

LAB 17

Varun Gunda
A20453991

2.1 Task 1: Using Firewall

Notes: 10.0.2.10 (A) from 10.0.2.9(B)

```
telnet addi. 10.0.2.10 scope:host
[04/29/20]seed@VM:~$ telnet 10.0.2.10
Trying 10.0.2.10...
Connected to 10.0.2.10.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM 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.

[04/29/20]seed@VM:~$
```

As seen above, initially, we were able to connect to 10.0.2.10 (A) from 10.0.2.9(B) over telnet but after adding entry in iptable to reject packets, we were not able to connect.

```
[04/29/20]seed@VM:~/.../lab17$ sudo iptables
s -A INPUT -p TCP --dport 23 -j REJECT -s 1
0.0.2.9
```

Command to prevent B from doing telnet to Machine A is above

```
[04/29/20]seed@VM:~/.../lab17$ sudo iptables -A OUTPUT -p TCP -j REJECT -d 10.0.2.9
[04/29/20]seed@VM:~/.../lab17$ telnet 10.0.2.9
Trying 10.0.2.9...
telnet: Unable to connect to remote host: Connection refused
[04/29/20]seed@VM:~/.../lab17$ sudo iptables -D OUTPUT -p TCP -j REJECT -d 10.0.2.9
[04/29/20]seed@VM:~/.../lab17$ telnet 10.0.2.9
Trying 10.0.2.9...
Connected to 10.0.2.9.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: ^CConnection closed by foreign host.
```

Command to prevent connection from A to B:

```
[04/29/20]seed@VM:~/.../lab17$ sudo iptables -A OUTPUT -p TCP -j REJECT -d 10.0.2.9 --dport 23
[04/29/20]seed@VM:~/.../lab17$ telnet 10.0.2.9
Trying 10.0.2.9...
telnet: Unable to connect to remote host: Connection refused
```

```
[04/29/20]seed@VM:~/.../lab17$ sudo ufw reject out to 208.80.154.232
Skipping adding existing rule
[04/29/20]seed@VM:~/.../lab17$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

Firefox Web Browser	Action	From
172.217.12.132	REJECT OUT	Anywhere
208.80.154.232	REJECT OUT	Anywhere

```
[04/29/20]seed@VM:~/.../lab17$ ping www.wikipedia.com | head -3
PING ncredir-lb.wikimedia.org (208.80.154.232) 56(84) bytes of data.
From 10.0.2.10 icmp_seq=1 Destination Port Unreachable
From 10.0.2.10 icmp_seq=1 Destination Port Unreachable
```

As seen above, command to allow external website wikipedia.com

Task 2: Implementing a Simple Firewall

The code for this is as shown below:

```
Makefile x netfilter.c x
1 #include <linux/kernel.h>
2 #include <linux/module.h>
3 #include <linux/netfilter.h>
4 #include <linux/netfilter_ipv4.h>
5 #include <linux/ip.h>
6 #include <linux/tcp.h>
7
8 static struct nf_hook_ops telnetFilterHook;
9
10
11 unsigned int telnetFilter(void *priv, struct sk_buff *skb,
12                          const struct nf_hook_state *state)
13 {
14     struct iphdr *iph;
15     struct tcphdr *tcph;
16
17     unsigned int s1,s2,s3,s4, d1,d2,d3,d4;
18
19     iph = ip_hdr(skb);
20     tcph = (void *)iph+iph->ihl*4;
21
22     //Finding source and destination addresses
23     s1 = ((unsigned char *)&iph->saddr)[0];
24     s2 = ((unsigned char *)&iph->saddr)[1];
25     s3 = ((unsigned char *)&iph->saddr)[2];
26     s4 = ((unsigned char *)&iph->saddr)[3];
27
28     d1 = ((unsigned char *)&iph->daddr)[0];
29     d2 = ((unsigned char *)&iph->daddr)[1];
30     d3 = ((unsigned char *)&iph->daddr)[2];
31     d4 = ((unsigned char *)&iph->daddr)[3];
32
33
34     //Preventing telnet connection from 10.0.2.9
35     if(iph->protocol == IPPROTO_TCP && tcph->dest == htons(23) && d1==10 && d2==0 && d3==2 && d4==9)
36     {
37         printk(KERN_INFO "Dropping telnet packet to %d.%d.%d.%d\n",
38                ((unsigned char *)&iph->daddr)[0],
39                ((unsigned char *)&iph->daddr)[1],
40                ((unsigned char *)&iph->daddr)[2],
41                ((unsigned char *)&iph->daddr)[3]);
42         return NF_DROP;
43     }
44 }
```

