Linux Firewall Exploration Lab

Task1

A 的 IP 地址为 10.0.2.5，B 的 IP 地址为 10.0.2.7。

Prevent A from doing telnet to Machine B

```
[09/17/20]seed@VM:~$ man ufw
[09/17/20]seed@VM:~$ vim /etc/default/ufw
[09/17/20]seed@VM:~$ vim /etc/default/ufw
[09/17/20]seed@VM:~$ sudo vim /etc/default/ufw
[09/17/20]seed@VM:~$ man ufw
[09/17/20]seed@VM:~$ sudo ufw deny out 23/tcp
Rules updated
Rules updated (v6)
[09/17/20]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: ^CConnection closed by foreign host.
[09/17/20]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
[09/17/20]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
^C
```

设置相应的 ufw 规则，禁止针对 tcp23 端口的流量流出，设置成功后无法启动相应的 telnet 服务

Prevent B from doing telnet to Machine A

```
[09/17/20]seed@VM:~$ sudo ufw delete 1
Deleting:
 deny out 23/tcp
Proceed with operation (y|n)? y
Rule deleted
[09/17/20]seed@VM:~$ sudo ufw delete 2
ERROR: Could not find rule '2'
[09/17/20]seed@VM:~$ sudo ufw delete 1
Deleting:
 deny out 23/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)
[09/17/20]seed@VM:~$ sudo ufw disable
Firewall stopped and disabled on system startup
[09/17/20]seed@VM:~$ sudo ufw deny in 23/tcp
Rules updated
Rules updated (v6)
[09/17/20]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

在 A 上设置相应的防火墙规则，禁止针对 tcp23 端口的流量进入

```
[09/17/20]seed@VM:~$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: ^CConnection closed by foreign host.
[09/17/20]seed@VM:~$ telnet 10.0.2.5
Trying 10.0.2.5...
^C
[09/17/20]seed@VM:~$
```

B 在开启防火墙后无法通过 telnet 连接到 A

Prevent A from visiting an external web site

```
[09/17/20]seed@VM:~/lab/lab6_task1$ sudo ufw deny out 80/tcp
Rule added
Rule added (v6)
[09/17/20]seed@VM:~/lab/lab6_task1$ wget www.baidu.com
--2020-09-17 08:04:08--  http://www.baidu.com/
Resolving www.baidu.com (www.baidu.com)... 180.101.49.11, 180.101.49.12
Connecting to www.baidu.com (www.baidu.com)|180.101.49.11|:80... ^C
[09/17/20]seed@VM:~/lab/lab6_task1$ sudo ufw disable
Firewall stopped and disabled on system startup
[09/17/20]seed@VM:~/lab/lab6_task1$ wget www.baidu.com
--2020-09-17 08:04:20--  http://www.baidu.com/
Resolving www.baidu.com (www.baidu.com)... 180.101.49.12, 180.101.49.11
Connecting to www.baidu.com (www.baidu.com)|180.101.49.12|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2381 (2.3K) [text/html]
Saving to: ‘index.html’

index.html          100%[===================>]   2.33K  --.-KB/s    in 0s

2020-09-17 08:04:20 (291 MB/s) - ‘index.html’ saved [2381/2381]
```

禁止流出指向 80 端口的流量即可

Task2

根据题目要求 5 条规则，所以写了两个过滤器（in or out）

```c
unsigned int TCP_out_Filter(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))
    {
        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;
    }
    else if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(80))
    {
        printk(KERN_INFO "Dropping 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 if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(22))
    {
        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;
    }
    else
    {
        return NF_ACCEPT;
    }
}
```

```c
unsigned int TCP_in_Filter(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))
    {
        printk(KERN_INFO "Dropping telnet packet from %d.%d.%d.%d\n",
        ((unsigned char *)&iph->saddr)[0],
        ((unsigned char *)&iph->saddr)[1],
        ((unsigned char *)&iph->saddr)[2],
        ((unsigned char *)&iph->saddr)[3]);
        return NF_DROP;
    }
    else if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(22))
    {
        printk(KERN_INFO "Dropping ssh packet from %d.%d.%d.%d\n",
        ((unsigned char *)&iph->saddr)[0],
        ((unsigned char *)&iph->saddr)[1],
        ((unsigned char *)&iph->saddr)[2],
        ((unsigned char *)&iph->saddr)[3]);
        return NF_DROP;
    }
    else
    {
        return NF_ACCEPT;
    }
}
```

载入相关模块后，telnet 访问 B，wget 访问 baidu，B telnet 访问 A 均失败，如下图所示

