Taks1

修改 DEFAULT_INPUT_POLICY 设置为 ACCEPT。

```
# /etc/default/ufw
#

# Set to yes to apply rules to
# accepted). You will need to
# the changes to take affect.
IPV6=yes

# Set the default input policy
# you change this you will mos
DEFAULT_INPUT_POLICY="ACCEPT"
```

设置 A 阻止 23 端口的连接。

```
[09/19/20]seed@VM:~$ sudo ufw deny 23
Rules updated
Rules updated (v6)
```

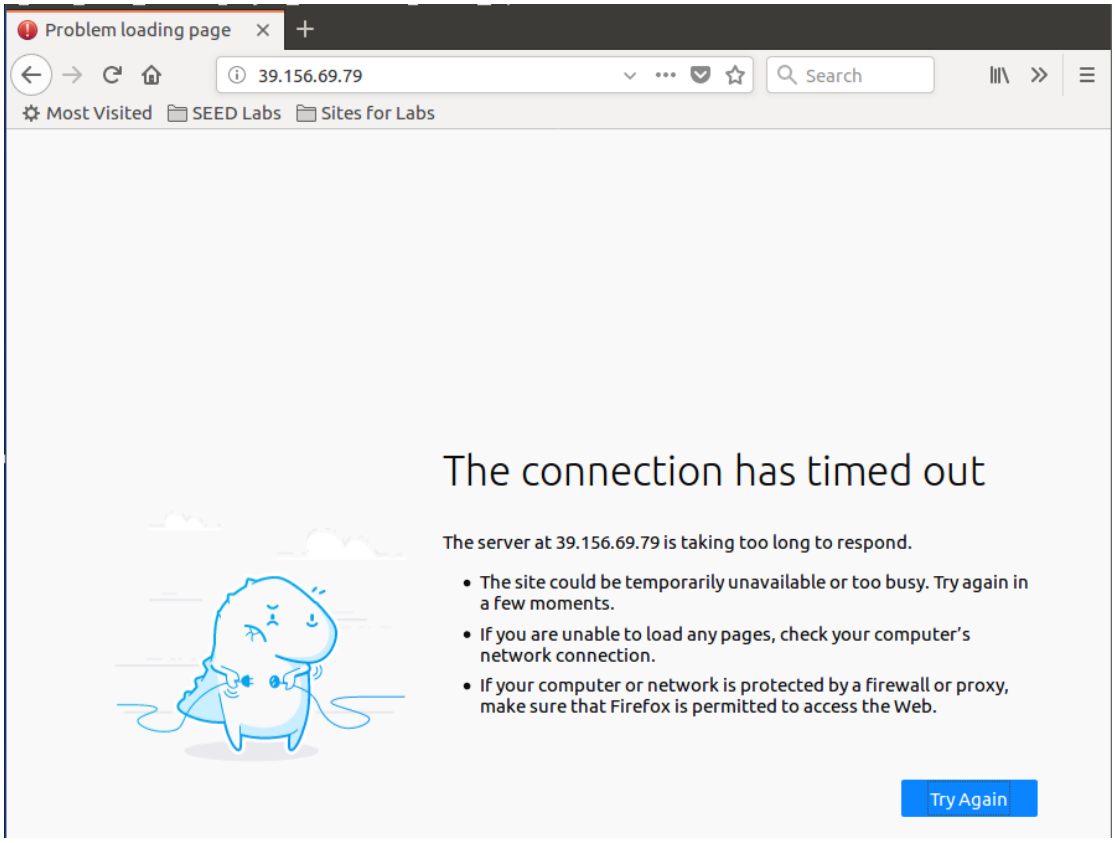
B 连接 A 的 telnet 服务

```
[09/19/20]seed@VM:~$ telnet 192.168.119.129
Trying 192.168.119.129...
telnet: Unable to connect to remote host: Connection timed out
```

在 A 中加入以下规则

```
[09/19/20]seed@VM:~$ sudo ufw deny out to 39.156.69.79
Rule added
```

