

Linux Firewall Exploration Lab

Task 1: Using Firewall on Machine A

Prevent A from doing telnet to machine B

```
sudo iptables -A OUTPUT -s 10.0.2.5 -d 10.0.2.15 -p tcp --dport 23 -j DROP
```

The screenshot shows a terminal window with the following content:

```
[03/30/20]seed@VM:~$ sudo iptables -A OUTPUT -s 10.0.2.5 -d 10.0.2.15 -p tcp --dport 23 -j DROP
[03/30/20]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:d2:78:ac
            inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fe80::900e:819f:d374:998a/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:186 errors:0 dropped:0 overruns:0 frame:0
            TX packets:289 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:66690 (66.6 KB) TX bytes:27389 (27.3 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:561 errors:0 dropped:0 overruns:0 frame:0
            TX packets:561 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:56644 (56.6 KB) TX bytes:56644 (56.6 KB)

[03/30/20]seed@VM:~$ telnet 10.0.2.15...
Trying 10.0.2.15...
```

The terminal window is part of a desktop environment, as evidenced by the window manager interface and icons in the dock.

Prevent B from doing telnet to machine A

```
sudo iptables -A INPUT -s 10.0.2.15 -d 10.0.2.5 -p tcp -dport 23 -j DROP
```

The screenshot shows a terminal window with the following content:

```
[03/30/20]seed@VM:~$ ifconfig
enp0s3  Link encap:Ethernet HWaddr 08:00:27:a1:23:df
        inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
        inet6 addr: fe80::7ebe:45a7:3ecc:b9de/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:196 errors:0 dropped:0 overruns:0 frame:0
              TX packets:161 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:24348 (24.3 KB) TX bytes:19630 (19.0 KB)

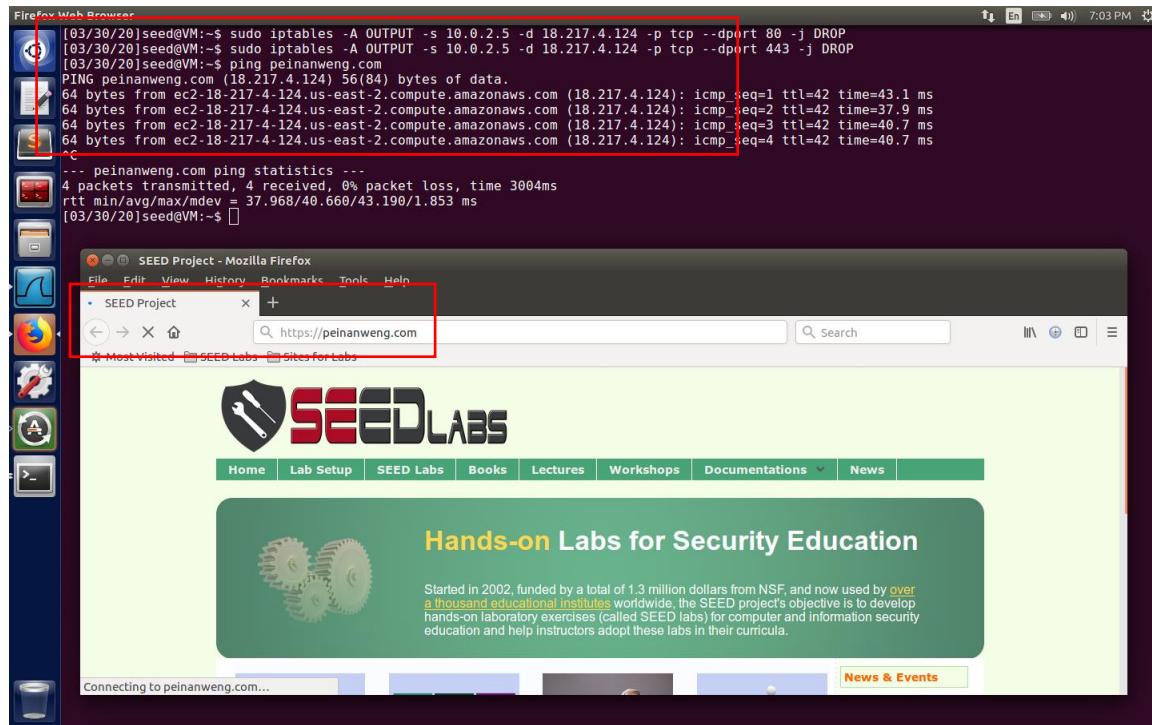
enp0s8  Link encap:Ethernet HWaddr 08:00:27:81:3d:07
        inet addr:192.168.60.1 Bcast:192.168.60.255 Mask:255.255.255.0
        inet6 addr: fe80::4bb6:b048:d936:c693/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:137 errors:0 dropped:0 overruns:0 frame:0
              TX packets:209 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:12091 (12.0 KB) TX bytes:15953 (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:598 errors:0 dropped:0 overruns:0 frame:0
              TX packets:598 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:63815 (63.8 KB) TX bytes:63815 (63.8 KB)

[03/30/20]seed@VM:~$ telnet 10.0.2.5
Trying 10.0.2.5...
```

Prevent A from visiting an external website (my personal website peinanweng.com)

```
sudo iptables -A OUTPUT -s 10.0.2.5 -d 18.217.4.124 -p tcp --dport 80 -j DROP  
sudo iptables -A OUTPUT -s 10.0.2.5 -d 18.217.4.124 -p tcp --dport 443 -j DROP
```



Task 2: Implementing a Simple Firewall

```
code netfilter.c

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

static struct nf_hook_ops in_filters_hook;
static struct nf_hook_ops post_routing_filters_hook;

void prn_pkt(char *info, unsigned char* saddr, unsigned char *daddr)
{
    printk(KERN_INFO "%s from %d.%d.%d.%d to %d.%d.%d.%d\n",
           info,
           saddr[0], saddr[1], saddr[2], saddr[3],
           daddr[0], daddr[1], daddr[2], daddr[3]
    );
}

unsigned int in_filter_hook_function(
    void *priv,
    struct sk_buff *skb,
    const struct nf_hook_state *state) {

    struct iphdr *iph;
    struct tcphdr *tcph;
    int host_B_ip = in_aton("10.0.2.15");

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

    // DROP TELNET packets from Machine B to Machine A
    if (iph->protocol == IPPROTO_TCP && ntohs(tcph->dest) == 23 &&
iph->saddr == host_B_ip) {
        prn_pkt("(IN) Dropping TELNET packets:", (unsigned
char*)&iph->saddr, (unsigned char*)&iph->daddr);
        return NF_DROP;
    }
    // DROP SSH packets from Machine B to Machine A
    else if (iph->protocol == IPPROTO_TCP && ntohs(tcph->dest) == 22
&& iph->saddr == host_B_ip) {
        prn_pkt("(IN) Dropping SSH packets:", (unsigned
char*)&iph->saddr, (unsigned char*)&iph->daddr);
        return NF_DROP;
    }
}
```

```

        }
    else {
        return NF_ACCEPT;
    }
}

unsigned int post_routing_filter_hook_function(
    void *priv,
    struct sk_buff *skb,
    const struct nf_hook_state *state) {
    struct iphdr *iph;
    struct tcphdr *tcph;
    int host_B_ip = in_aton("10.0.2.15");
    int facebook_ip = in_aton("157.240.18.35");

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

    // DROP TELNET packets from Machine A to Machine B
    if (iph->protocol == IPPROTO_TCP && ntohs(tcph->dest) == 23 &&
iph->daddr == host_B_ip) {
        prn_pkt("(POST-ROUTING) Dropping TELNET packets:",
(unsigned char*)&iph->saddr, (unsigned char*)&iph->daddr);
        return NF_DROP;
    }
    // DROP SSH packets from Machine A to Machine B
    else if (iph->protocol == IPPROTO_TCP && ntohs(tcph->dest) == 22
&& iph->daddr == host_B_ip) {
        prn_pkt("(POST-ROUTING) Dropping SSH packets:", (unsigned
char*)&iph->saddr, (unsigned char*)&iph->daddr);
        return NF_DROP;
    }
    // DROP HTTP/HTTPS packets from Machine A to external website
    (Facebook)
    else if (iph->protocol == IPPROTO_TCP && (ntohs(tcph->dest) == 80
|| ntohs(tcph->dest) == 443) && iph->daddr == facebook_ip) {
        prn_pkt("(POST-ROUTING) Dropping HTTP/HTTPS packets to
www.facebook.com:", (unsigned char*)&iph->saddr, (unsigned
char*)&iph->daddr);
        return NF_DROP;
    }
    else {
        return NF_ACCEPT;
    }
}

int setUpFilter(void)
{
    printk(KERN_INFO "Registering net filters.\n");
}