```
Registering a TCP out filter.
Registering a TCP in filter.
Dropping telnet packet to 10.0.2.7
Dropping telnet packet to 10.0.2.7
Dropping http packet to 180.101.49.12
Dropping http packet to 180.101.49.12
Dropping telnet packet from 10.0.2.7
Dropping telnet packet from 10.0.2.7
 Filters are being removed.
```

```
[09/17/20]seed@VM:~$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: ^CConnection closed by foreign host.
[09/17/20]seed@VM:~$ telnet 10.0.2.5
Trying 10.0.2.5...
^C
[09/17/20]seed@VM:~$
```

```
[09/17/20]seed@VM:~/lab/lab6_task1$ sudo insmod Filter.ko
[09/17/20]seed@VM:~/lab/lab6_task1$ telnet 10.0.2.7
Trying 10.0.2.7...
^C
[09/17/20]seed@VM:~/lab/lab6_task1$ wget www.baidu.com
--2020-09-17 20:47:24--  http://www.baidu.com/
Resolving www.baidu.com (www.baidu.com)... 180.101.49.12, 180.101.49.11
Connecting to www.baidu.com (www.baidu.com)|180.101.49.12|:80... ^C
[09/17/20]seed@VM:~/lab/lab6_task1$ sudo rmmod Filter
[09/17/20]seed@VM:~/lab/lab6_task1$ telnet 10.0.2.7
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: ^CConnection closed by foreign host.
[09/17/20]seed@VM:~/lab/lab6_task1$ wget www.baidu.com
--2020-09-17 20:48:00--  http://www.baidu.com/
Resolving www.baidu.com (www.baidu.com)... 180.101.49.11, 180.101.49.12
Connecting to www.baidu.com (www.baidu.com)|180.101.49.11|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2381 (2.3K) [text/html]
Saving to: ‘index.html.1’
```

Task3

```
[09/17/20]seed@VM:~/lab/lab6_task1$ sudo ufw deny out to 128.230.18.200
Rules updated
[09/17/20]seed@VM:~/lab/lab6_task1$ sudo ufw deny out 23/tcp
Rules updated
Rules updated (v6)
[09/17/20]seed@VM:~/lab/lab6_task1$ sudo ufw enable
Firewall is active and enabled on system startup
[09/17/20]seed@VM:~/lab/lab6_task1$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     DENY OUT    Anywhere
128.230.18.200             DENY OUT    Anywhere
23/tcp                     DENY OUT    Anywhere
80/tcp (v6)                DENY OUT    Anywhere (v6)
23/tcp (v6)                DENY OUT    Anywhere (v6)

[09/17/20]seed@VM:~/lab/lab6_task1$ ping www.syr.edu -c 5
PING syr.edu (128.230.18.200) 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
--- syr.edu ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4071ms

