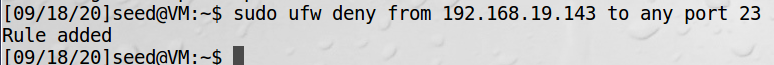
**I.Linux Firewall Exploration Lab**

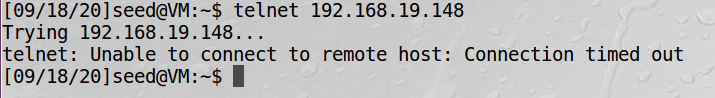
**Task1：**

（1）Prevent A from doing telnet to Machine B：

对虚拟机B设置防火墙：



A尝试和B进行telnet连接失败：

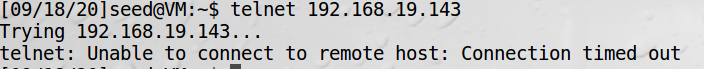


（2）Prevent B from doing telnet to Machine A：

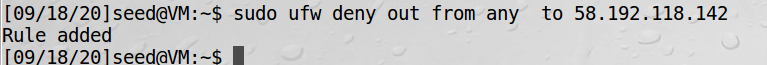
对虚拟机A设置防火墙：



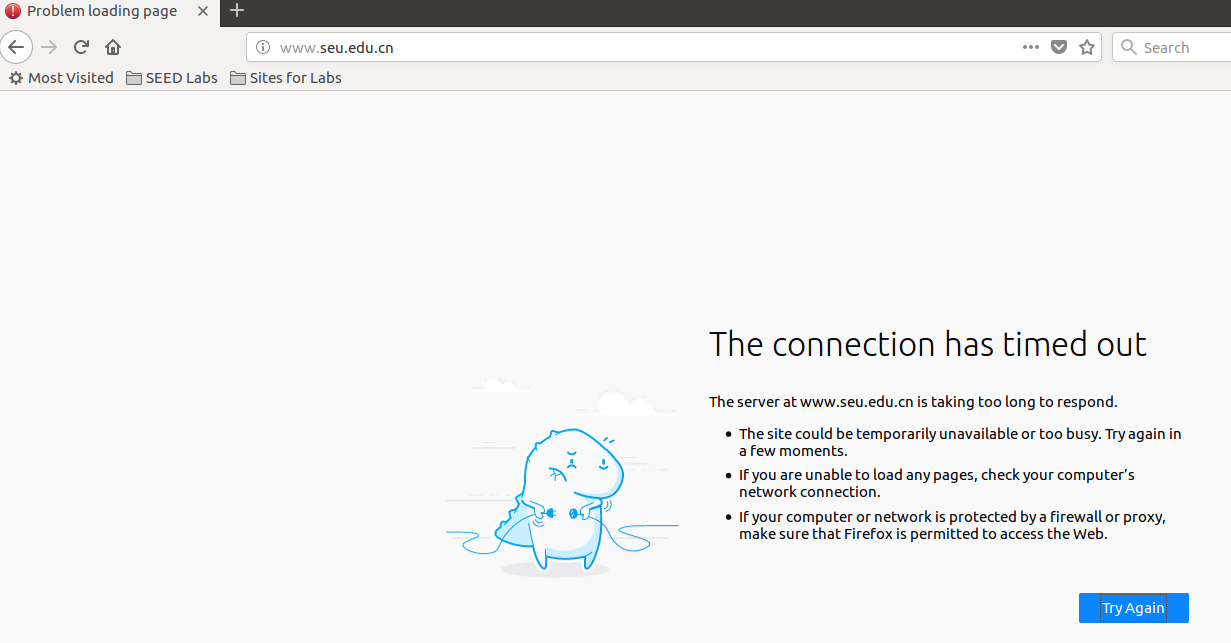
B尝试和A进行telnet连接失败：



（3）Prevent A from visiting an external web site：



无法再访问东南大学主页：



**Task2：**

代码主要部分如下：

……

unsigned int hook\_func1(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\_ICMP)

{

printk(KERN\_INFO "ICMP is banned\n");

return NF\_DROP;

}

else if(iph->protocal==IPPROTO\_TCP && tcph->dest==htons(22))

{

printk(KERN\_INFO "SSH is banned\n");

return NF\_DROP;

}

else if(iph->protocol == IPPROTO\_TCP && tcph->dest == htons(23))

{

printk(KERN\_INFO "Dropping telnet 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;

}

}

unsigned int hook\_func2(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\_ICMP){

printk(KERN\_INFO "ICMP is banned\n");

return NF\_DROP;