```

```
    in_filters_hook.hook = in_filter_hook_function;
    in_filters_hook.hooknum = NF_INET_LOCAL_IN;
    in_filters_hook(pf = PF_INET;
    in_filters_hook.priority = NF_IP_PRI_FIRST;

    post_routing_filters_hook.hook =
post_routing_filter_hook_function;
    post_routing_filters_hook.hooknum = NF_INET_POST_ROUTING;
    post_routing_filters_hook(pf = PF_INET;
    post_routing_filters_hook.priority = NF_IP_PRI_FIRST;

    nf_register_hook(&in_filters_hook);
    nf_register_hook(&post_routing_filters_hook);

    return 0;
}

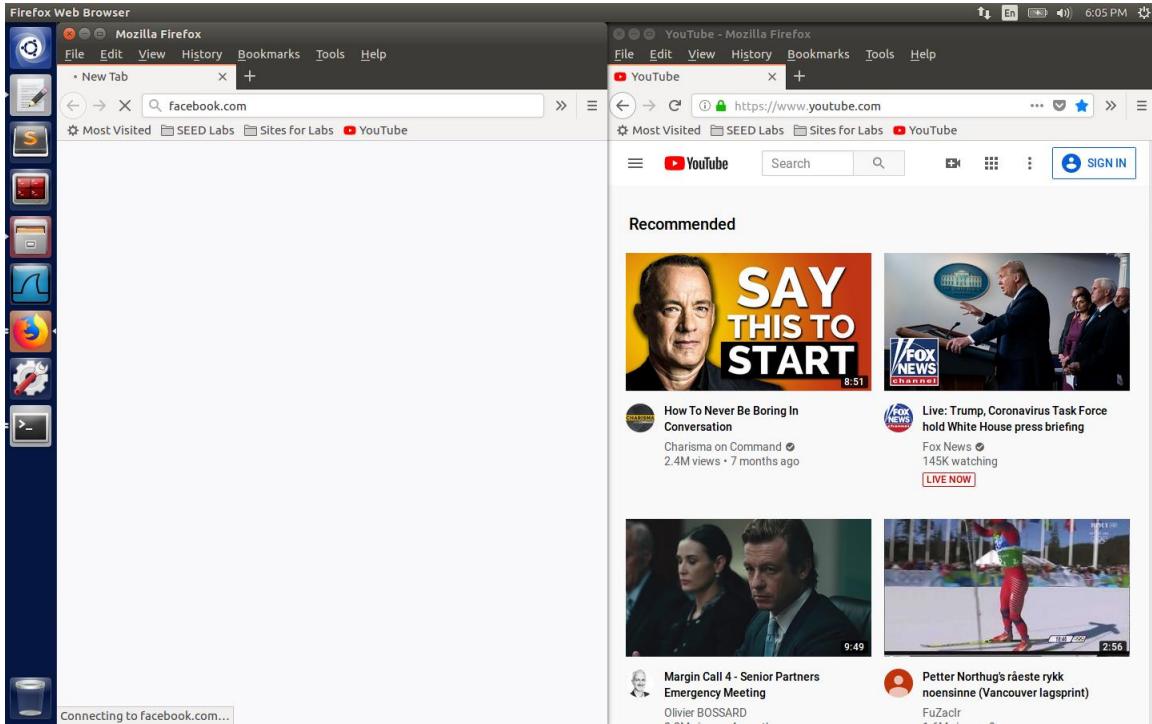
void removeFilter(void)
{
    printk(KERN_INFO "Net filters are being removed.\n");
    nf_unregister_hook(&in_filters_hook);
    nf_unregister_hook(&post_routing_filters_hook);
}

module_init(setUpFilter);
module_exit(removeFilter);

MODULE_LICENSE("GPL");

/* END */
```

The result of blocking Telnet and SSH is the same as what we have done in task 1 (Keep trying, then time-out). Here I will show the result of blocking external website.



We can get access to all external websites except `facebook.com` because of our firewall.

```
[ 1597.511470] (IN) Dropping TELNET packet: from 10.0.2.15 to 10.0.2.5
[ 1599.525869] (IN) Dropping TELNET packet: from 10.0.2.15 to 10.0.2.5
[ 1600.297993] (POST-ROUTING) Dropping TELNET packets: from 10.0.2.5 to 10.0.2.15
[ 1603.715808] (IN) Dropping TELNET packet: from 10.0.2.15 to 10.0.2.5
[ 1611.904097] (IN) Dropping TELNET packet: from 10.0.2.15 to 10.0.2.5
[ 1616.425811] (POST-ROUTING) Dropping TELNET packets: from 10.0.2.5 to 10.0.2.15
[ 1628.023813] (IN) Dropping TELNET packet: from 10.0.2.15 to 10.0.2.5
[ 1649.194344] (POST-ROUTING) Dropping TELNET packets: from 10.0.2.5 to 10.0.2.15
[ 1661.798499] (IN) Dropping TELNET packet: from 10.0.2.15 to 10.0.2.5
[ 1786.579324] (POST-ROUTING) Dropping SSH packets: from 10.0.2.5 to 10.0.2.15
[ 1787.593485] (POST-ROUTING) Dropping SSH packets: from 10.0.2.5 to 10.0.2.15
[ 1789.610332] (POST-ROUTING) Dropping SSH packets: from 10.0.2.5 to 10.0.2.15
[ 1792.060422] (IN) Dropping SSH packets: from 10.0.2.15 to 10.0.2.5
[ 1793.061086] (IN) Dropping SSH packets: from 10.0.2.15 to 10.0.2.5
[ 1793.833734] (POST-ROUTING) Dropping SSH packets: from 10.0.2.5 to 10.0.2.15
[ 1795.076383] (IN) Dropping SSH packets: from 10.0.2.15 to 10.0.2.5
[ 1799.201846] (IN) Dropping SSH packets: from 10.0.2.15 to 10.0.2.5
[ 1802.026219] (POST-ROUTING) Dropping SSH packets: from 10.0.2.5 to 10.0.2.15
[ 1807.390323] (IN) Dropping SSH packets: from 10.0.2.15 to 10.0.2.5
[ 1818.154365] (POST-ROUTING) Dropping SSH packets: from 10.0.2.5 to 10.0.2.15
[ 1823.509384] (IN) Dropping SSH packets: from 10.0.2.15 to 10.0.2.5
[ 1851.946041] (POST-ROUTING) Dropping SSH packets: from 10.0.2.5 to 10.0.2.15
[ 1856.261091] (IN) Dropping SSH packets: from 10.0.2.15 to 10.0.2.5
[ 2027.575437] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2027.825762] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2028.585506] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2028.842122] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2030.601864] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2030.857579] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2034.729405] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2034.986049] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2042.921481] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2043.177618] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2059.049917] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2059.050562] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2090.438249] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2090.688922] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2091.465645] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2091.689588] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2093.481392] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2093.705415] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2097.705582] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2097.962227] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2105.897851] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 2106.153838] (POST-ROUTING) Dropping HTTP packets to www.facebook.com: from 10.0.2.5 to 157.240.18.35
[ 04/02/20]seed@VM:~/Lab_Firewalls$
```

Kernel messages: Our packets were blocked by the firewall.

Task 3: Evading Egress Filtering

In Task 2, we have already block Telnet packets to our Machine B and HTTP/HTTPS packets to facebook.com.

