LAB 17
Varun Gunda
A20453991

2.1 Task 1: Using Firewall

Notes: 10.0.2.10 (A) from 10.0.2.9(B)

```
[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 iptable
s -A INPUT -p TCP --dport 23 -j REJECT -s 1
0.0.2.9
```

Command to prevent B from doing telnet to Machine Ais above

```
[04/29/20]seed@VM:~/.../lab17$ sudo iptable[04/29/20]seed@VM:~/.../lab17$ sudo iptables -A OU
TPUT -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 2
3
[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 | netfilter.c

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

static struct nf_hook_ops telnetFilterHook;


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

    unsigned int s1,s2,s3,s4, d1,d2,d3,d4;

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

    //Finding source and destination addresses
    s1 = ((unsigned char *)&iph->saddr)[0];
    s2 = ((unsigned char *)&iph->saddr)[1];
    s3 = ((unsigned char *)&iph->saddr)[2];
    s4 = ((unsigned char *)&iph->saddr)[3];

    d1 = ((unsigned char *)&iph->daddr)[0];
    d2 = ((unsigned char *)&iph->daddr)[1];
    d3 = ((unsigned char *)&iph->daddr)[2];
    d4 = ((unsigned char *)&iph->daddr)[3];


    //Preventing telnet connection from 10.0.2.9
    if(iph->protocol == IPPROTO_TCP && tcph->dest == htons(23) && d1==10 && d2==0 && d3==2 && d4==9)
    {
        printk(KERN_INFO "Dropping telnet packet to %d.%d.%d.%d\n",
        ((unsigned char *)&iph->daddr) [0],
        ((unsigned char *)&iph->daddr) [1],
        ((unsigned char *)&iph->daddr) [2],
        ((unsigned char *)&iph->daddr) [3]);
        return NF_DROP;
    }
```

```
43      }
44      //Preventing telnet connection to 10.0.2.9
45      else if(iph->protocol == IPPROTO_TCP && tcph->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 && tcph->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          );
Wireshark   return NF_DROP;
66      }
67
68      //Preventing all outgoing ftp packets
69      else if (iph->protocol == IPPROTO_TCP && tcph->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;
```

```
        ((unsigned char *)&iph->daddr) [2],
        ((unsigned char *)&iph->daddr) [3]
        );
        return NF_DROP;
    }

    else {
        return NF_ACCEPT;
    }
}

int setUpFilter(void) {
        printk(KERN_INFO "Registering a Telnet filter.\n");
        telnetFilterHook.hook = telnetFilter;
        telnetFilterHook.hooknum = NF_INET_POST_ROUTING;
        telnetFilterHook.pf = PF_INET;
        telnetFilterHook.priority = NF_IP_PRI_FIRST;

        // Register the hook.
        nf_register_hook(&telnetFilterHook);
        return 0;
}

void removeFilter(void) {
        printk(KERN_INFO "Telnet filter is being removed.\n");
        nf_unregister_hook(&telnetFilterHook);
}

module_init(setUpFilter);
module_exit(removeFilter);

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-ar
gs]
 #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...
```

```
[ 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
```

Dropping ftp packets to B

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

```
[ 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/t
cp
Rule added
Rule added (v6)
```

```
[05/01/20]seed@VM:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), dis
abled (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)                DENY OUT    Anywhere
(v6)
```

Now establishing a tunnel :

