Task1:

在机器 A 上打开防火墙:

```
[09/19/20]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

用机器 B 去 telnet 机器 A，可以看见一直无法连接:

```
[09/19/20]seed@VM:~$ sudo telnet 10.0.2.9
Trying 10.0.2.9...
```

同理，在机器 B 上打开防火墙，可以使得机器 B 也无法 telnet 它。

在机器 A 上对 www.seu.edu.cn 打开防火墙，再次 telnet 发现已经无法到达了:

```
[09/19/20]seed@VM:~$ sudo ufw deny out to 121.194.14.14
2
Rules updated
```

```
[09/19/20]seed@VM:~$ telnet 121.194.14.142
Trying 121.194.14.142...
telnet: Unable to connect to remote host: Connection re
fused
[09/19/20]seed@VM:~$
```

Task2:

编写 netfilter 过滤代码，过滤掉指定机器 10.0.2.6 发来的的包:

```
static struct nf_hook_ops nfho;
static unsigned char *drop_ip="\x0a\x00\x02\x06";
unsigned int hook_func(void *priv, struct sk_buff *skb,
 const struct nf_hook_state *state)
{
        struct iphdr *ip_header=(struct iphdr *)skb_net
work_header(skb);
        unsigned char  *src_ip=ip_header->saddr;
        unsigned char *dest_ip=ip_header->daddr;

        if(src_ip==drop_ip)
        {
                return NF_DROP;
        }
        else
        {
                return NF_ACCEPT;
        }
}
int init_module()
{
        nfho.hook=hook_func;
        nfho.hooknum=NF_INET_PRE_ROUTING;
        nfho.pf=PF_INET;
        nfho.priority=NF_IP_PRI_FIRST;
        nf_register_hook(&nfho);
        return 0;
}
```

编写 makefile 文件:

```
obj-m :=hook.o
KERNELDIR?=/lib/modules/$(shell uname -r)/build/
PWD :=$(shell pwd)
default:
        $(MAKE) -C $(KERNELDIR) M=$(PWD) modules
clean:
        $(MAKE) -C $(KERNELDIR) M=$(PWD) clean
```

Make 内核后打开 hook:

```
[09/19/20]seed@VM:~$ sudo insmod hook.ko
[09/19/20]seed@VM:~$ lsmod
Module                  Size  Used by
hook                   16384  0
```

再次 ping 该地址的主机发现已经被屏蔽:

```
[09/19/20]seed@VM:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

Task3.a:

先打开防火墙屏蔽掉所有 telnet 报文:

```
[09/19/20]seed@VM:~$ sudo ufw deny out from 10.0.2.9 to
 any port 23
Rule added
```

在 A 和 B 之间建立 ssh 连接:

```
[09/19/20]seed@VM:~$ ssh -L 8000:10.0.2.6:23 seed@10.0.
2.6
seed@10.0.2.6's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-gener
ic 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 22:27:39 2020
```

此时再尝试通过 ssh 隧道对 B 进行 telnet:

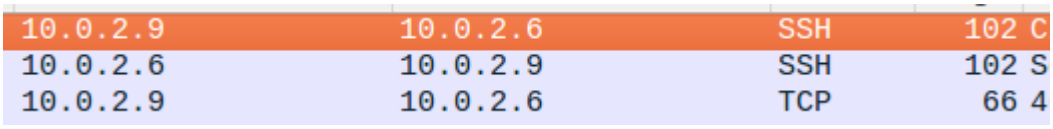
```
[09/19/20]seed@VM:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Sep 19 22:29:38 EDT 2020 from 10.0.2.6
on pts/19
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-gener
ic i686)

 * 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.

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

查看 wireshark 抓取的报文可以看到，主机 A 和 B 之间的通信都是通过 ssh 协议传输 tcp 报文：

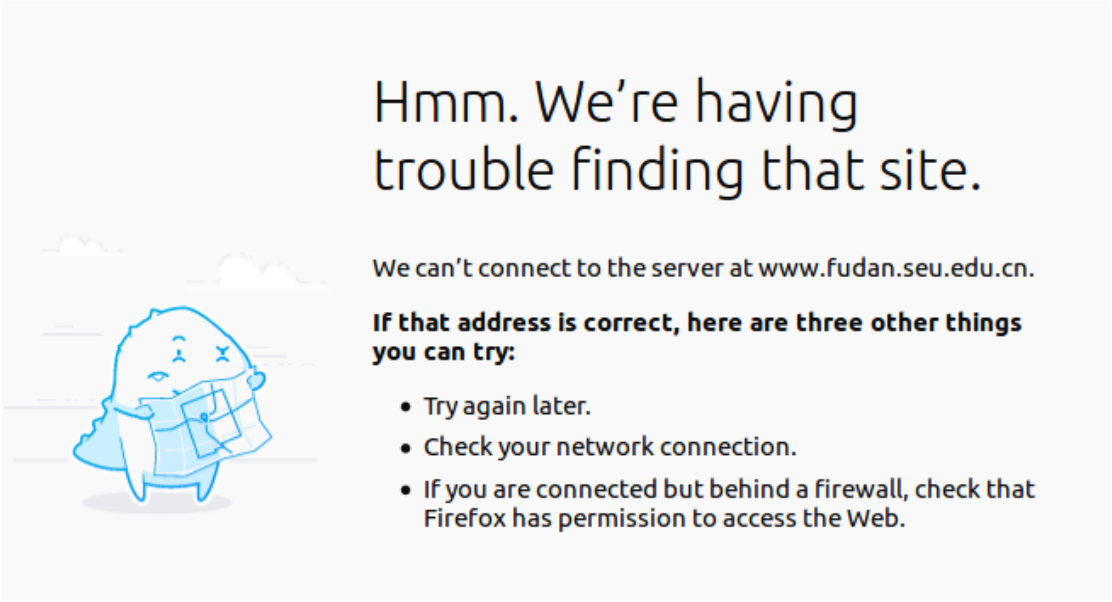


Task3.b：

先用防火墙屏蔽掉复旦大学官网：（因为 seu 官网证书出现了问题，火狐浏览器阻止了访问，所以换一个学校的官网）

```
[09/19/20]seed@VM:~$ sudo ufw deny out from 10.0.2.9 to
 202.120.224.81
Rules updated
```

然后使用火狐浏览器访问该网站，发现已经无法连接：



然后使用 ssh 与机器 B 进行连接后，再次访问网站，发现已经可以访问到该网站了：

```
[09/19/20]seed@VM:~$ ssh -D 9000 -C seed@10.0.2.6
seed@10.0.2.6's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-gener
ic 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 22:30:22 2020
```

Task4:

先打开服务器 A 防火墙阻止其被从外部访问:

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

设置反向 ssh 隧道:

```
[09/19/20]seed@VM:~$ ssh -p 22 -qngfNTR 7000:localhost:
22 seed@10.0.2.6
```

在 B 上对 A 进行连接，发现连接成功，于是可以实现 B 对 A 的访问:

```
[09/19/20]seed@VM:~$ ssh -p 7000 seed@localhost
The authenticity of host '[localhost]:7000 ([127.0.0.1]
:7000)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKR
i561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)?
yes
Warning: Permanently added '[localhost]:7000' (ECDSA) t
o the list of known hosts.
seed@localhost's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-gener
ic 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 22:52:23 2020 from 10.0.2.6
```