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

command: `ssh -L 8000:10.0.2.15:23 seed@10.0.2.15`

Bind Machine A 8000 port to Machine B 23 port.

```
[04/02/20]seed@VM:~/Lab_Firewalls$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:d2:78:ac
      inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
         inet6 addr: fe80::905e:819f:fe:374:998a/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:13455 errors:0 dropped:0 overruns:0 frame:0
            TX packets:7411 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:14169952 (14.1 MB) TX bytes:1217194 (1.2 MB)

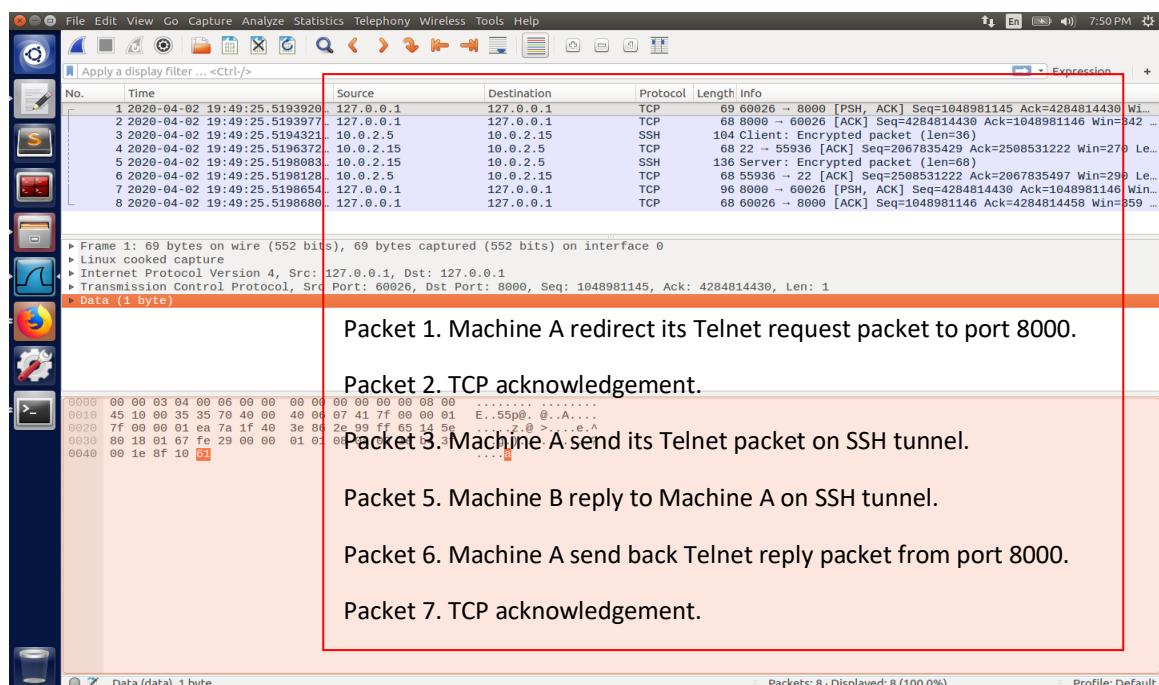
lo      Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:65536 Metric:1
        RX packets:2087 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2087 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:165702 (165.7 KB) TX bytes:165702 (165.7 KB)

[04/02/20]seed@VM:~/Lab_Firewalls$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is ']'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Apr  2 19:45:50 EDT 2020 from 10.0.2.15 on pts/19
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.

[04/02/20]seed@VM:~$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:a1:23:df
      inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
         inet6 addr: fe80::7abe:45a7:3ecc:b9de/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:2554 errors:0 dropped:0 overruns:0 frame:0
            TX packets:2114 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:226132 (226.1 KB) TX bytes:294741 (294.7 KB)
```

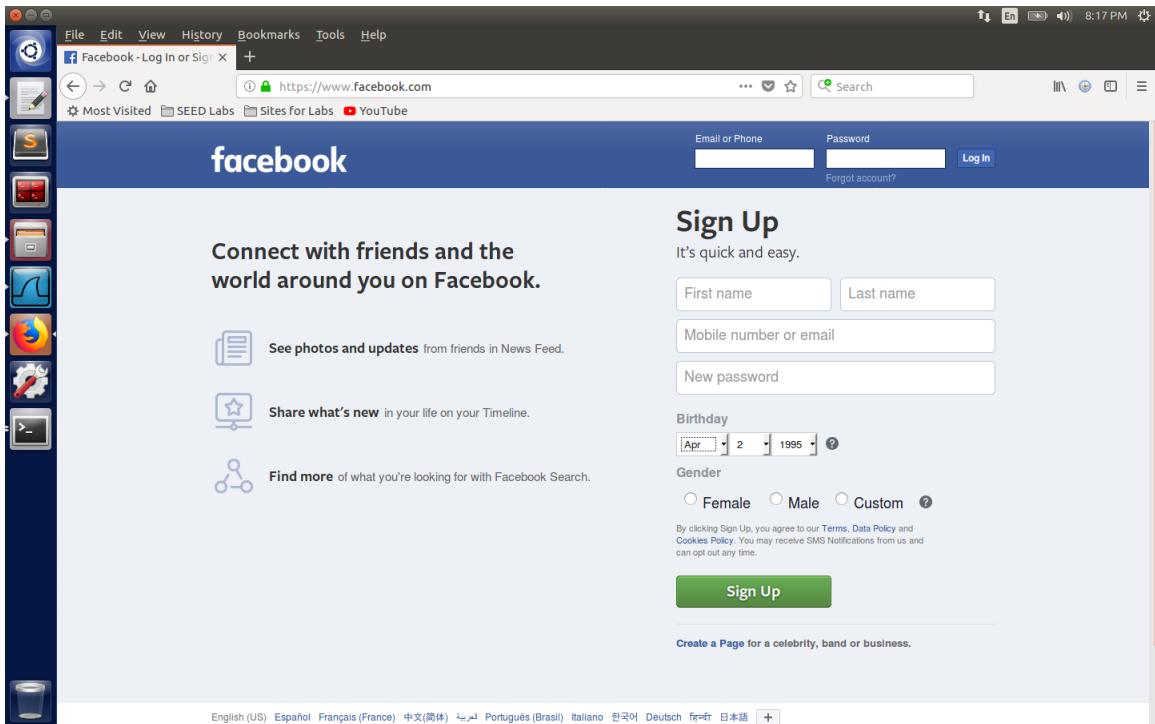


Task 3.b: Connect to Facebook using SSH Tunnel

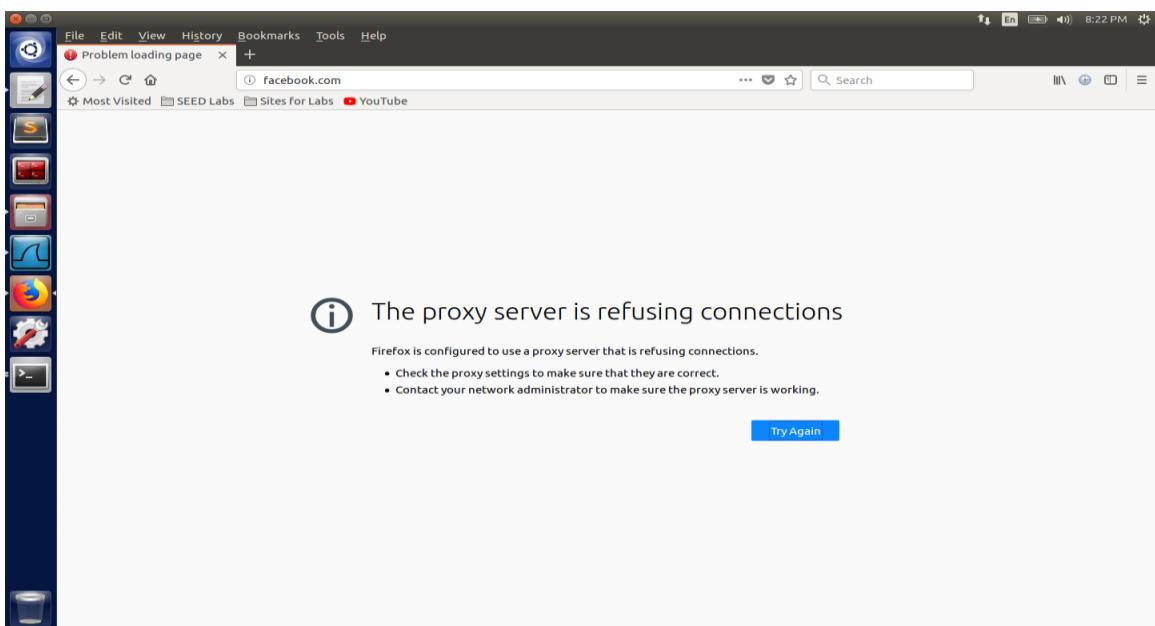
command: `ssh -D 9000 -C seed@10.0.2.15`

Bind Machine A 9000 port to Machine B. Then set proxy server for Firefox.

