Linux Firewall Exploration Lab

57117118 司晓凯

Task 1: Using Firewall

Prevent A from doing telnet to Machine B

开启防火墙之前，A 可以成功 telnet 到 B。

```
[09/16/20]seed@VM:.../default$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Sep 10 23:20:53 EDT 2020 from 10.0.2.4 on pts/20
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.
```

在 B 上开启防火墙，并且添加一条过滤规则

```
[09/17/20]seed@VM:.../default$ sudo ufw deny from 10.0.2.4 to any port 23
Rule added
```

```
[09/17/20]seed@VM:.../default$ telnet 10.0.2.6
Trying 10.0.2.6...
```

A 无法成功 telnet 到 B

Prevent B from doing telnet to Machine A.

重复以上操作

```
[09/17/20]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
Password:
Last login: Thu Sep 17 02:06:19 EDT 2020 from 10.0.2.4 on pts/21
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:~$ sudo ufw deny from 10.0.2.6 to any port 23
Rule added
```

```
[09/17/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
```

无法联通

Prevent A from visiting an external web site.

```
[09/17/20]seed@VM:~$ ping www.seu.edu.cn
PING widc142.seu.edu.cn (58.192.118.142) 56(84) bytes of data.
64 bytes from 58.192.118.142: icmp_seq=1 ttl=248 time=4.76 ms
64 bytes from 58.192.118.142: icmp_seq=2 ttl=248 time=4.34 ms
64 bytes from 58.192.118.142: icmp_seq=3 ttl=248 time=3.90 ms
64 bytes from 58.192.118.142: icmp_seq=4 ttl=248 time=4.22 ms
```

不设置任何过滤规则前，VM A ping www.seu.edu.cn，可以 ping 通。

```
[09/17/20]seed@VM:~$ sudo ufw deny out to 58.192.118.142
Rule added
```

设置 ufw 规则，deny 所有发往宿地址为 58.192.118.142 的报文

```
PING widc142.seu.edu.cn (58.192.118.142) 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
```

Task 2: Implementing a Simple Firewall

编写 filter1.c，对于所有源地址为 B 的 IP 地址 10.0.2.6 且指向 A 的 22 端口（SSH 端口）和 23 端口（telnet 端口）的报文，都丢弃掉。

```
/* IP address */
static unsigned char *drop_ip="\x0a\x00\x02\x06";//10.0.2.6
```

```
/*if src ip==10.0.2.6 and the dst port is 23 or 22*/
if (iph->saddr==*(unsigned int *)drop_ip && iph->protocol==IPPROTO_TCP && (tcph-
>dest == htons(23)||tcph->dest == htons(22)))
```

在 A 上将 filter1.c 编译成模块 filter1.ko，并且将其加入到内核中。

```
[09/17/20]seed@VM:~/.../lab1$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed/week32/lab1 modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  CC [M]  /home/seed/week32/lab1/filter1.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/week32/lab1/filter1.mod.o
  LD [M]  /home/seed/week32/lab1/filter1.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
```

```
sudo insmod filter1.ko
```

在 B 上尝试 telnet 或者 SSH 主机 A，发现无法成功

编写 filter1.c，对于所有宿地址为 B 的 IP 地址 10.0.2.6 且指向 B 的 22 端口（SSH 端口）和 23 端口（telnet 端口）的报文，都丢弃掉。

```
/* IP address */
static unsigned char *drop_ip="\x0a\x00\x02\x06";//10.0.2.6
```

```
/*if src ip==10.0.2.6 and the dst port is 23 or 22*/
if (iph->saddr==*(unsigned int *)drop_ip && iph->protocol==IPPROTO_TCP && (tcph-
>dest == htons(23)||tcph->dest == htons(22)))
```