```

43     }
44     //Preventing telnet connection to 10.0.2.9
45     else if(iph->protocol == IPPROTO_TCP && tcp->dest == htons(23) && s1==10 && s2==0 && s3==2 && s4==10)
46     {
47         printk(KERN_INFO "Dropping telnet packet from %d.%d.%d.%d\n",
48             ((unsigned char *)&iph->saddr) [0],
49             ((unsigned char *)&iph->saddr) [1],
50             ((unsigned char *)&iph->saddr) [2],
51             ((unsigned char *)&iph->saddr) [3]
52         );
53         return NF_DROP;
54     }
55
56     //Preventing telnet connection to 10.0.2.9
57     else if(iph->protocol == IPPROTO_TCP && tcp->dest == htons(22) && d1==10 && d2==0 && d3==2 && d4==9)
58     {
59         printk(KERN_INFO "Dropping SSH packet to %d.%d.%d.%d\n",
60             ((unsigned char *)&iph->daddr) [0],
61             ((unsigned char *)&iph->daddr) [1],
62             ((unsigned char *)&iph->daddr) [2],
63             ((unsigned char *)&iph->daddr) [3]
64         );
65         return NF_DROP;
66     }
67
68     //Preventing all outgoing ftp packets
69     else if (iph->protocol == IPPROTO_TCP && tcp->dest == htons(21)) {
70         printk(KERN_INFO "Dropping ftp packet to %d.%d.%d.%d\n",
71             ((unsigned char *)&iph->daddr) [0],
72             ((unsigned char *)&iph->daddr) [1],
73             ((unsigned char *)&iph->daddr) [2],
74             ((unsigned char *)&iph->daddr) [3]);
75         return NF_DROP;
76     }
77
78     //Preventing connection to www.wikipedia.com
79     else if(iph->protocol == IPPROTO_TCP && d1==208 && d2==80 && d3==154 && d4==232)
80     {
81         printk(KERN_INFO "Dropping tcp packet to wikipedia.com\n",
82             ((unsigned char *)&iph->daddr) [0],
83             ((unsigned char *)&iph->daddr) [1],
84             ((unsigned char *)&iph->daddr) [2],
85             ((unsigned char *)&iph->daddr) [3]
86         );
87         return NF_DROP;

```

Wireshark

```

84     ((unsigned char *)&iph->daddr) [4],
85     ((unsigned char *)&iph->daddr) [3]
86     );
87     return NF_DROP;
88 }
89
90 else {
91     return NF_ACCEPT;
92 }
93 }
94
95 int setUpFilter(void) {
96     printk(KERN_INFO "Registering a Telnet filter.\n");
97     telnetFilterHook.hook = telnetFilter;
98     telnetFilterHook.hooknum = NF_INET_POST_ROUTING;
99     telnetFilterHook.pf = PF_INET;
100    telnetFilterHook.priority = NF_IP_PRI_FIRST;
101
102    // Register the hook.
103    nf_register_hook(&telnetFilterHook);
104    return 0;
105 }
106
107 void removeFilter(void) {
108     printk(KERN_INFO "Telnet filter is being removed.\n");
109     nf_unregister_hook(&telnetFilterHook);
110 }
111
112 module_init(setUpFilter);
113 module_exit(removeFilter);
114
115 MODULE_LICENSE("GPL");

```

Now built and installed the module as shown below:

```

[04/30/20]seed@VM:~/lab17_codes$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed/lab17_codes modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
CC [M] /home/seed/lab17_codes/netfilter.o
In file included from ./include/linux/printk.h:6:0,
                 from ./include/linux/kernel.h:13,
                 from /home/seed/lab17_codes/netfilter.c:1:
/home/seed/lab17_codes/netfilter.c: In function 'telnetFilter':
./include/linux/kern_levels.h:4:18: warning: too many arguments for format [-Wformat-extra-args]
#define KERN_SOH "\001" /* ASCII Start Of Header */
                        ^
./include/linux/kern_levels.h:13:19: note: in expansion of macro 'KERN_SOH'
#define KERN_INFO KERN_SOH "6" /* informational */
                        ^
/home/seed/lab17_codes/netfilter.c:81:16: note: in expansion of macro 'KERN_INFO'
    printk(KERN_INFO "Dropping tcp packet to wikipedia.com\n",
               ^
Building modules, stage 2.
MODPOST 1 modules
CC /home/seed/lab17_codes/netfilter.mod.o
LD [M] /home/seed/lab17_codes/netfilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[04/30/20]seed@VM:~/lab17_codes$ sudo insmod netfilter.ko

```

Preventing connection from A to B