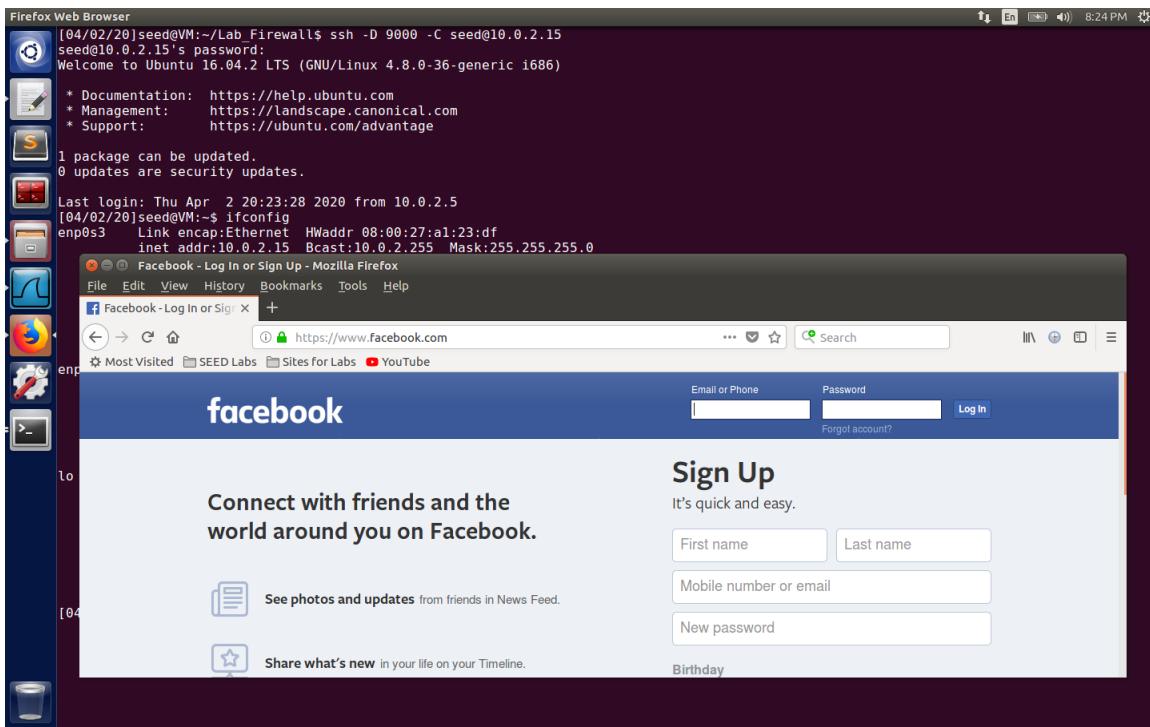
Then we could get access to `facebook.com`.



If we break the SSH tunnel, we cannot get access to `facebook.com` (and also other websites), because our proxy server is no longer available.



After we established the tunnel again, we can get access to **facebook.com** again.



Wireshark – Machine B side

Capturing from any

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-04-02 20:12:31.3147199	10.0.2.5	10.0.2.15	SSH	472	Client: Encrypted packet (len=404)
2	2023-04-02 20:12:31.3148629	10.0.2.15	157.240.18.36	TLSv1.2	417	Application Data
3	2023-04-02 20:12:31.3541659	157.240.18.36	10.0.2.15	TLSv1.2	91	Application Data
4	2023-04-02 20:12:31.3541625	10.0.2.15	157.240.18.36	TCP	56	60166 → 443 [ACK] Seq=1826793337 Ack=239464 Win=63000 L...
5	2023-04-02 20:12:31.3542733	10.0.2.15	10.0.2.5	SSH	136	Server: Encrypted packet (len=68)
6	2023-04-02 20:12:31.3622294	157.240.18.36	10.0.2.15	TLSv1.2	540	Application Data
7	2023-04-02 20:12:31.3622418	10.0.2.15	157.240.18.36	TCP	56	60166 → 443 [ACK] Seq=1826793337 Ack=239468 Win=64400 L...
8	2023-04-02 20:12:31.3624012	10.0.2.15	10.0.2.5	SSH	592	Client: Encrypted packet (len=524)
9	2023-04-02 20:12:31.3626890	10.0.2.5	10.0.2.15	TCP	68	56036 → 22 [ACK] Seq=2796331868 Ack=2757717888 Win=2405...
10	2023-04-02 20:12:31.3651575	10.0.2.5	10.0.2.15	SSH	504	Client: Encrypted packet (len=436)
11	2023-04-02 20:12:31.3652187	10.0.2.15	157.240.18.36	TLSv1.2	450	Application Data
12	2023-04-02 20:12:31.3959474	157.240.18.36	10.0.2.15	TLSv1.2	91	Application Data
13	2023-04-02 20:12:31.3960526	10.0.2.15	10.0.2.5	SSH	136	Server: Encrypted packet (len=68)
14	2023-04-02 20:12:31.4383649	10.0.2.5	10.0.2.15	TCP	68	56036 → 22 [ACK] Seq=2796332304 Ack=2757717956 Win=2405...
15	2023-04-02 20:12:31.4402267	10.0.2.15	157.240.18.36	TCP	56	60166 → 443 [ACK] Seq=1826793731 Ack=239483 Win=64408 L...

Frame 1: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.15

Transmission Control Protocol, Src Port: 56036, Dst Port: 22, Seq: 2796331464, Ack: 2757717296, Len: 404

SSH Protocol

Packet 1. Machine A send its http requests to Machine B.

Packet 2. Then Machine B get the page from facebook.com for machine A.

Packet 3. Facebook Web server reply.

Packet 4. TCP acknowledgement.

Packet 5. Send back reply to Machine A.

Packets: 369 · Displayed: 369 (100.0%) · Profile: Default

Wireshark – Machine A side

Capturing from any

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-04-02 20:13:30.2544918	127.0.0.1	127.0.0.1	TCP	144	35316 → 9000 [PSH, ACK] Seq=3056724153 Ack=1089562155 W...
2	2023-04-02 20:13:30.2845622	10.0.2.15	10.0.2.15	SSH	176	Client: Encrypted packet (len=108)
3	2023-04-02 20:13:30.2844980	10.0.2.15	10.0.2.15	SSH	136	Server: Encrypted packet (len=68)
4	2023-04-02 20:13:30.2844232	10.0.2.15	10.0.2.15	TCP	68	56036 → 22 [ACK] Seq=2796352200 Ack=27577197472 Win=2405...
5	2023-04-02 20:13:30.2844994	127.0.0.1	127.0.0.1	TCP	103	9000 → 35316 [PSH, ACK] Seq=1089562155 Ack=3056724229 W...
6	2023-04-02 20:13:30.3047269	127.0.0.1	127.0.0.1	TCP	107	35334 → 9000 [PSH, ACK] Seq=3993483759 Ack=3329314153 W...
7	2023-04-02 20:13:30.3047880	10.0.2.15	10.0.2.15	SSH	144	Client: Encrypted packet (len=76)
8	2023-04-02 20:13:30.3261428	127.0.0.1	127.0.0.1	TCP	68	35316 → 9000 [ACK] Seq=3056724229 Ack=1089562190 Win=36...
9	2023-04-02 20:13:30.3352239	10.0.2.15	10.0.2.15	SSH	144	Server: Encrypted packet (len=76)
10	2023-04-02 20:13:30.3353168	127.0.0.1	127.0.0.1	TCP	107	9000 → 35334 [PSH, ACK] Seq=3329314153 Ack=3993483798 W...

Frame 5: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 9000, Dst Port: 35316, Seq: 1089562155, Ack: 3056724229, Len: 35

Data (35 bytes)

Data: 170303001efa3e4823981a1cae... [Length: 35]

Packet 1. Machine A send its http requests to port 9000.

Packet 2. SSH pushforward the http request to Machine B.

Packet 3. Get reply from Machine B.

Packet 4. TCP acknowledgement.

