网安综合课程设计实验报告 6

Linux Firewall Exploration Lab

Task 1: Using Firework

1> 阻止 A 通过 telnet 连接 B

在 A 中的命令为:

```
[09/16/20]seed@VM:~$ su
Password:
root@VM:/home/seed# ufw enable
Firewall is active and enabled on system startup
root@VM:/home/seed# ufw status
Status: active
root@VM:/home/seed# ufw deny out to any port 23
Rule added
Rule added (v6)
root@VM:/home/seed# telnet 10.0.2.6
Trying 10.0.2.6...
```

可以看到 A 无法 telnet 连接 B

2> 阻止 B 通过 telnet 连接 A

在 A 中的命令为:（先删除掉之前的命令）

```
root@VM:/home/seed# ufw delete deny out to any port 23
Rule deleted
Rule deleted (v6)
root@VM:/home/seed# ufw deny 23
Rule added
Rule added (v6)
root@VM:/home/seed# ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         DENY        Anywhere
23 (v6)                    DENY        Anywhere (v6)

root@VM:/home/seed#
```

在 B 中尝试 telnet 连接:（首先证明 B 无防火墙）

```
root@VM:/home/seed# ufw status
Status: active
root@VM:/home/seed# telnet 10.0.2.5
Trying 10.0.2.5...
```

发现成功阻止了 B 的连接

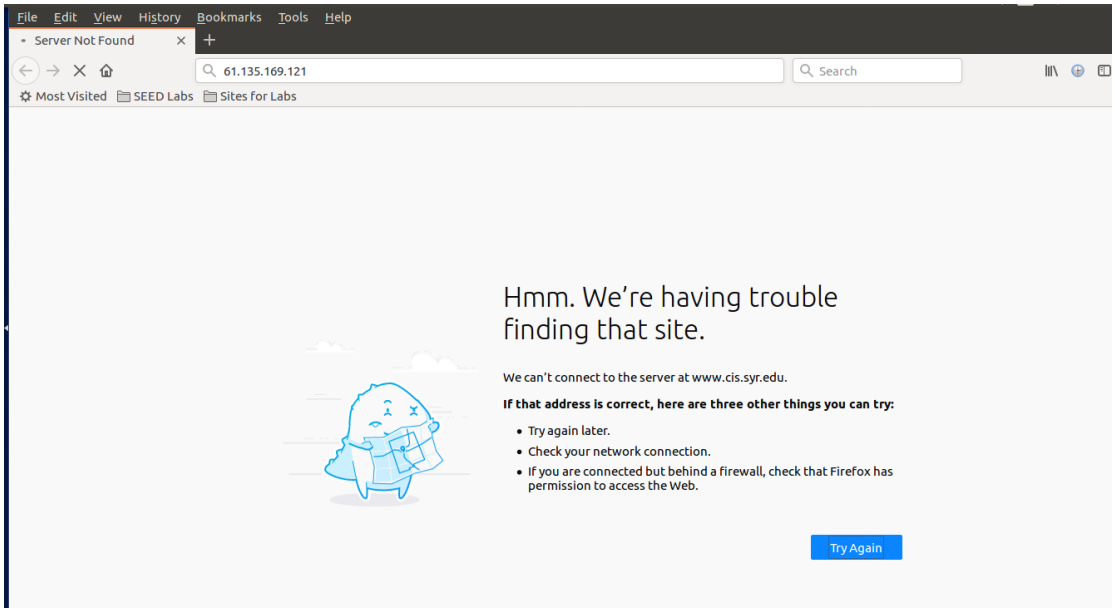
3> 阻止 A 访问外部网络

首先，A 是可以正常进行访问百度的

在 A 中进行如下设置：

```
root@VM:/home/seed# ufw deny from  61.135.169.121
Rule added
root@VM:/home/seed# ufw status
Status: active

To                         Action      From
--                         ------      ----
Anywhere                   DENY        61.135.169.121
```

再进行测试：



Task2　Implement a Simple Firewall

编写 telnetFilter.c 文件如下：

telnetFilter.c (~/Desktop) - gedit

Open

telnetFilter.c　telnetfilter.c

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

unsigned int telnetFilter(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 ==IPPORTO_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 {
                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;