```
[04/30/20]seed@VM:~/lab17_codes$ telnet 10.0.2.9
Trying 10.0.2.9...
```

```
[ 1794.167939] Registering a telnet filter.
[ 1796.214121] Dropping telnet packet to 10.0.2.9
[ 1797.213672] Dropping telnet packet to 10.0.2.9
[ 1799.235489] Dropping telnet packet to 10.0.2.9
```

Preventing connection from A to B

```
[04/29/20]seed@VM:~$ telnet 10.0.2.10
Trying 10.0.2.10...
telnet: Unable to connect to remote host:
No route to host
```

```
1722.520409] Dropping telnet packet from 10.0.2.9
1723.522399] Dropping telnet packet from 10.0.2.9
1725.537609] Dropping telnet packet from 10.0.2.9
1729.727342] Dropping telnet packet from 10.0.2.9
1737.015355] Dropping telnet packet from 10.0.2.9
```

Dropping ftp packets to B

```
[04/30/20]seed@VM:~/lab17_codes$ ftp 10.0.2.9
ftp: connect: Connection timed out
ftp> exit
[04/30/20]seed@VM:~/lab17_codes$
```

```
[ 2687.513121] Dropping ftp packet to 10.0.2.9
[ 2688.511733] Dropping ftp packet to 10.0.2.9
[ 2690.526887] Dropping ftp packet to 10.0.2.9
[ 2694.620890] Dropping ftp packet to 10.0.2.9
```

Dropping packets to wikipedia.com

```
[ 3269.620489] Registering a Telnet filter.  
[ 3290.872231] Dropping packet to wikipedia.com  
[ 3291.890597] Dropping packet to wikipedia.com  
[ 3293.905597] Dropping packet to wikipedia.com
```

2.3 Task 3: Evading Egress Filtering

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

The following rules were added to deny telnet connections

```
[05/01/20]seed@VM:~$ sudo ufw deny out 23/tcp  
Rule added  
Rule added (v6)
```

```
[05/01/20]seed@VM:~$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: allow (incoming), allow (outgoing), disabled (routed)  
New profiles: skip
```

To	Action	From
--	-----	----
172.217.12.132	REJECT OUT	Anywhere
208.80.154.232	REJECT OUT	Anywhere
23/tcp	DENY OUT	Anywhere
23/tcp (v6) (v6)	DENY OUT	Anywhere

Now establishing a tunnel :