[09/17/20]seed@VM:~/lab/lab6_task1$ telnet 10.0.2.7
Trying 10.0.2.7...
^C
```

通过设置规则，禁止了虚拟机 A 访问雪城大学官网与其他主机的 telnet 的服务

Task3.a

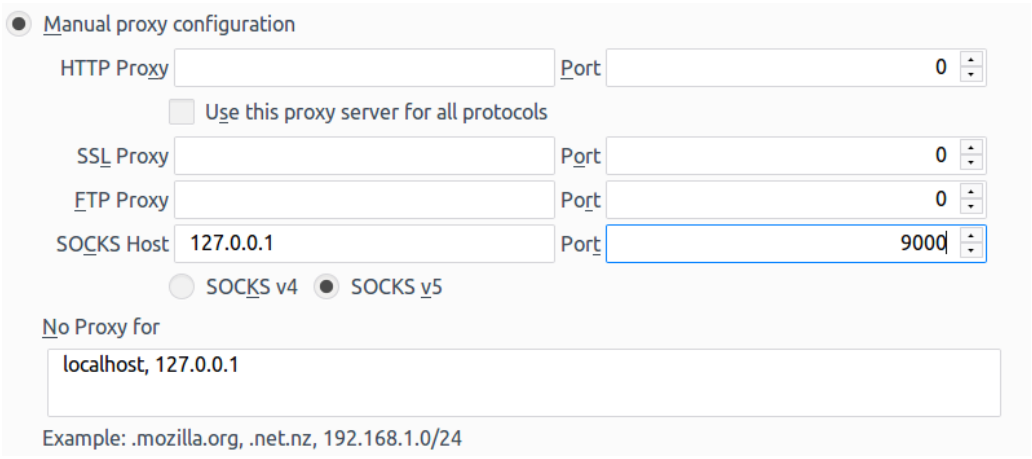
```
[09/17/20]seed@VM:~$ ssh -L 8000:10.0.2.7:23 seed@10.0.2.7
seed@10.0.2.7's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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.
```

```
[09/17/20]seed@VM:~$ 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 Sep 17 22:20:42 EDT 2020 from 10.0.2.7 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.

[09/17/20]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:67:74:9f
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::1f18:5bf6:2184:623c/64 Scope:Link
```

通过 ssh 隧道实现了访问 machineB 的 23 端口并登陆成功

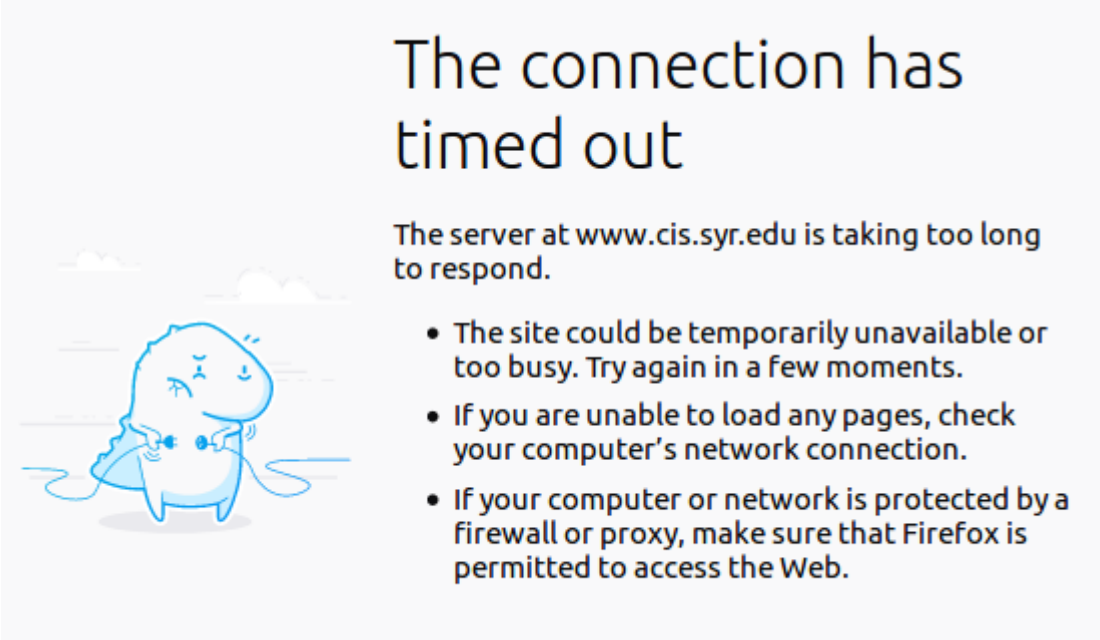
Task3.b

```
[09/17/20]seed@VM:~$ ssh -D 9000 -C seed@10.0.2.7
seed@10.0.2.7's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic