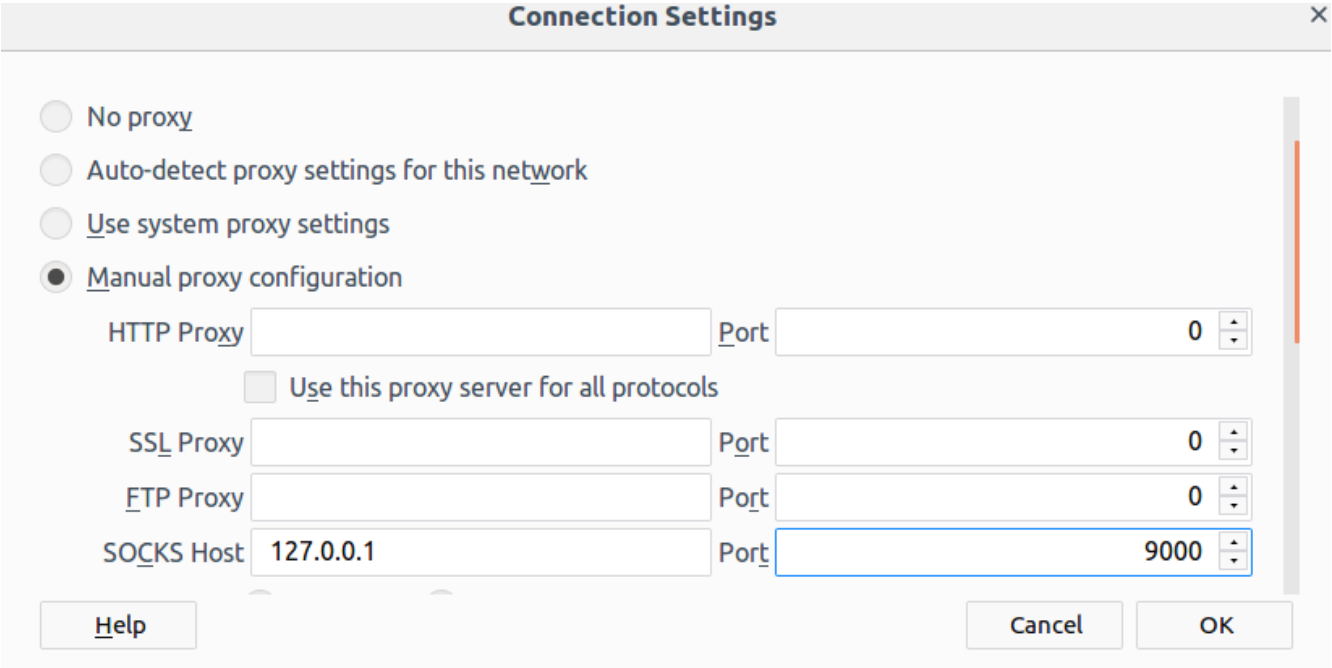
```
[05/01/20]seed@VM:~$ ssh -L 8000:10.0.2.9:2
3 seed@10.0.2.9
The authenticity of host '10.0.2.9 (10.0.2.
9)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI
+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connectin
g (yes/no)? yes
Warning: Permanently added '10.0.2.9' (ECDS
A) 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.
```

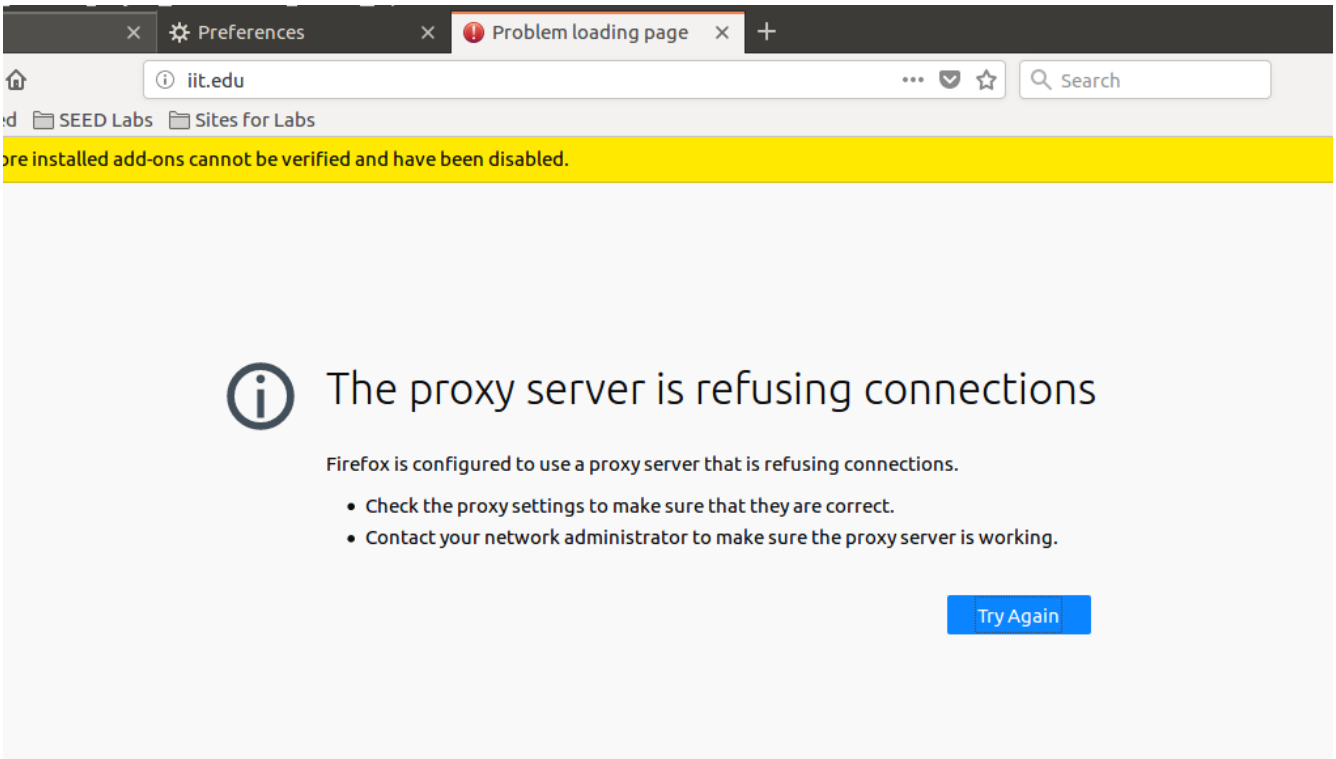
Task 3.b: Connect to iit.edu using SSH Tunnel.