```
[05/01/20]seed@VM:~$ ssh -L 8000:10.0.2.9:23 seed@10.0.2.9
The authenticity of host '10.0.2.9 (10.0.2.9)' 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 '10.0.2.9' (ECDSA) to the list of known hosts.
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.canoni
```


Connecting to B now works:

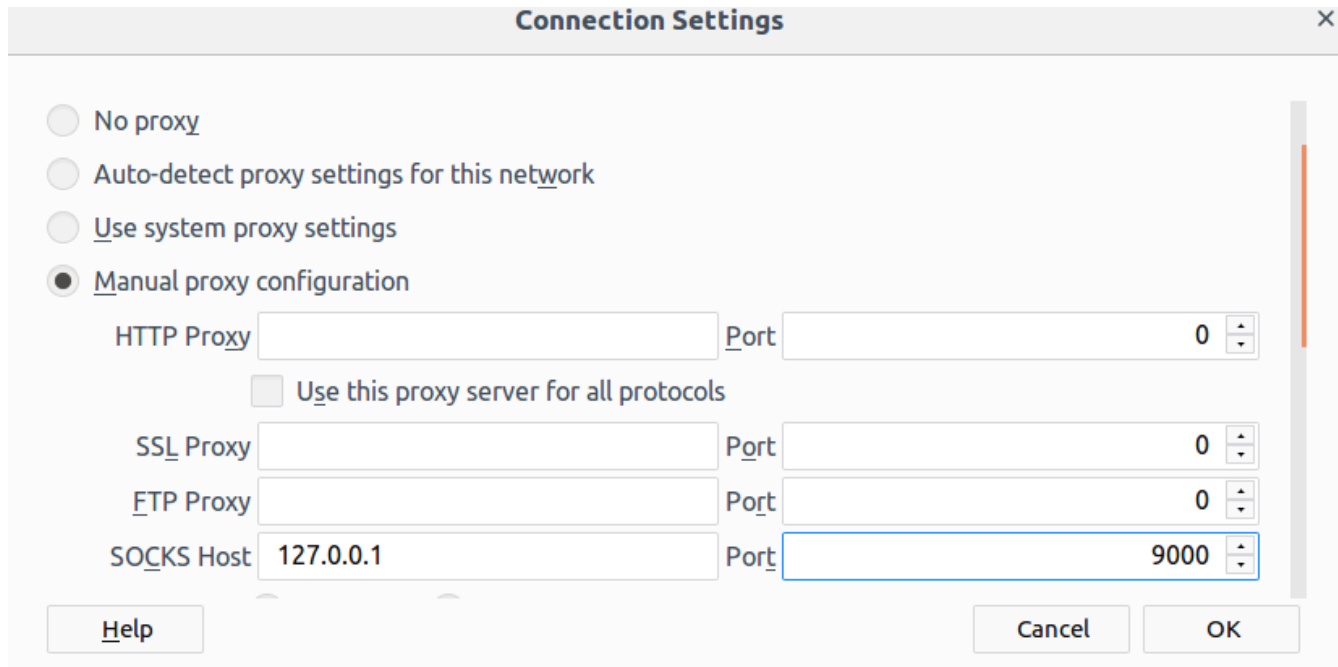
```
[05/01/20]seed@VM:~$ telnet 10.0.2.9
Trying 10.0.2.9...
Connected to 10.0.2.9.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri May  1 01:17:50 EDT 2020 fr
om 10.0.2.10 on pts/4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.
8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canoni
cal.com
 * Support:       https://ubuntu.com/advan
tage

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

Task 3.b: Connect to iit.edu using SSH Tunnel.