 * 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: Thu Sep 17 22:22:52 2020 from 10.0.2.7
[09/17/20]seed@VM:~$
```

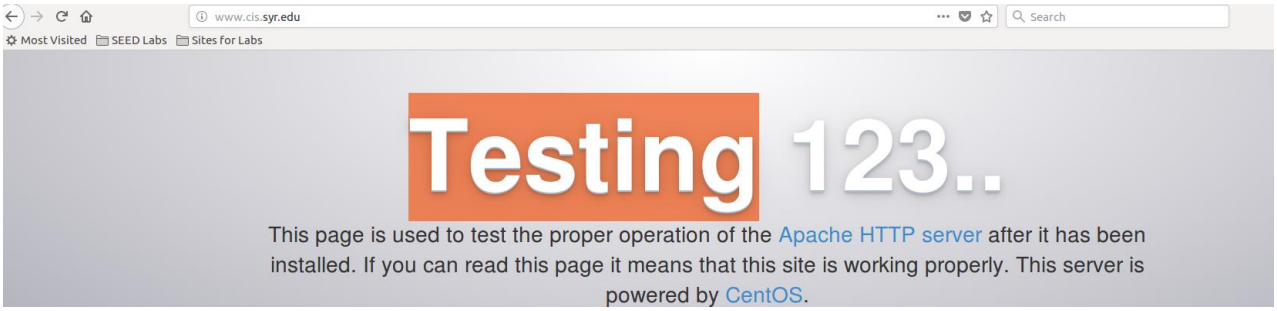


启动 ssh，设置代理，访问结果如下图

虽然显示 test，但是因为 B 访问这一网站也显示 test，所以说明已经访问成功



关闭 ssh 与代理设置后会显示访问失败，连接超时。



重新设置后会再次显示该界面

```
 3 2020-09-17 22:56:09.21478… 10.0.2.5          10.0.2.7          SSH      102 Client: Encrypted packet (len=36)
 4 2020-09-17 22:56:09.21513… 10.0.2.7          10.0.2.5          TCP       66 22 → 38004 [ACK] Seq=4076667754 Ack=710845189
 5 2020-09-17 22:56:09.21577… 10.0.2.7          128.230.247.70    TCP       74 60032 → 80 [SYN] Seq=3306606266 Win=29200 Len=
 6 2020-09-17 22:56:09.44437… 128.230.247.70    10.0.2.7          TCP       60 80 → 60032 [SYN, ACK] Seq=93247 Ack=3306606267
 7 2020-09-17 22:56:09.44451… 10.0.2.7          128.230.247.70    TCP       60 60032 → 80 [ACK] Seq=3306606267 Ack=93248 Win=
 8 2020-09-17 22:56:09.44483… 10.0.2.7          10.0.2.5          SSH      110 Server: Encrypted packet (len=44)
```

Wireshark 截图显示 A 先将访问内容通过 ssh 发给 B，B 在进行相关访问，然后

将访问结果返回给 A

Task4

```
[09/18/20]seed@VM:~$ sudo ufw deny in proto tcp from 10.0.2.7 to any port 80
Rule added
[09/18/20]seed@VM:~$ sudo ufw deny in proto tcp from 10.0.2.7 to any port 23
Rule added
[09/18/20]seed@VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     DENY        10.0.2.7
23/tcp                     DENY        10.0.2.7
```

首先进行主机 A 的配置，禁止 B 主机访问 23 端口和 80 端口

设置主机 C 的相关文件/etc/ssh/sshd_config，添加 GatewayPorts yes

```
[09/18/20]seed@VM:~$ ssh -NfR 6666:localhost:22 seed@10.0.2.8
seed@10.0.2.8's password:
[09/18/20]seed@VM:~$
```

设置逆向的 ssh 隧道，使得主机 B 可以通过访问主机 C 的 6666 端口来访问主机 A

```
[09/18/20]seed@VM:~$ ssh -p 6666 seed@10.0.2.8
The authenticity of host '[10.0.2.8]:6666 ([10.0.2.8]:6666)' can't be establishe
d.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.0.2.8]:6666' (ECDSA) to the list of known hosts.
seed@10.0.2.8'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.


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.

[09/18/20]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:2e:d0:60
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::58b1:b122:5294:a985/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:209 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

主机 B 访问主机 A 成功

学号：57117127

姓名：贺博文