打不开百度（39.156.69.79）



Task2

编写 lab6task6.c，实现对 telnet 连接的阻断

```c
#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>

static struct nf_hook_ops nfho;
unsigned int hook_func(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{
                return NF_ACCEPT;
        }
}
int init_module(void){
        printk(KERN_INFO "Registering a Telnet filter.\n");
        nfho.hook = hook_func;
        nfho.hooknum = NF_INET_POST_ROUTING;
        nfho.pf = PF_INET;
        nfho.priority = NF_IP_PRI_FIRST;
        nf_register_hook(&nfho);
        return 0;
}
void cleanup_module(void){
        printk(KERN_INFO "Telnetfilter is being removed.\n");
        nf_unregister_hook(&nfho);
}
```

编写 Makefle

```
obj-m :=lab6task2.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
```

make

```
[09/19/20]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-generi
c'
  CC [M]  /home/seed/lab6task2.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/lab6task2.mod.o
  LD [M]  /home/seed/lab6task2.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic
'
```

启用此模块后，无法进行 telnet 连接，关闭此模块，telnet 连接正常进行。

```
[09/19/20]seed@VM:~$ sudo insmod lab6task2.ko
[09/19/20]seed@VM:~$ telnet 192.168.119.139
Trying 192.168.119.139...
^C
[09/19/20]seed@VM:~$ sudo rmmod lab6task2.ko
[09/19/20]seed@VM:~$ telnet 192.168.119.139
Trying 192.168.119.139...
Connected to 192.168.119.139.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login:
```

dmesg 的输出如下

```
[61746.388699] Registering a Telnet filter.
[61872.684893] Telnetfilter is being removed.
[62037.690163] Registering a Telnet filter.
[62040.879471] Dropping telnet packet to 192.168.119.139
[62041.899238] Dropping telnet packet to 192.168.119.139
[62043.914711] Dropping telnet packet to 192.168.119.139
[62047.978847] Dropping telnet packet to 192.168.119.139
[62056.170795] Dropping telnet packet to 192.168.119.139
[62072.298658] Dropping telnet packet to 192.168.119.139
[62088.300027] Telnetfilter is being removed.
```

Task3

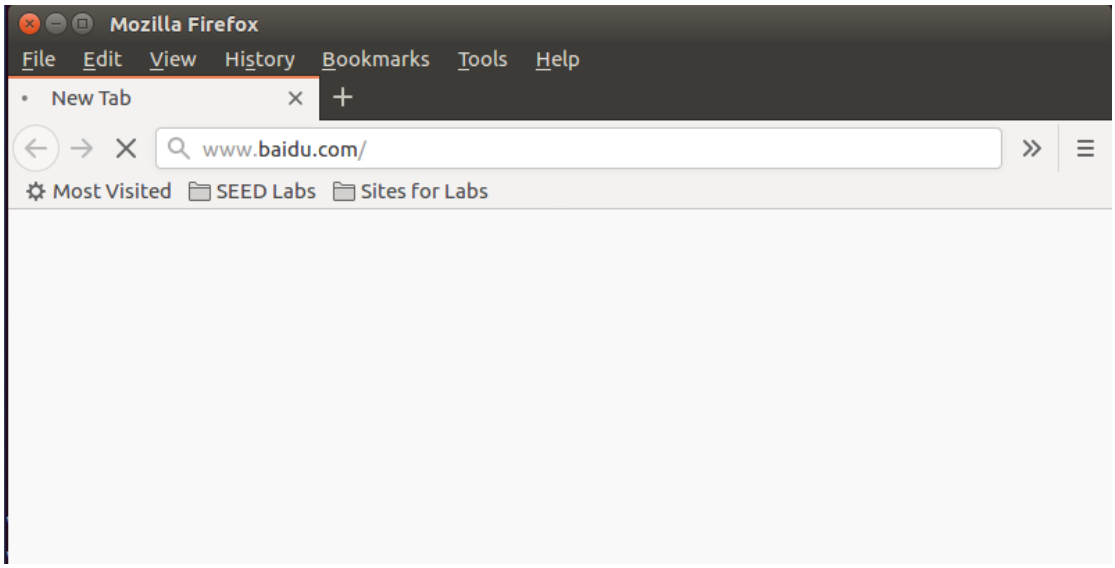
在 A 中添加规则，阻止 23 端口的所有连接。此时 A 不能与 B 进行 telnet 连接。

```
[09/19/20]seed@VM:~$ sudo ufw deny out to any port 23
Rule added
Rule added (v6)
[09/19/20]seed@VM:~$ telnet 192.168.119.139
Trying 192.168.119.139...
```