}

else if(iph->protocal==IPPROTO\_TCP && tcph->dest==htons(22))

{

printk(KERN\_INFO "SSH is banned\n");

return NF\_DROP;

}

else 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

{

return NF\_ACCEPT;

}

}

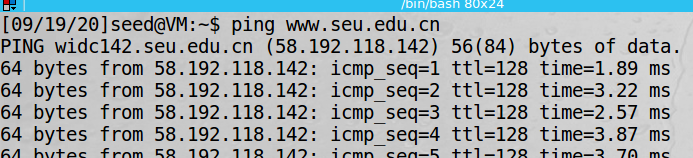
……

**Task3：**

先使用命令设置A的防火墙，禁止向外进行telnet：

sudo ufw deny out from 192.168.19.148 to any port 23

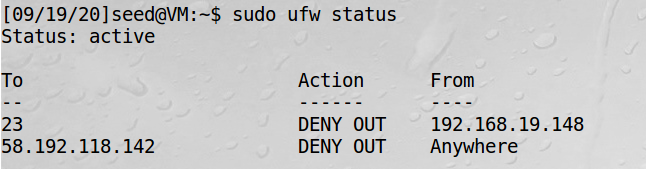
此处使用东南大学主页，查询东南大学主页的ip地址，并将其写入/etc/hosts：



执行命令禁止任何主机访问www.seu.edu.n：

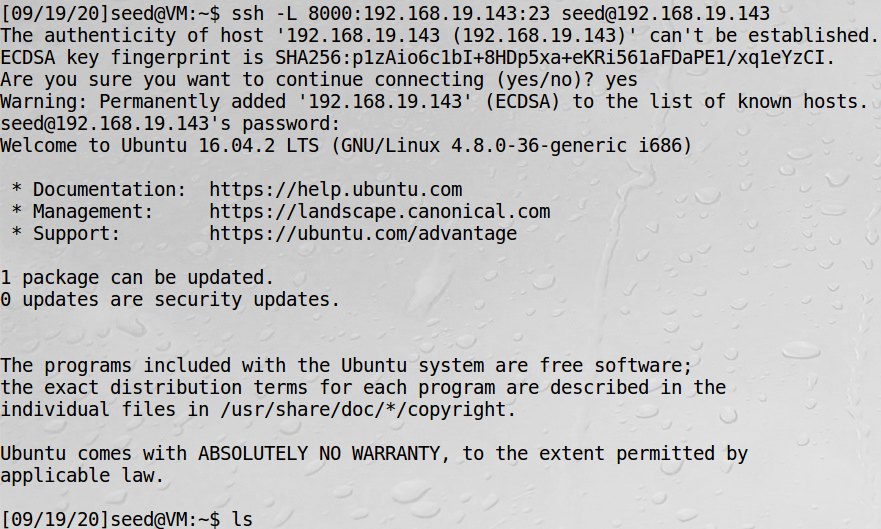
sudo ufw deny out from any to 58.192.118.142