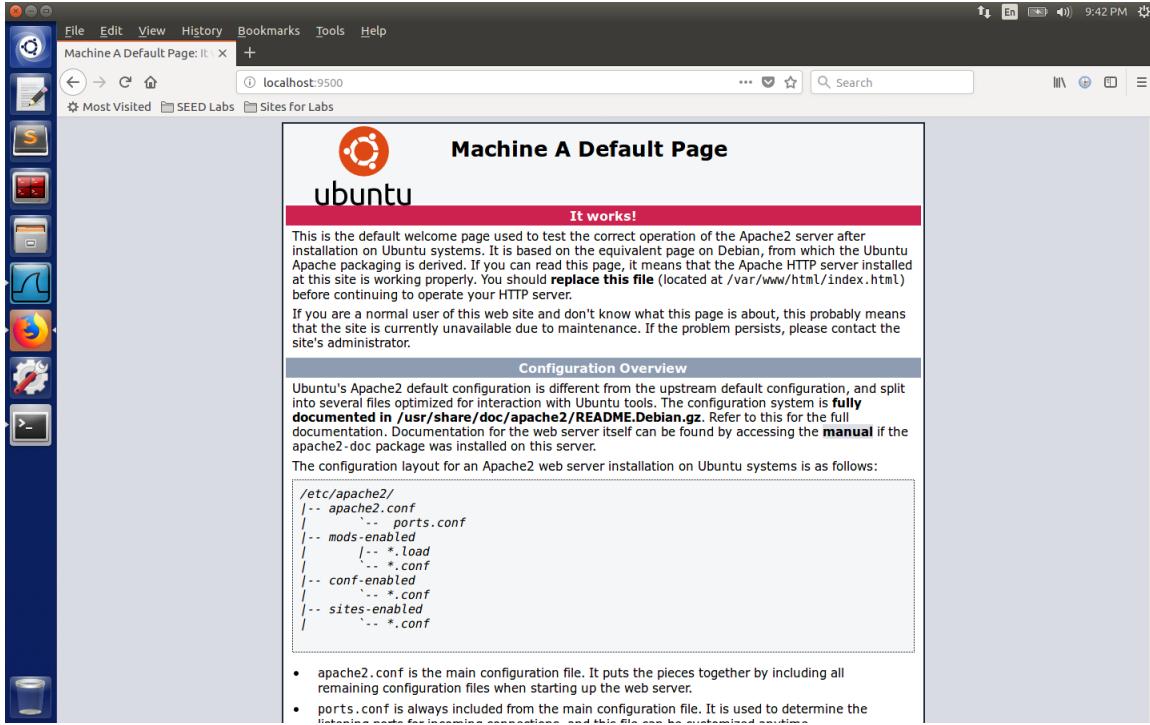
Packet 5. Send back reply from port 9000 to the browser.

Packets: 280 · Displayed: 280 (100.0%) · Profile: Default

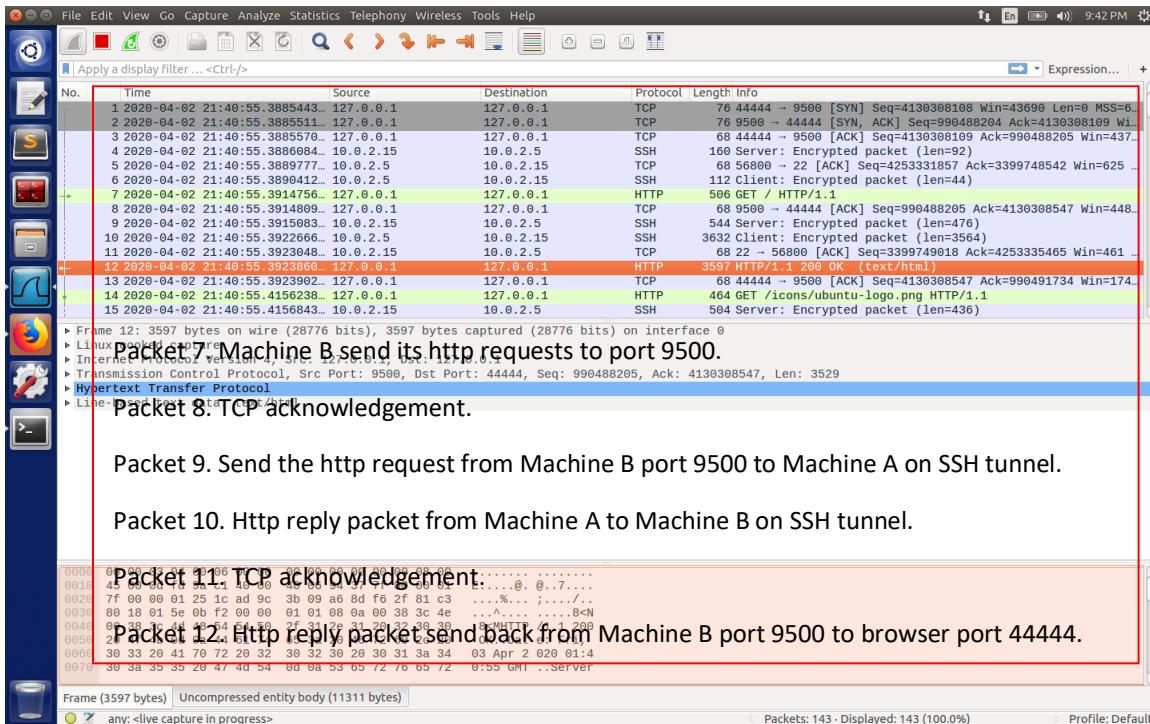
Task 4: Evading Ingress Filtering

command: ssh -R 9500:10.0.2.5:80 seed@10.0.2.15

Remote Bind: Bind Machine B 9500 port to Machine A 80 port.

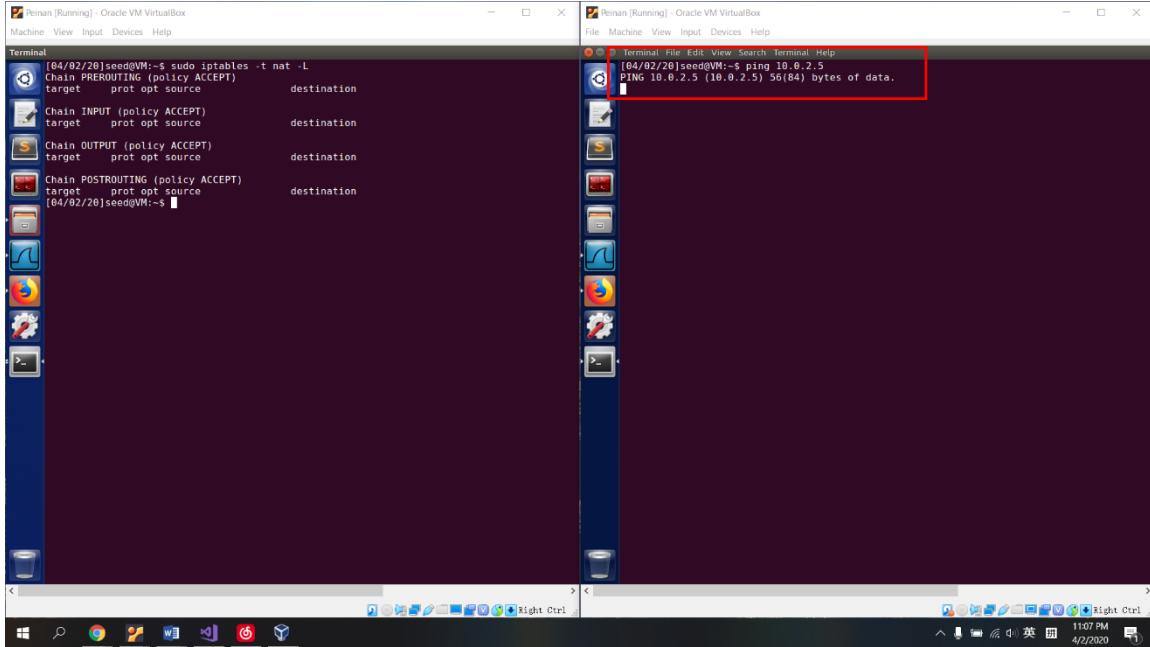


We can see the page on Machine A by searching **localhost:9500** on Machine B.