        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);
```

编写 Makefile 文件如下：

Makefile (~/Desktop/1) - gedit

Open

```
obj-m += telnetFilter.o

all:
        make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules

clean:
        make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean
```

编译如下：

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

插入模块之后用 telnet 命令发现无法登录到远程机。

Task 3: Ecading Egress Filtering

1> 准备工作:

准备三台主机，IP 地址分别为:

A: `inet addr:10.0.2.7`

B: `inet addr:10.0.2.6`

C: `inet addr:10.0.2.5`

目前 A 可以通过 telnet 连接 B:

```
root@VM:/home/seed# 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:
```

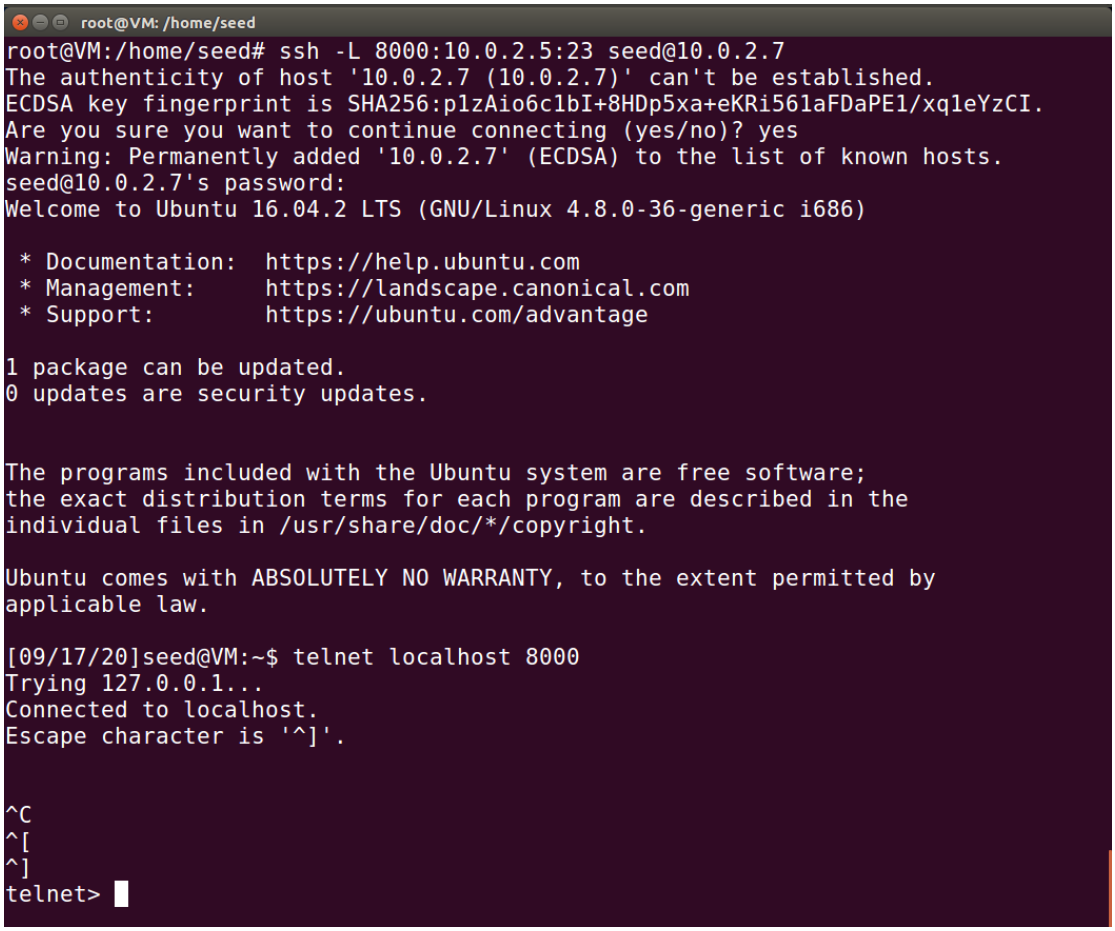
也可以访问 61.135.169.121（百度）

在 A 处建立防火墙