添加以下规则，拦截对百度（39.156.69.79）的访问

```
[09/19/20]seed@VM:~$ sudo ufw deny out to 39.156.69.79
Rule added
```

访问百度失败。



Task3.a

A 通过 ssh 连接 B

```
[09/19/20]seed@VM:~$ ssh -L 8000:192.168.119.139:23 seed@192.168.11
9.139
seed@192.168.119.139'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: Sat Sep 19 23:17:16 2020 from 192.168.119.129
```

再在 A 上通过 telnet 连接本机的 8000 端口

```
[09/19/20]seed@VM:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login:
```

查看 wireshark 抓包情况，telnet 通过隧道绕过防火墙。

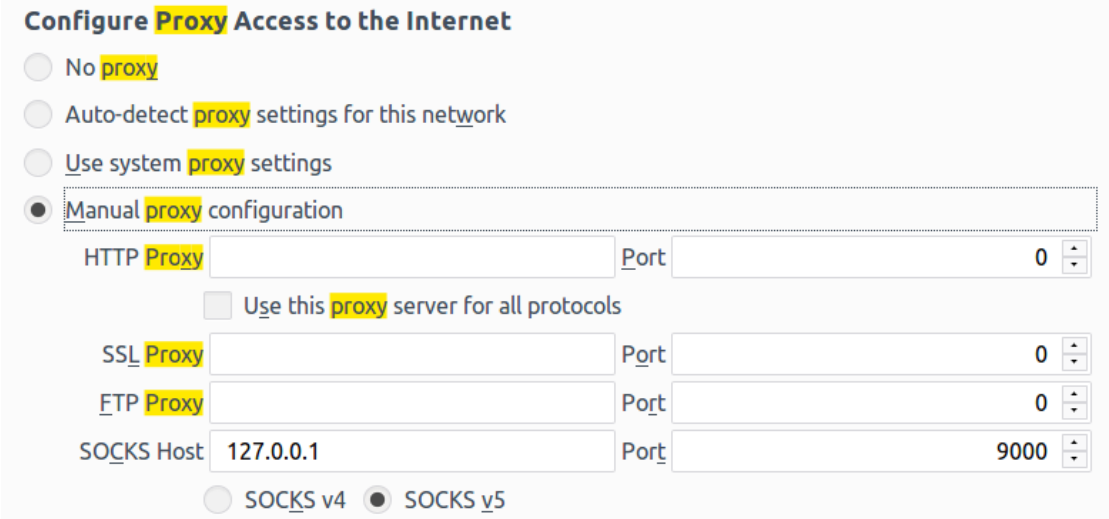
23	2020-09-19 23:20:06.7987778…	192.168.119.139	192.168.119.129	SSH	118 Ser
24	2020-09-19 23:20:06.7988174…	192.168.119.129	192.168.119.139	TCP	66 582
25	2020-09-19 23:20:06.7990523…	192.168.119.129	192.168.119.139	SSH	118 Cli
26	2020-09-19 23:20:06.7997311…	192.168.119.139	192.168.119.129	SSH	126 Ser
27	2020-09-19 23:20:06.7998790…	192.168.119.129	192.168.119.139	SSH	166 Cli
28	2020-09-19 23:20:06.8008264…	192.168.119.139	192.168.119.129	SSH	118 Ser
29	2020-09-19 23:20:06.8009907…	192.168.119.129	192.168.119.139	SSH	126 Cli
30	2020-09-19 23:20:06.8038524…	192.168.119.139	192.168.119.129	SSH	110 Ser
31	2020-09-19 23:20:06.8040056…	192.168.119.129	192.168.119.139	SSH	110 Cli
32	2020-09-19 23:20:06.8046084…	192.168.119.139	192.168.119.129	SSH	134 Ser
33	2020-09-19 23:20:06.8473704…	192.168.119.129	192.168.119.139	TCP	66 582