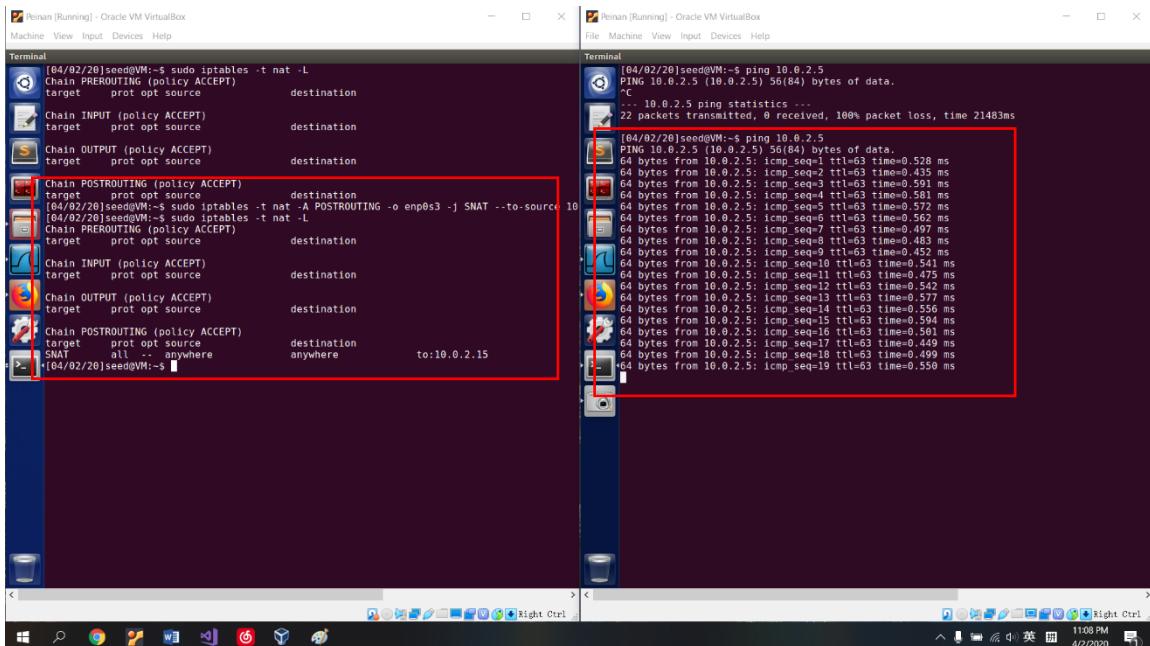
Task 5(SNAT): Use iptables to set up a SNAT. Use Wireshark to prove that your SNAT is working.

Before: Host V cannot get ICMP reply from Host U.

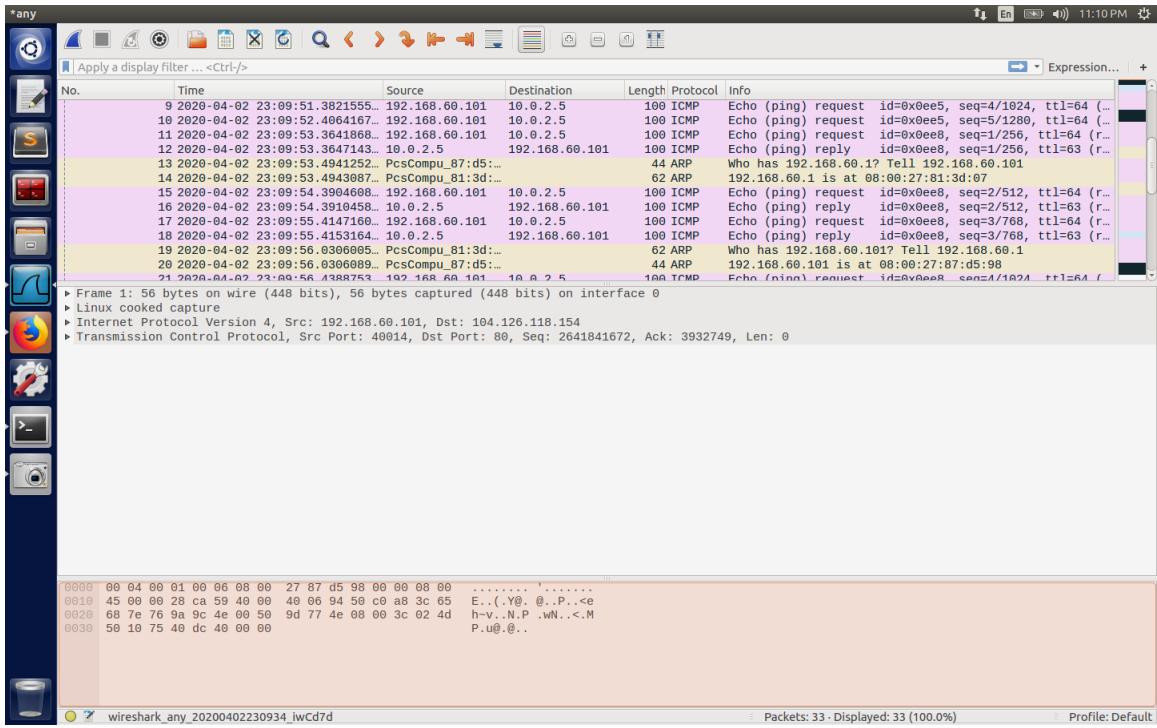


After we set the SNAT on our server machine (Both Internal and NAT Network).

Host V can get ICMP reply from Host U.



Wireshark – Host V

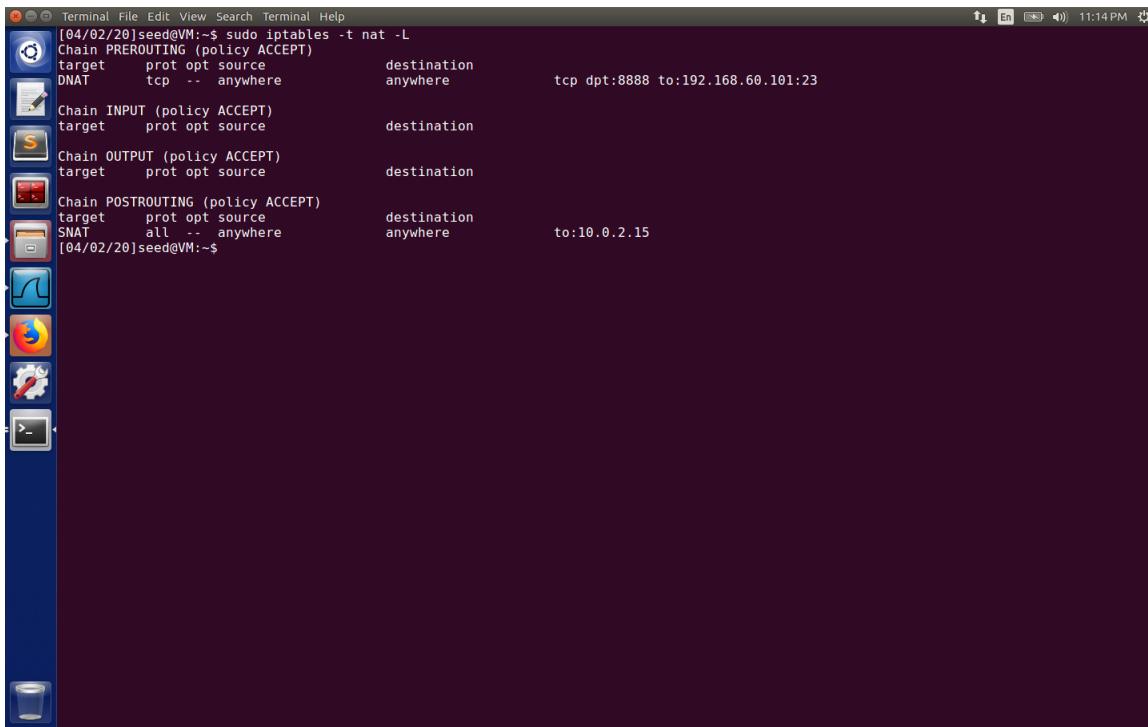


Packet 9 and Packet 10: before setting SNAT.

Packet after 11: After setting SNAT.

Task 6(DNAT): Use iptables to set up a DNAT for port forwarding. Use Wireshark to prove that your DNAT is working.

Set DNAT on server. See the following **iptables**.



