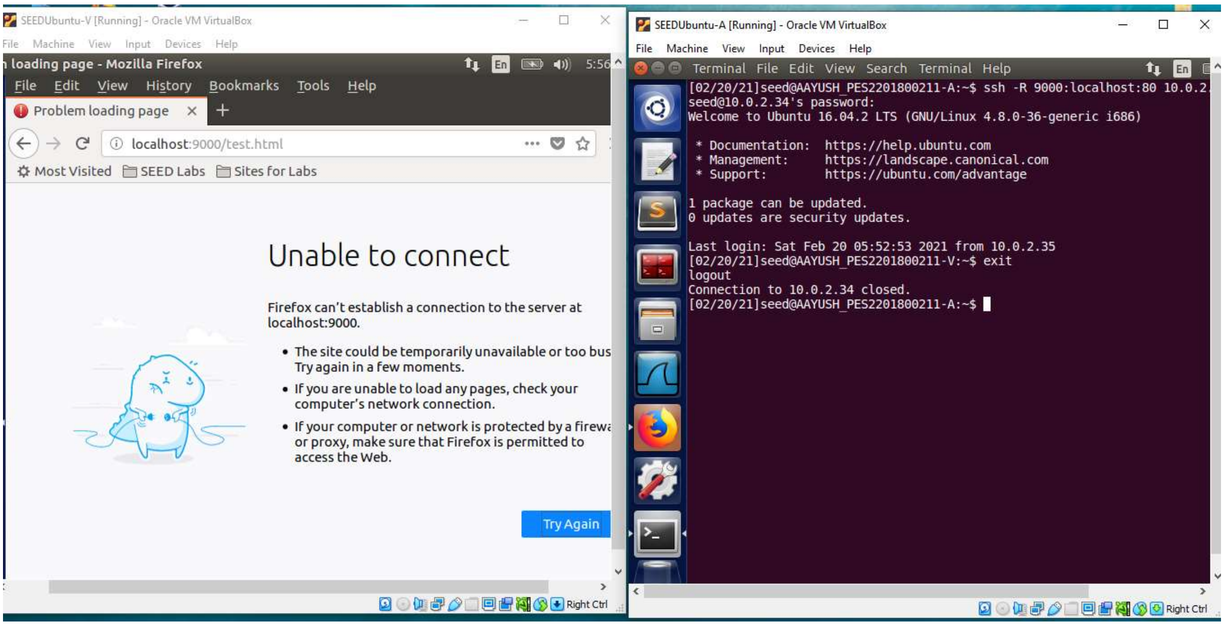


```
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ ssh -R 9000:localhost:80 10.0.2.34
The authenticity of host '10.0.2.34 (10.0.2.34)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.34' (ECDSA) to the list of known hosts.
seed@10.0.2.34'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

1 package can be updated.
0 updates are security updates.

Last login: Sat Feb 20 05:47:46 2021 from 10.0.2.34
[02/20/21]seed@AAYUSH_PES2201800211-V:~$
```

Now we create a tunnel on port 9000 to get the http traffic from VM2. Voila we get the test.html page as shown below on port 9000.



This is Aayush's VM1 :)


SEEDUbuntu-V [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Problem loading page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Problem loading page
localhost:9000/test.html
Most Visited
SEED Labs
Sites for Labs
Try Again
Right Ctrl
SEEDUbuntu-A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
Right Ctrl

Unable to connect

Firefox can't establish a connection to the server at localhost:9000.

- The site could be temporarily unavailable or too bus Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewa or proxy, make sure that Firefox is permitted to access the Web.

```
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ ssh -R 9000:localhost:80 10.0.2.
seed@10.0.2.34'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

1 package can be updated.
0 updates are security updates.

Last login: Sat Feb 20 05:52:53 2021 from 10.0.2.35
[02/20/21]seed@AAYUSH_PES2201800211-V:~$ exit
logout
Connection to 10.0.2.34 closed.
[02/20/21]seed@AAYUSH_PES2201800211-A:~$ 
```

On destroying the ssh tunnel connection we lose the ability to reach the webpage via 9000 port.