```
root@VM:/etc/default# ufw deny out 23
Rule added
Rule added (v6)
root@VM:/etc/default# telnet 10.0.2.5
Trying 10.0.2.5...
```

```
root@VM:/etc/default# ufw deny out to 61.135.169.121
Rule added
root@VM:/etc/default# ping 61.135.169.121
PING 61.135.169.121 (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
^C
```

2> Telnet to machine B throught the firewall



3> Connect to Facebook using SSH Tunnel

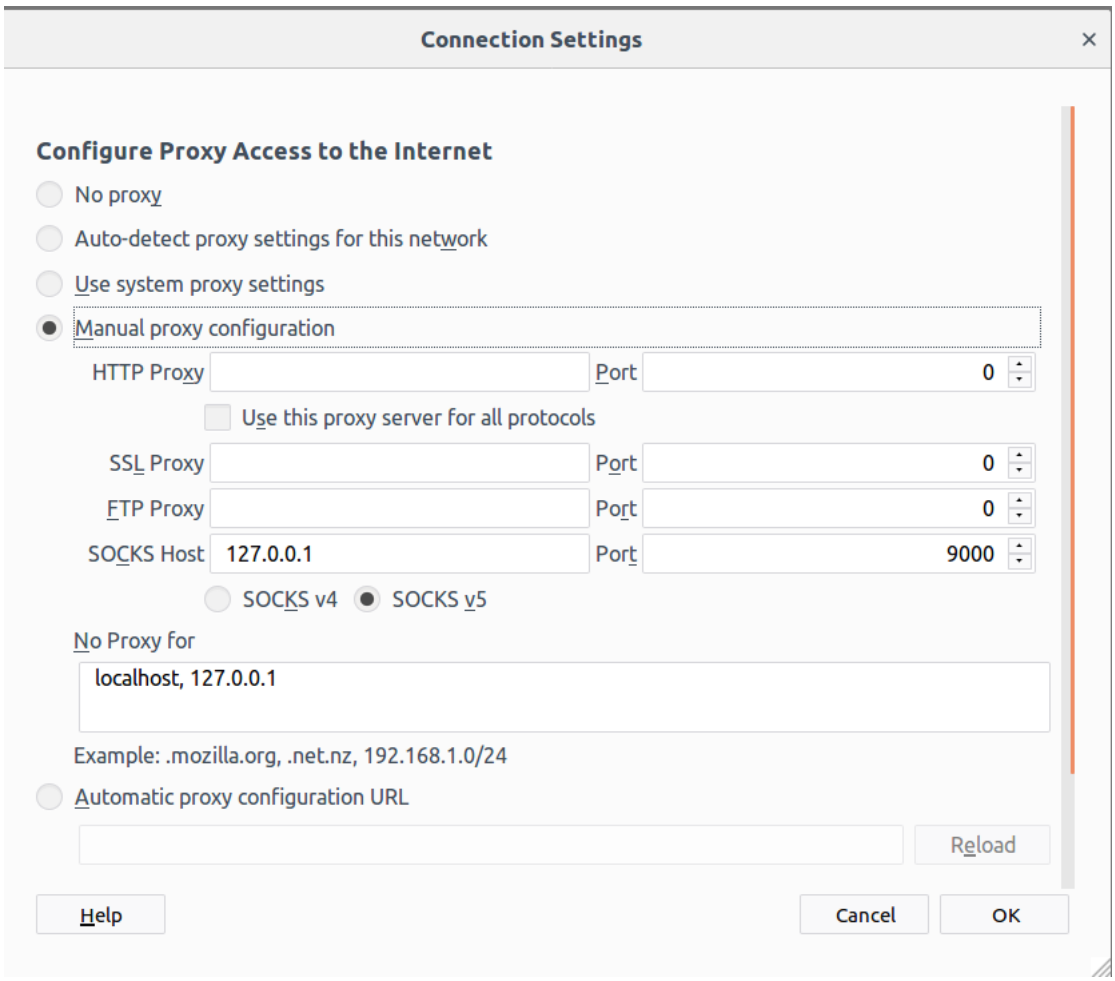
静态方法:

```
root@VM: /home/seed
[09/17/20]seed@VM:~$ sudo ufw deny to 61.135.169.121
Rule added
[09/17/20]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
^C
--- www.a.shifen.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2040ms

[09/17/20]seed@VM:~$ sudo ssh -L 61.138.168.121:80 seed@10.0.2.7
Bad local forwarding specification '61.138.168.121:80'
[09/17/20]seed@VM:~$ sudo ssh -L 8000:61.138.168.121:80 seed@10.0.2.7
The authenticity of host '10.0.2.7 (10.0.2.7)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.7' (ECDSA) to the list of known hosts.
seed@10.0.2.7's password:
bind: Address already in use
channel_setup_fwd_listener_tcpip: cannot listen to port: 8000
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: Thu Sep 17 06:02:17 2020 from 10.0.2.6
[09/17/20]seed@VM:~$ telnet localhost 8000
```

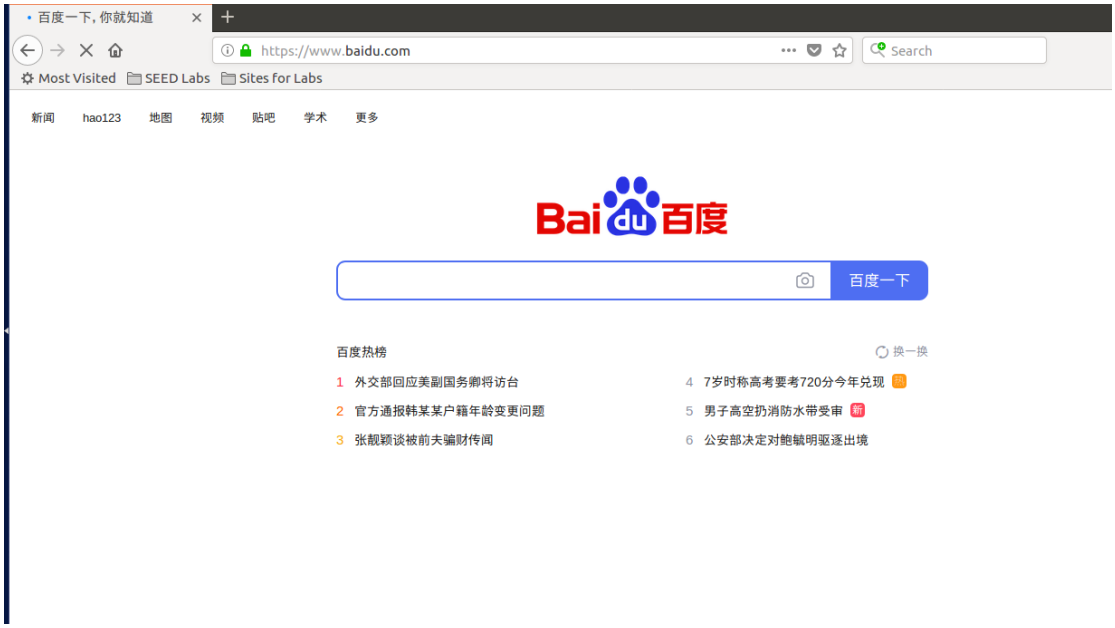
动态方法:

```
[09/17/20]seed@VM:~$ ssh -D 9000 -C seed@10.0.2.7
The authenticity of host '10.0.2.7 (10.0.2.7)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.7' (ECDSA) to the list of known hosts.
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.

Last login: Thu Sep 17 07:36:19 2020 from 10.0.2.7
[09/17/20]seed@VM:~$
```

设置浏览器属性



访问目的网站



Task 4: Evading Ingress Filtering

在内网 A 中进行隧道的建立：

```
[09/17/20]seed@VM:~$ ssh -NfR 80:localhost:22 seed@10.0.2.7
```

在外网 B 可以进行连接

```
[09/17/20]seed@VM:~$ ssh localhost -p 80
```

代理到了内网。