Task3.b

有防火墙时，无法访问百度，A 通过 ssh 连接 B，建立 ssh 端口的动态转发

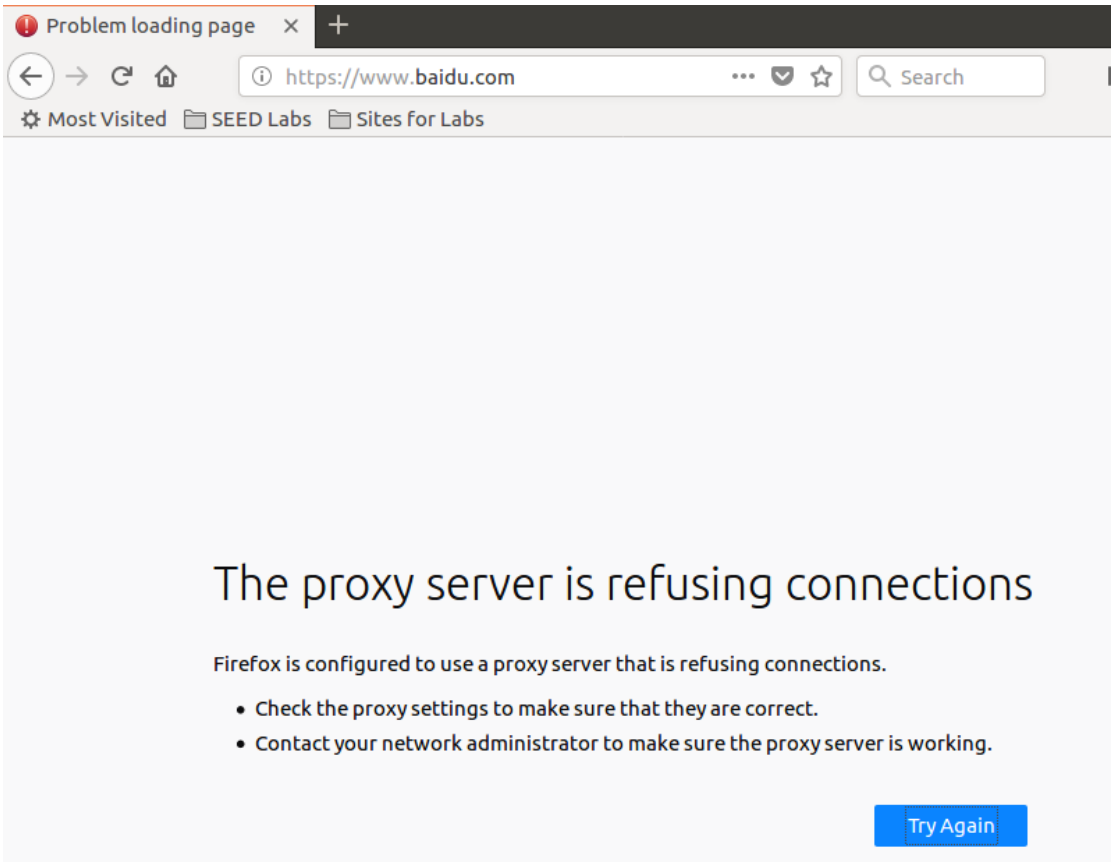
```
[09/19/20]seed@VM:~$ ssh -D 9000 -C seed@192.168.119.139
seed@192.168.119.139's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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: Sat Sep 19 23:17:29 2020 from 192.168.119.129
```

修改浏览器设置，将数据转发至 9000 端口



可以访问百度。

断开与 B 的 ssh 连接，访问百度失败



Task4

在 A 中添加以下规则，阻止 22 和 80 端口的连接

```
[09/19/20]seed@VM:~$ sudo ufw deny 22
Rule added
Rule added (v6)
[09/19/20]seed@VM:~$ sudo ufw deny 80
Rule added
Rule added (v6)
```

在 B 中利用 nmap 查看 A 的端口情况，22 和 80 端口关闭。

```
[09/19/20]seed@VM:~$ nmap 192.168.119.129

Starting Nmap 7.01 ( https://nmap.org ) at 2020-09-19 23:34 EDT
Nmap scan report for 192.168.119.129
Host is up (0.0038s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   open     telnet
53/tcp   open     domain
80/tcp   filtered http
3128/tcp open     squid-http
```

利用 ssh 隧道，将 B 的 10000 端口转发到 22 端口

```
[09/19/20]seed@VM:~$ ssh -f -N -R 10000:localhost:22 seed@192.168.1
19.139
```

在 B 上建立反向隧道

```
[09/19/20]seed@VM:~$ ssh seed@localhost -p 10000
The authenticity of host '[localhost]:10000 ([127.0.0.1]:10000)' ca
n'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 '[localhost]:10000' (ECDSA) to the list
of known hosts.
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

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 b
y
applicable law.
```