Following settings and commands to block iit.edu



Connection Settings

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy Port

☐ Use this proxy server for all protocols

SSL Proxy Port

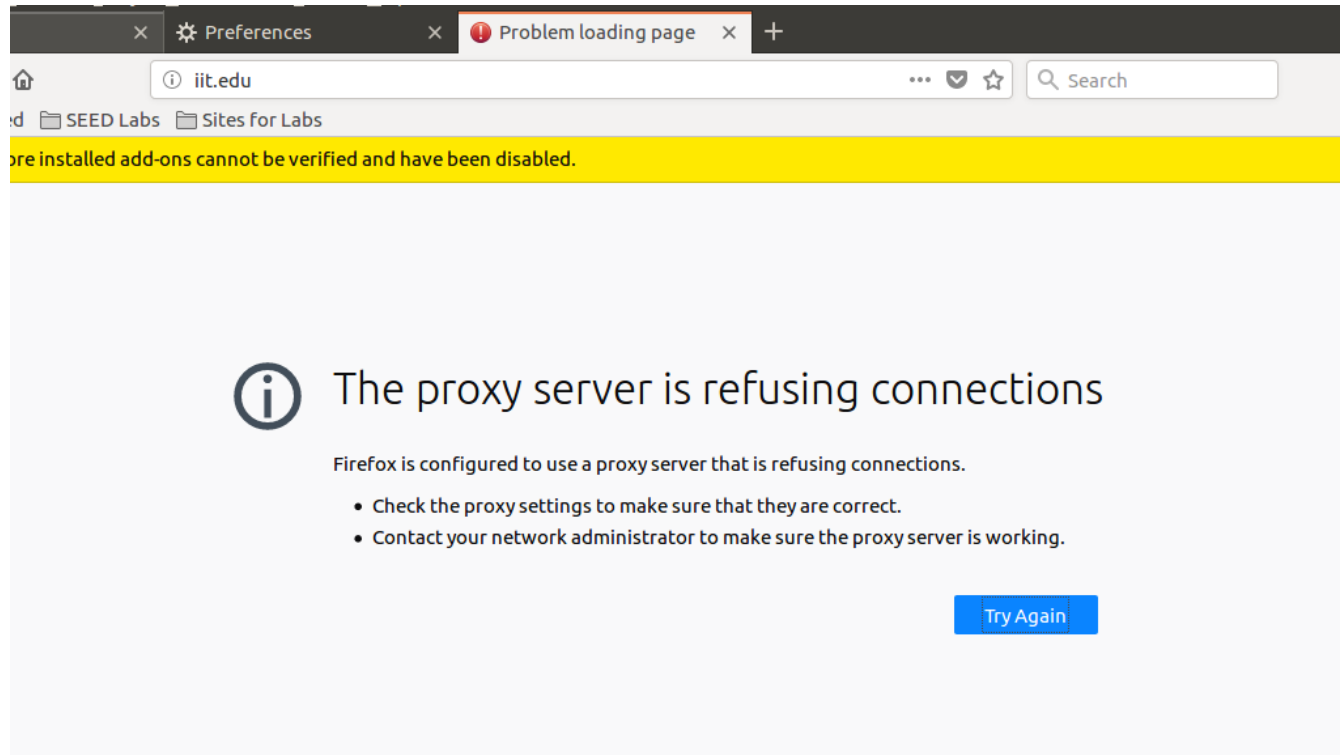
FTP Proxy Port

SOCKS Host Port

[Help](#) [Cancel](#) [OK](#)

```
[05/01/20]seed@VM:~$ sudo ufw deny out to 174.14  
3.130.167  
Rules updated
```

As seen here iit.edu can't be accessed



Establishing ssh tunnel

```
[05/01/20]seed@VM:~$ ssh -D 9000 -C 10.0.2.9
The authenticity of host '10.0.2.9 (10.0.2.9)' 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 '10.0.2.9' (ECDSA) to the list of known hosts.
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

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

Last login: Fri May  1 01:29:42 2020 from 10.0.2.9
[05/01/20]seed@VM:~$
```

Now I can ping iit.edu as seen below

```
[05/01/20]seed@VM:~$ ping iit.edu
PING iit.edu (174.143.130.167) 56(84) bytes of data.
64 bytes from www-c2.iit.edu (174.143.130.167):
icmp_seq=1 ttl=49 time=48.1 ms
64 bytes from www-c2.iit.edu (174.143.130.167):
icmp_seq=2 ttl=49 time=44.1 ms
^C
--- iit.edu ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 44.195/46.188/48.181/1.993 ms
```

The image shows a Wireshark packet capture of an SSH session. The top pane displays a list of packets, with packet 110 selected. The middle pane shows the details of the selected packet, which is an SSH Client: Encrypted packet (len=44). The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-05-01 02:06:08.5893914...	10.0.2.10	10.0.2.9	SSH	110	Client: Encrypted packet (len=44)
2	2020-05-01 02:06:08.5902123...	10.0.2.9	10.0.2.10	TCP	66	22 → 46514 [ACK] Seq=3666207509 Ack=281241...
3	2020-05-01 02:06:08.5910718...	10.0.2.9	10.0.2.10	SSH	142	Server: Encrypted packet (len=76)
4	2020-05-01 02:06:08.5911048...	10.0.2.10	10.0.2.9	TCP	66	46514 → 22 [ACK] Seq=2812416313 Ack=366620...
5	2020-05-01 02:06:08.7435888...	10.0.2.10	10.0.2.9	SSH	110	Client: Encrypted packet (len=44)
6	2020-05-01 02:06:08.7450811...	10.0.2.9	10.0.2.10	SSH	142	Server: Encrypted packet (len=76)
7	2020-05-01 02:06:08.7451488...	10.0.2.10	10.0.2.9	TCP	66	46514 → 22 [ACK] Seq=2812416357 Ack=366620...
8	2020-05-01 02:06:08.9035373...	10.0.2.10	10.0.2.9	SSH	110	Client: Encrypted packet (len=44)
9	2020-05-01 02:06:08.9056522...	10.0.2.9	10.0.2.10	SSH	158	Server: Encrypted packet (len=92)

Transmission Control Protocol, Src Port: 46514, Dst Port: 22, Seq: 2812416269, Ack: 3666207509, Len: 44

Source Port: 46514
Destination Port: 22
[Stream index: 0]
[TCP Segment Len: 44]
Sequence number: 2812416269
[Next sequence number: 2812416313]
Acknowledgment number: 3666207509
Header Length: 32 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 2048