Following settings and commands to block iit.edu




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

As seen here iit.edu can’tbe accessed

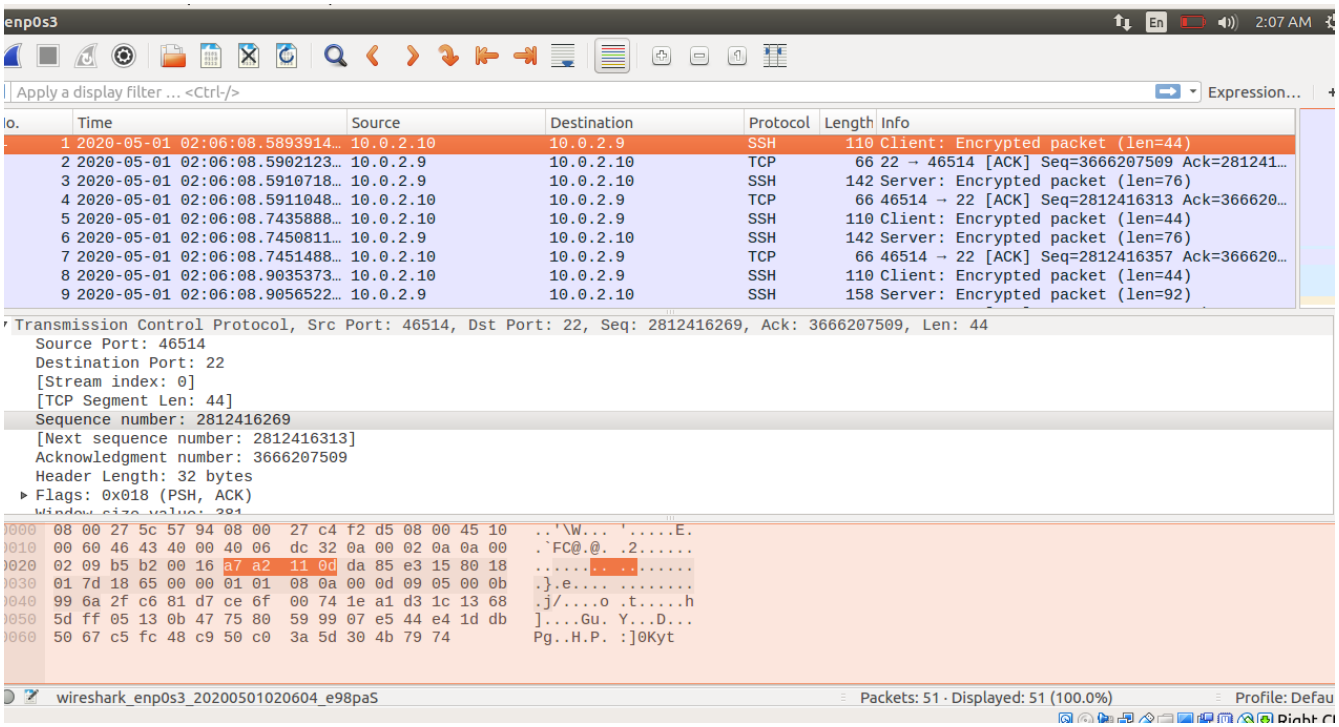


Establishing ssh tunnel

```
[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)' c
an't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp
5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (ye
s/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 4.8.0-3
6-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.c
om
 * 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 d
ata.
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 los
s, time 1001ms
rtt min/avg/max/mdev = 44.195/46.188/48.181/1.99
3 ms
```



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

```
Terminal
[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 ([12
7.0.0.1]:8001)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HD
p5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (y
es/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.