重复之前的操作，在 A 上尝试 telnet 或者 SSH 主机 B，无法成功。

添加模块 filter3.ko，实现一条规则——阻止 A 访问网站 www.baidu.com

编写 filter1.c，对于所有宿地址为 www.baidu.com 的 IP 地址 182.61.220.6 和 182.61.220.7 且宿端口为 80 端口（HTTP 端口）的报文，都丢弃掉。

```
/* IP address */
static unsigned char *drop_ip1="\xb6\x3d\xc8\x06";//182.61.200.6
static unsigned char *drop_ip2="\xb6\x3d\xc8\x07";//182.61.200.7

/*if dst ip==58.192.118.142 and the dst port is 80*/
if ((iph->daddr==*(unsigned int *)drop_ip1||iph->daddr==*(unsigned int
*)drop_ip2) && iph->protocol==IPPROTO_TCP && tcph->dest == htons(80))
```

在 A 上使用 wget www.baidu.com 向 www.baidu.com 发送报文，无法建立连接。

```
[09/18/20]seed@VM:~/.../lab1$ wget www.baidu.com
--2020-09-18 03:36:16--  http://www.baidu.com/
Resolving www.baidu.com (www.baidu.com)... 182.61.200.7, 182.61.200.6
Connecting to www.baidu.com (www.baidu.com)|182.61.200.7|:80... failed: Connect
ion timed out.
Connecting to www.baidu.com (www.baidu.com)|182.61.200.6|:80... failed: Connect
ion timed out.
Retrying.
```

Task 3: Evading Egress Filtering

3.a: Telnet to Machine B through the firewall

在主机 A 上输入指令 ssh -L 8000:10.0.2.6:23 seed@10.0.2.5，建立 A 和 C 之间的 SSH 隧道。

```
[09/18/2020 02:21] seed@ubuntu:~$ telnet localhost 8000
Trying ::1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Sep 17 09:31:35 EDT 2020 from 10.0.2.4 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.
```

```
SSH Protocol
   Packet Length (encrypted): b96789b9
   Encrypted Packet: 198de0ba79628b3c861d5b6d9a65a1ee1028f00b2f996340...
```

机 A 与 C 一直通过 SSH 隧道进行报文交换，且交换的内容都被加密。

Telnet 成功后 A 执行“ls”操作，试图获取 B 当前目录下所有文件信息。

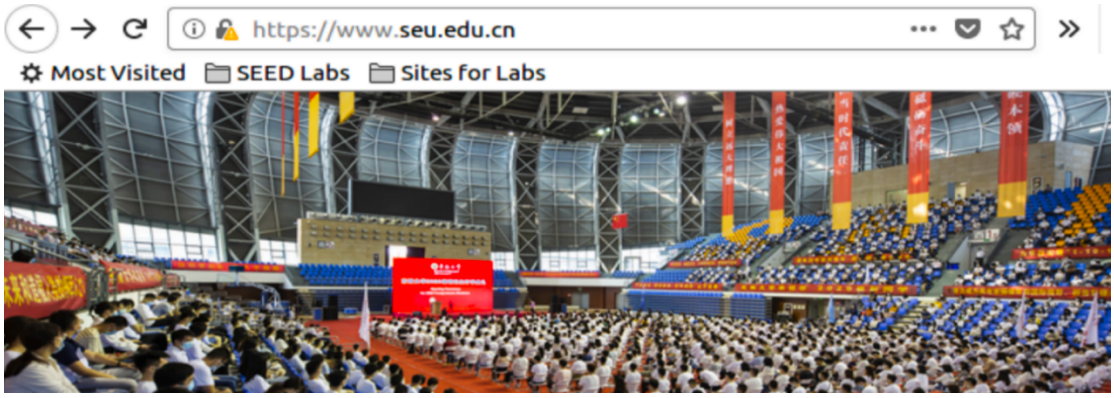
```
Telnet
   Data: \r\n
   Data: \033[0m\033[01;34mandroid\033[0m        examples.desktop
   Data: \033[01;34mbin\033[0m                get-pip.py         \033[01
   Data: \033[01;34mCustomization\033[0m      gratuitous.py      \033[01
   Data: \033[01;34mDesktop\033[0m            index.html         reply.p
   Data: \033[01;34mDocuments\033[0m          index.html.1       request
   Data: \033[01;34mDownloads\033[0m          \033[01;34mlib\033[0m
```

3.b: Connect to www.seu.edu.cn using SSH Tunnel.