0000 08 00 27 5c 57 94 08 00 27 c4 f2 d5 08 00 45 10 ..\W... ..E.
0010 00 60 46 43 40 00 40 06 dc 32 0a 00 02 0a 0a 00 .FC@. .2.....
0020 02 09 b5 b2 00 16 a7 a2 11 0d da 85 e3 15 80 18
0030 01 7d 18 65 00 00 01 01 08 0a 00 0d 09 05 00 0b .}.e.....
0040 99 6a 2f c6 81 d7 ce 6f 00 74 1e a1 d3 1c 13 68 .j/...o .t....h
0050 5d ff 05 13 0b 47 75 80 59 99 07 e5 44 e4 1d db]....Gu. Y...D..
0060 50 67 c5 fc 48 c9 50 c0 3a 5d 30 4b 79 74 Pg...H.P. :]0Kyt

1. Run Firefox and go visit the iit.edu page. Can you see the iit.edu page? Please describe your observation.

Yes I can see the iit.edu page. It works with the help of established tunnel.

2. After you get the iit.edu page, break the SSH tunnel, clear the Firefox cache, and try the connection again. Please describe your observation.

Since the tunnel is broke, we cant access iit.edu anymore as it is denied

3. Establish the SSH tunnel again and connect to iit.edu. Describe your observation.

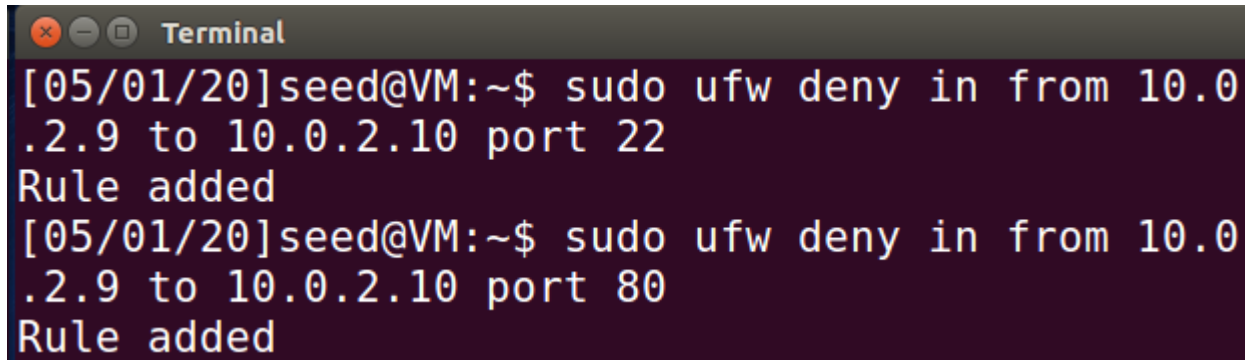
It works this time.

4. Please explain what you have observed, especially on why the SSH tunnel can help bypass the egress filtering. You should use Wireshark to see what exactly is happening on the wire. Please describe your observations and explain them using the packets that you have captured.

The communication is happening between B and iit.edu and A to B and this is how A is able to access iit.edu

Task 4: Evading Ingress Filtering

Blocking incoming connections to port 22 and 80 on A

A terminal window titled "Terminal" with a dark background and light-colored text. It shows two commands being executed to block incoming connections to ports 22 and 80 from the IP range 10.0.2.9 to 10.0.2.10. The first command is "sudo ufw deny in from 10.0.2.9 to 10.0.2.10 port 22" and the second is "sudo ufw deny in from 10.0.2.9 to 10.0.2.10 port 80". Both commands are followed by the output "Rule added".

```
[05/01/20]seed@VM:~$ sudo ufw deny in from 10.0.2.9 to 10.0.2.10 port 22
Rule added
[05/01/20]seed@VM:~$ sudo ufw deny in from 10.0.2.9 to 10.0.2.10 port 80
Rule added
```


Establishing ssh connection.

```
[05/01/20]seed@VM:~$ ssh localhost -p 8001
The authenticity of host '[localhost]:8001 ([127.0.0.1]:8001)' 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 '[localhost]:8001' (ECDSA) to the list of known hosts.
seed@localhost'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 May  1 02:16:32 2020 from 10.0.2.9
[05/01/20]seed@VM:~$
```

As seen below, I can access apache server over port 8000.