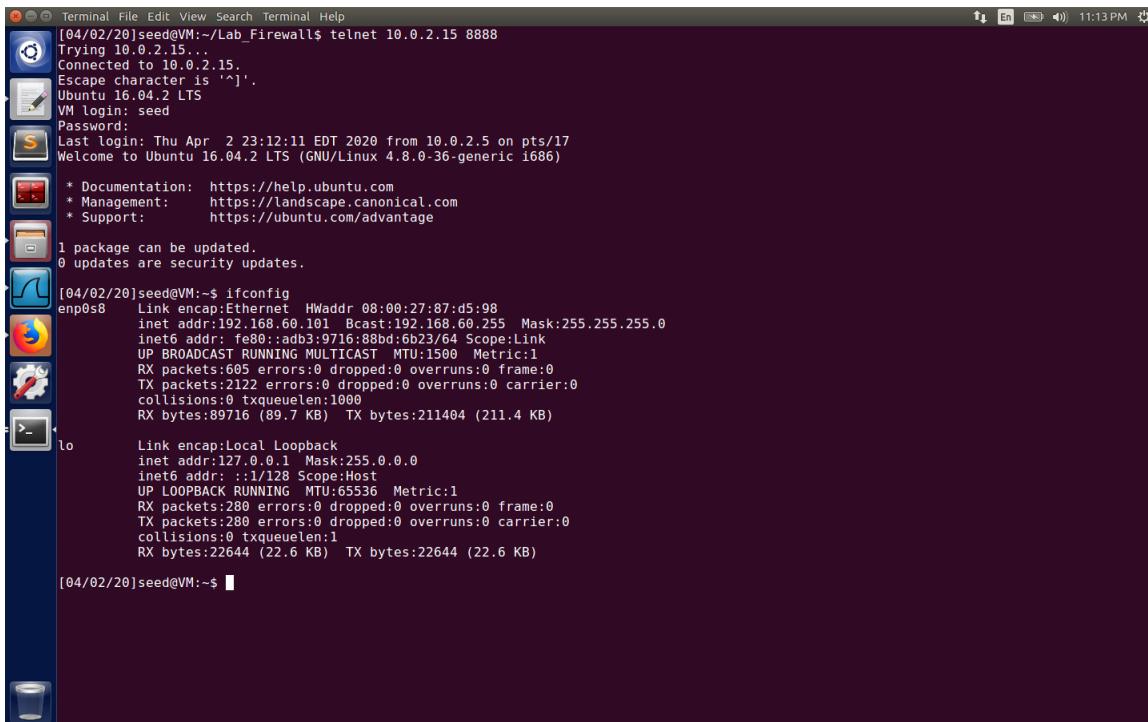
```
[04/02/20]seed@VM:~$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
DNAT      tcp  --  anywhere       anywhere          tcp dpt:8888 to:192.168.60.101:23

Chain INPUT (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination

Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
SNAT     all  --  anywhere       anywhere          to:10.0.2.15
[04/02/20]seed@VM:~$
```

Telnet 10.0.2.15, but actually connected to 192.168.60.101 in the internal network.



```
[04/02/20]seed@VM:~/Lab_Firewall$ telnet 10.0.2.15 8888
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^].
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Apr  2 23:12:11 EDT 2020 from 10.0.2.5 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

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

[04/02/20]seed@VM:~$ ifconfig
enp0s8    Link encap:Ethernet HWaddr 08:00:27:87:d5:98
          inet addr:192.168.60.101  Bcast:192.168.60.255  Mask:255.255.255.0
          inet6 addr: fe80::fe80:27ff:fe87:d598/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:608 errors:0 dropped:0 overruns:0 frame:0
            TX packets:2122 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:89710 (89.7 KB)  TX bytes:211404 (211.4 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:280 errors:0 dropped:0 overruns:0 frame:0
            TX packets:280 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:22644 (22.6 KB)  TX bytes:22644 (22.6 KB)

[04/02/20]seed@VM:~$
```

Wireshark: Telnet Packets

The screenshot shows the Wireshark interface with a list of captured network packets. A red box highlights the first few packets (7721-7724) and the packet details for 7724.

Packets 7721-7724:

- Packet 7721: Host U send its Telnet requests to the server.
- Packet 7722: Redirect to Host V in the internal network (192.168.60.101).
- Packet 7723: Telnet reply.
- Packet 7724: Server send back Telnet reply to Host U.

Packet 7724 Details:

No.	Time	Source	Destination	Protocol	Length	Info
7724	2020-04-02 23:14:22.259057	10.0.2.5	192.168.60.101	TELNET	69	57542 → 8888 [PSH, ACK] Seq=1151225775 Ack=1998367512 W...
7725	2020-04-02 23:14:22.2593319	192.168.60.101	10.0.2.5	TELNET	69	Telnet Data ...
7726	2020-04-02 23:14:22.2593399	10.0.2.15	10.0.2.5	TCP	68	8888 → 57542 [PSH, ACK] Seq=1998367512 Ack=1151225776 W...
7727	2020-04-02 23:14:22.2596623	10.0.2.5	10.0.2.15	TCP	68	57542 → 8888 [ACK] Seq=1151225776 Ack=1998367513 Win=31...
7728	2020-04-02 23:14:22.2596682	10.0.2.5	192.168.60.101	TCP	68	57542 → 23 [ACK] Seq=1151225776 Ack=1998367513 Win=3187...
7729	2020-04-02 23:14:22.3175512	10.0.2.5	10.0.2.15	TCP	69	57542 → 8888 [PSH, ACK] Seq=1151225776 Ack=1998367513 W...
7730	2020-04-02 23:14:22.3175694	10.0.2.5	192.168.60.101	TELNET	69	Telnet Data ...
7731	2020-04-02 23:14:22.3179724	192.168.60.101	10.0.2.5	TELNET	69	Telnet Data ...
7732	2020-04-02 23:14:22.3179939	10.0.2.15	10.0.2.5	TCP	69	8888 → 57542 [PSH, ACK] Seq=1998367513 Ack=1151225777 W...
7733	2020-04-02 23:14:22.3182627	10.0.2.5	10.0.2.15	TCP	68	57542 → 8888 [ACK] Seq=1151225777 Ack=1998367514 Win=31...
7734	2020-04-02 23:14:22.3183022	10.0.2.5	192.168.60.101	TCP	68	57542 → 23 [ACK] Seq=1151225777 Ack=1998367514 Win=3187...
7735	2020-04-02 23:14:22.7388094	10.0.2.5	192.168.60.101	TELNET	70	Telnet Data ...
7736	2020-04-02 23:14:22.7406538	192.168.60.101	10.0.2.5	TELNET	70	Telnet Data ...

Frame 7721: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 57542, Dst Port: 8888, Seq: 1151225775, Ack: 1998367512, Len: 1
Data (1 byte)

Packet 7721. Host U send its Telnet requests to the server.

Packet 7722. Redirect to Host V in the internal network (192.168.60.101).

Packet 7723. Telnet reply.

Packet 7724. Server send back Telnet reply to Host U.

Hex dump for Packet 7724:

Hex	Dec	Text
0000	00 00 00 01 00 00 00 00	?? ?? ?? ?? ?? ?? ?? ??
0010	45 10 00 00 00 00 00 00	?? ?? ?? ?? ?? ?? ?? ??
0020	00 02 0f e0 c6 22 b8 44	.. .D.O.w...
0030	9e 4f af 77 1c ab 18M..
0040	00 18 00 f9 ee 13 00 00 01 01 08 0a 00 4d 9c cdka

Task 7(DNAT): Use iptables to set up a DNAT for load balancing and demonstrate how it works. In my lecture, I didn't get a perfect load balancing. Can you improve my result?