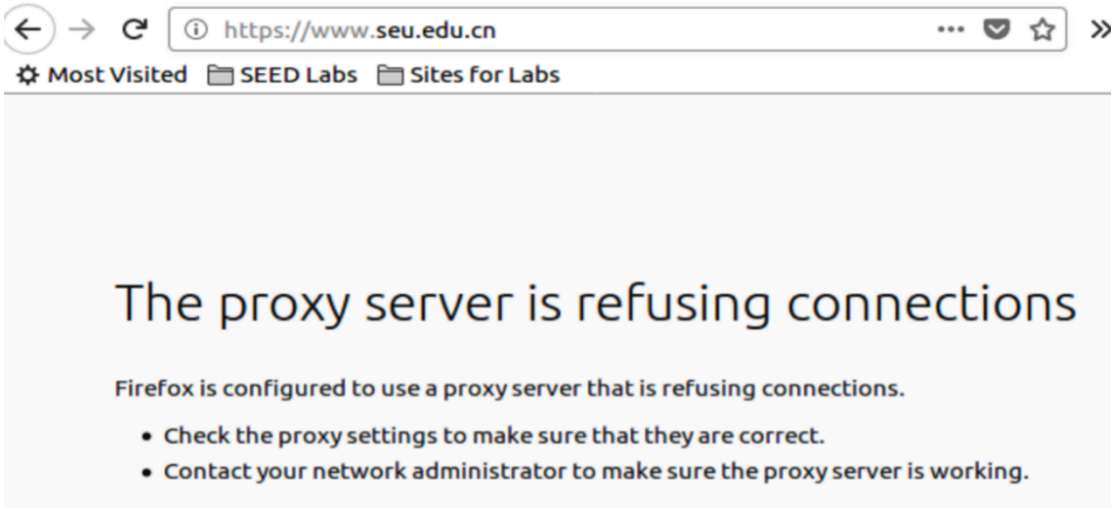
建立 A 和 C 之间的动态 SSH 隧道

```
[09/18/20]seed@VM:~/.../lab1$ ssh -D 9000 -C seed@10.0.2.5
seed@10.0.2.5's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

使 Firefox 使用 localhost 作为代理
可以看到 www.seu.edu.cn 的网页。



关闭 SSH 隧道后，无法访问 www.seu.edu.cn



重新打开 SSH 隧道后，可以重新访问 www.seu.edu.cn。

Task 4: Evading Ingress Filtering

在主机 A 上用 ufw 指令设置防火墙过滤规则，禁止来自主机 B 的 SSH 和 HTTP 报文.

```
[09/18/20]seed@VM:~/.../lab1$ sudo ufw deny from 10.0.2.6 to any port 22
Rule added
[09/18/20]seed@VM:~/.../lab1$ sudo ufw deny from 10.0.2.6 to any port 80
Rule added
```

```
[09/18/20]seed@VM:~$ ssh 10.0.2.4
ssh: connect to host 10.0.2.4 port 22: Connection timed out
```

```
[09/18/20]seed@VM:~$ wget 10.0.2.4
--2020-09-18 22:24:47--  http://10.0.2.4/
Connecting to 10.0.2.4:80... failed: Connection timed out.
```

防火墙规则设置后，主机 B 无法直接访问 A 的 22 和 80 端口

A 主动与 B 建立反向 SSH 连接

```
[09/19/20]seed@VM:~$ ssh -NfR 10000:localhost:22 seed@10.0.2.6
```

B 再次访问 10.0.2.4 的 80 端口，可以成功访问。

```
[09/19/20]seed@VM:~$ ssh seed@localhost -p 10000
The authenticity of host '[localhost]:10000 ([127.0.0.1]:10000)' can't be esta
lished.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:10000' (ECDSA) to the list of known ho
ts.
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
```

```
[09/19/20]seed@VM:~$ wget 10.0.2.4
--2020-09-19 09:10:50--  http://10.0.2.4/
Connecting to 10.0.2.4:80... connected.
HTTP request sent, awaiting response... 200 OK
```