防火墙规则如下：



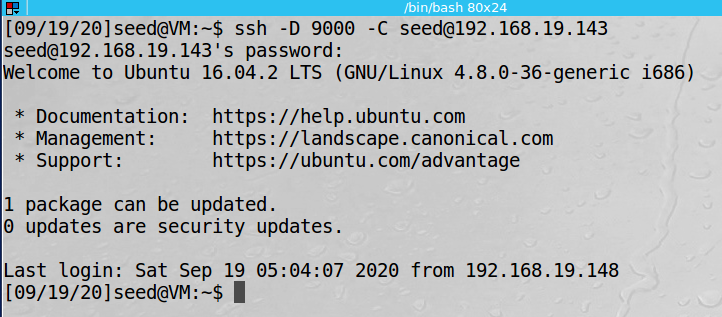
**Task3.a：**

这里采用B和C一体的形式，A成功通过通道与B进行telnet连接：



**Task3.b：**

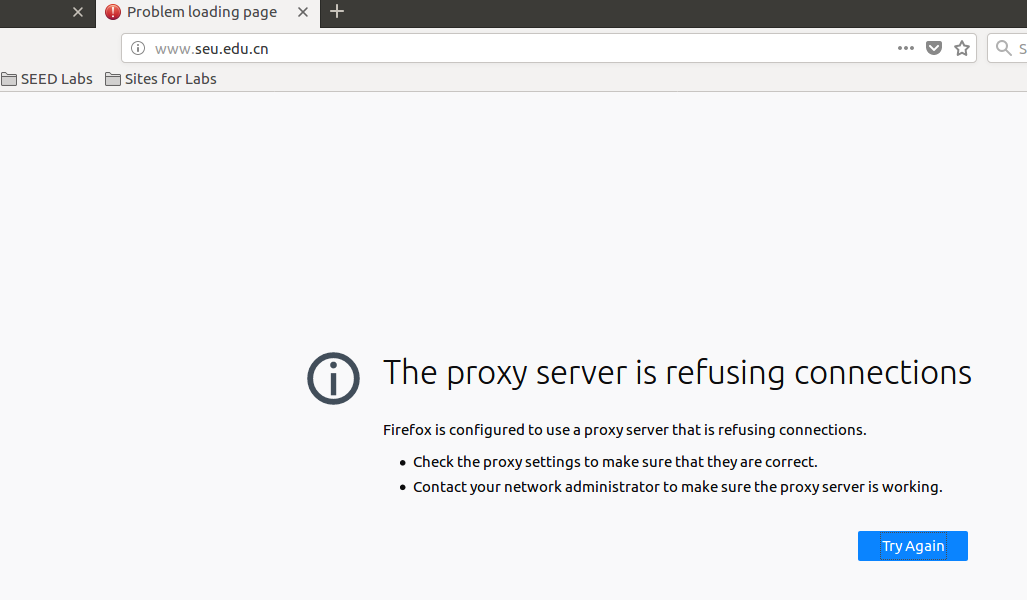
首先通过ssh连接到B：



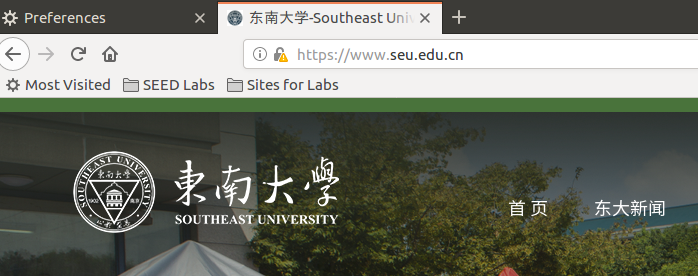
尝试访问东南大学主页成功：



断开SSH连接后，无法再访问校园主页：



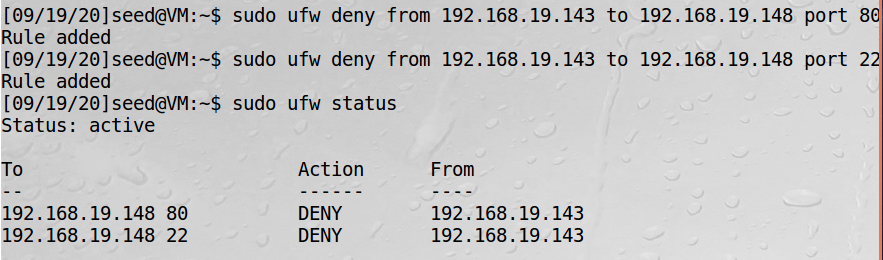
再次通过ssh连接上B后，可以访问校园主页：



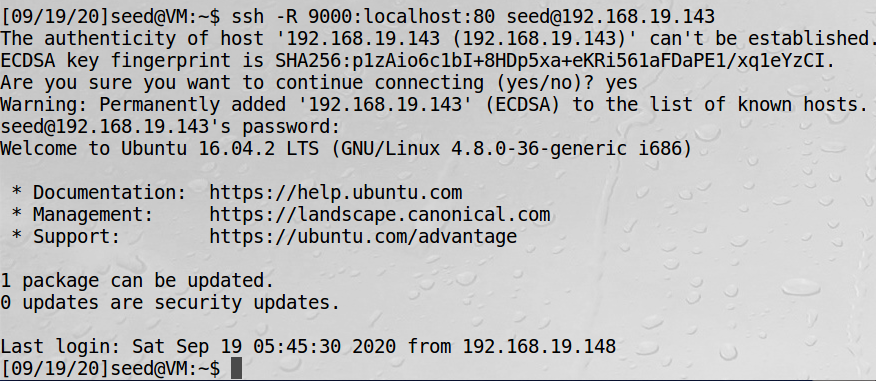
因为当A与B建立SSH连接时，B作为A的代理访问外界网页，将返回的数据传给A；当A与B断开连接后失去代理，因此无法再成功访问。

**Task4：**

先拒绝B对A的80和22端口的访问请求：



在A上与B建立反向SSH连接：



在B上使用ssh连接A成功：