Set rules on server.

```
[04/02/20]seed@VM:~$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
DNAT      tcp  --  anywhere       anywhere    tcp dpt:8888 to:192.168.60.101:23

Chain INPUT (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination

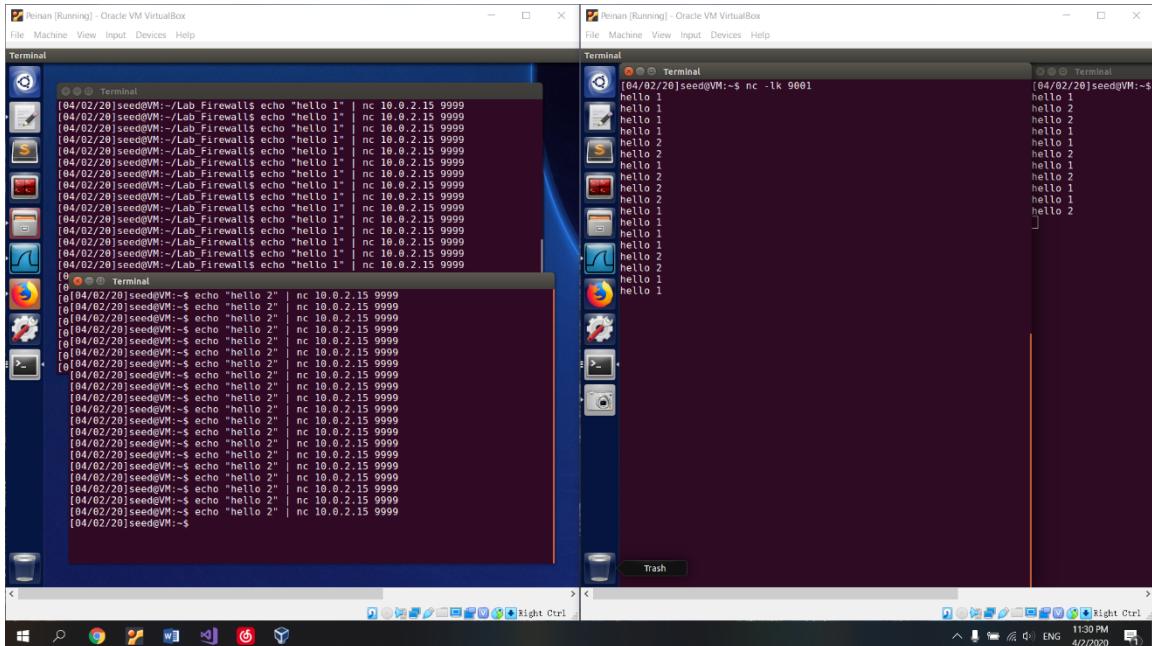
Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
SNAT     all  --  anywhere       anywhere    to:10.0.2.15
[04/02/20]seed@VM:~$ sudo iptables -t nat -A PREROUTING -p tcp --dport 9999 \
> -m statistic --mode random --probability .50 \
> -j DNAT --to-destination 192.168.60.101:9001
[04/02/20]seed@VM:~$ sudo iptables -t nat -A PREROUTING -p tcp --dport 9999 -m statistic --mode random --probability .50 -j DNAT --to-de
stination 192.168.60.101:9002
[04/02/20]seed@VM:~$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
DNAT      tcp  --  anywhere       anywhere    tcp dpt:8888 to:192.168.60.101:23
DNAT      tcp  --  anywhere       anywhere    tcp dpt:9999 statistic mode random probability 0.5000000000 to:192.168.60.101:9001
DNAT      tcp  --  anywhere       anywhere    tcp dpt:9999 statistic mode random probability 0.5000000000 to:192.168.60.101:9002

Chain INPUT (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination

Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
SNAT     all  --  anywhere       anywhere    to:10.0.2.15
[04/02/20]seed@VM:~$
```

Results



How to improve: set the first probability to 0.5 and the second one 1.

If $K > 2$, then let the probability of N -th server be $[1 / (K - N + 1)]$

For example, we have 4 servers.

Server 1 Probability = $1 / 4 = 0.25$

Server 2 Probability = 1 / 3 = 0.33

Server 3 Probability = 1 / 2 = 0.5

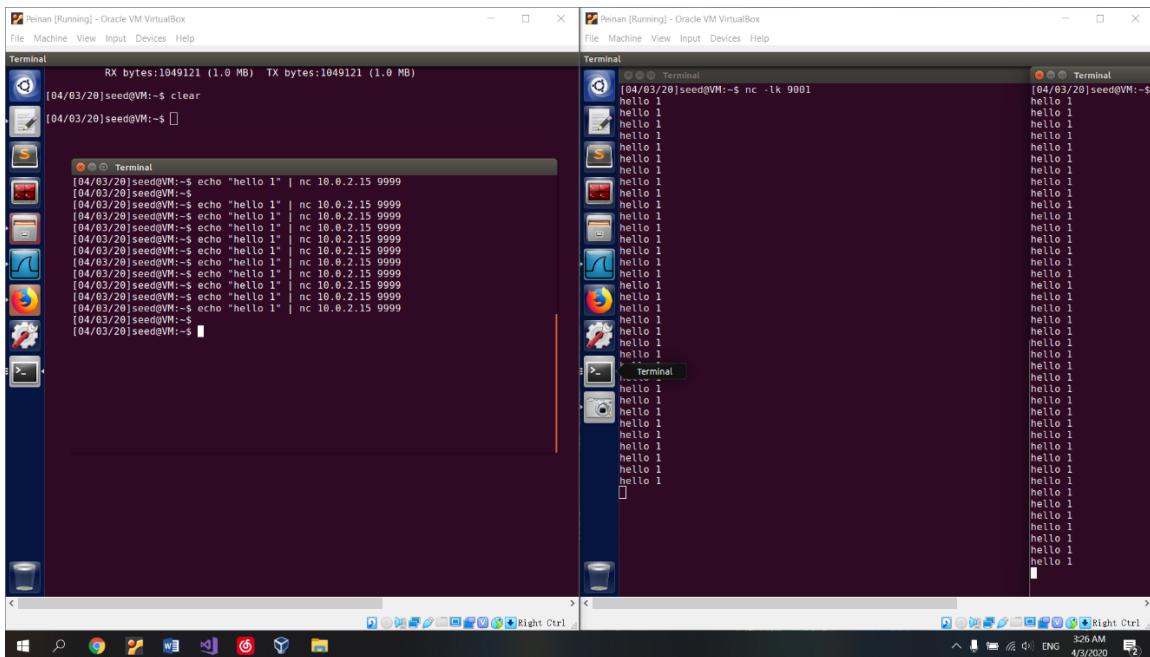
Server 4 Probability = 1 / 1 = 1

```
[Terminal File Edit View Search Terminal Help]
[04/03/20]seed@VM:-$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
DNAT     tcp  --  anywhere       anywhere          tcp dpt:8888 to:192.168.60.101:23
DNAT     tcp  --  anywhere       anywhere          tcp dpt:9999 statistic mode random probability 0.500000000000 to:192.168.60.101:9001
DNAT     tcp  --  anywhere       anywhere          tcp dpt:9999 statistic mode random probability 1.000000000000 to:192.168.60.101:9002

Chain INPUT (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination

Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
SNAT     all  --  anywhere       anywhere          to:10.0.2.15
[04/03/20]seed@VM:-$
```



Task 8(Connection Track): Set up a firewall rule based on connections.

Command 1: `sudo iptables -A OUTPUT -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT`

Command 2: `sudo iptables -A OUTPUT -p tcp -j REJECT`

Only allow TCP packets with ESTABLISHED and RELATED state, no new TCP connections.

See results & screenshots on the next page.

Before: Host U could telnet 10.0.2.15 then telnet 192.168.60.101(host V) in the internal network.

```
[04/02/20]seed@VM:~/Lab_Firewall$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^']'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Apr  2 23:44:04 EDT 2020 from 10.0.2.5 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

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

[04/02/20]seed@VM:~$ telnet 192.168.60.101
Trying 192.168.60.101...
Connected to 192.168.60.101.
Escape character is '^']'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Apr  2 23:44:13 EDT 2020 from 192.168.60.1 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

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

[04/02/20]seed@VM:~$ ifconfig
enp0s8      Link encap:Ethernet HWaddr 08:00:27:87:d5:98
            inet addr:192.168.60.101 Bcast:192.168.60.255 Mask:255.255.255.0
                  inet6 addr: fe80::adb3:9716:88bd:6b23/64 Scope:Link
                     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                     RX packets:1931 errors:0 dropped:0 overruns:0 frame:0
                     TX packets:2966 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:1000
                     RX bytes:559830 (559.8 KB)  TX bytes:277878 (277.8 KB)

lo          Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
```

After: Can't do that, because the firewall disallow new TCP connections.

```
[04/02/20]seed@VM:~/Lab_Firewall$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^']'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Apr  2 23:39:50 EDT 2020 from 10.0.2.5 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

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

[04/02/20]seed@VM:~$ telnet 10.0.2.5...
telnet: Unable to connect to remote host: Connection refused
[04/02/20]seed@VM:~$ telnet 192.168.60.101...
telnet: Unable to connect to remote host: Connection refused
[04/02/20]seed@VM:~$
```