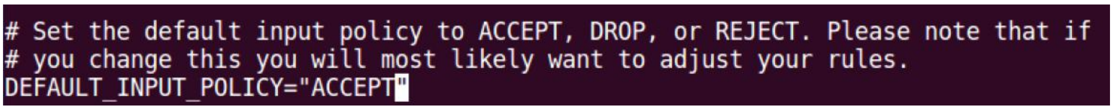
网络空间安全实训作业

57117225

宋宇星

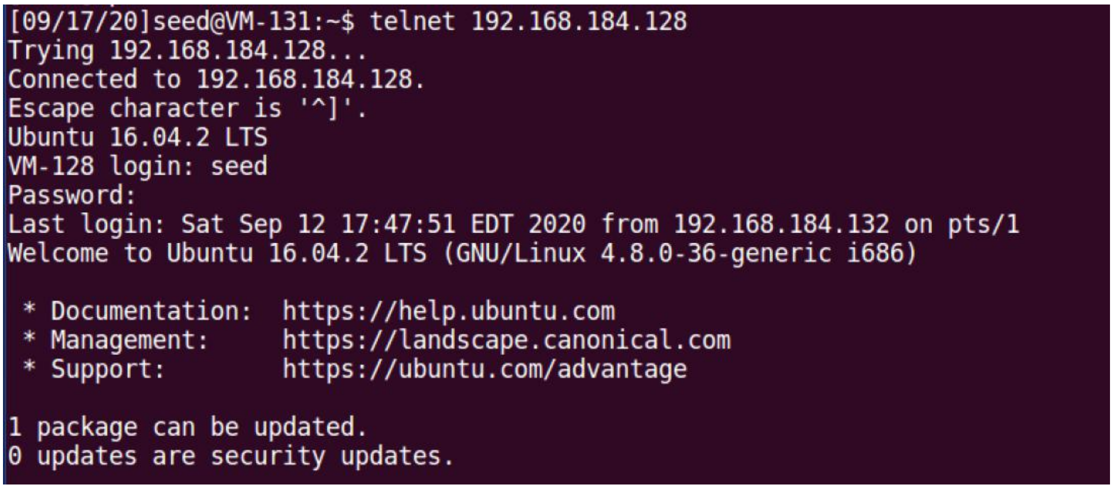
Task1：

配置



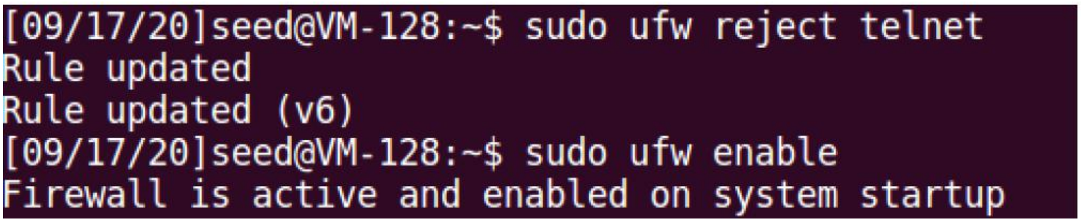
```
# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="ACCEPT"
```

允许远程控制



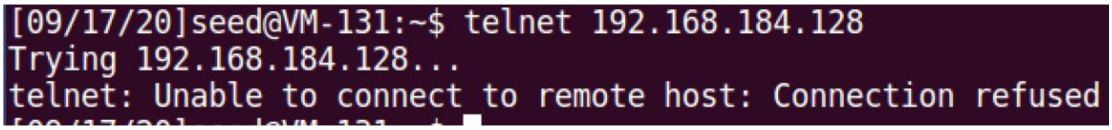
```
[09/17/20]seed@VM-131:~$ telnet 192.168.184.128
Trying 192.168.184.128...
Connected to 192.168.184.128.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM-128 login: seed
Password:
Last login: Sat Sep 12 17:47:51 EDT 2020 from 192.168.184.132 on pts/1
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic 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.
```

开启防火墙



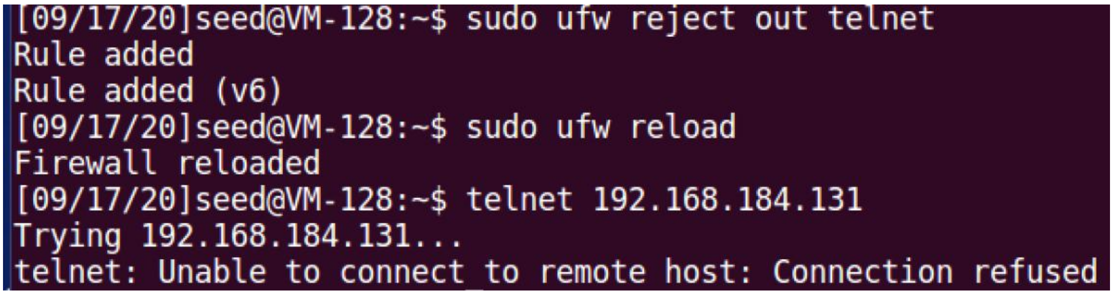
```
[09/17/20]seed@VM-128:~$ sudo ufw reject telnet
Rule updated
Rule updated (v6)
[09/17/20]seed@VM-128:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

现在不能远程控制了



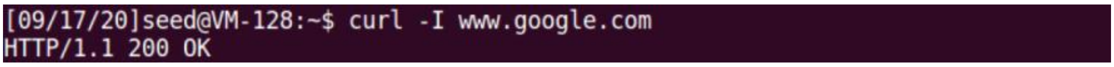
```
[09/17/20]seed@VM-131:~$ telnet 192.168.184.128
Trying 192.168.184.128...
telnet: Unable to connect to remote host: Connection refused
```

添加一条规则，阻止来自 A 的远程登陆



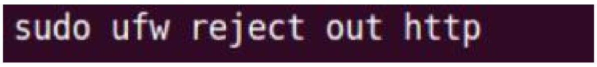
```
[09/17/20]seed@VM-128:~$ sudo ufw reject out telnet
Rule added
Rule added (v6)
[09/17/20]seed@VM-128:~$ sudo ufw reload
Firewall reloaded
[09/17/20]seed@VM-128:~$ telnet 192.168.184.131
Trying 192.168.184.131...
telnet: Unable to connect to remote host: Connection refused
```

成功受到外部网站的应答



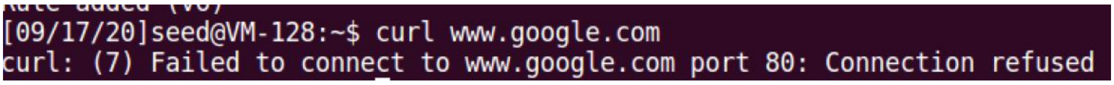
```
[09/17/20]seed@VM-128:~$ curl -I www.google.com
HTTP/1.1 200 OK
```

启动防火墙阻止访问外部网站



```
sudo ufw reject out http
```

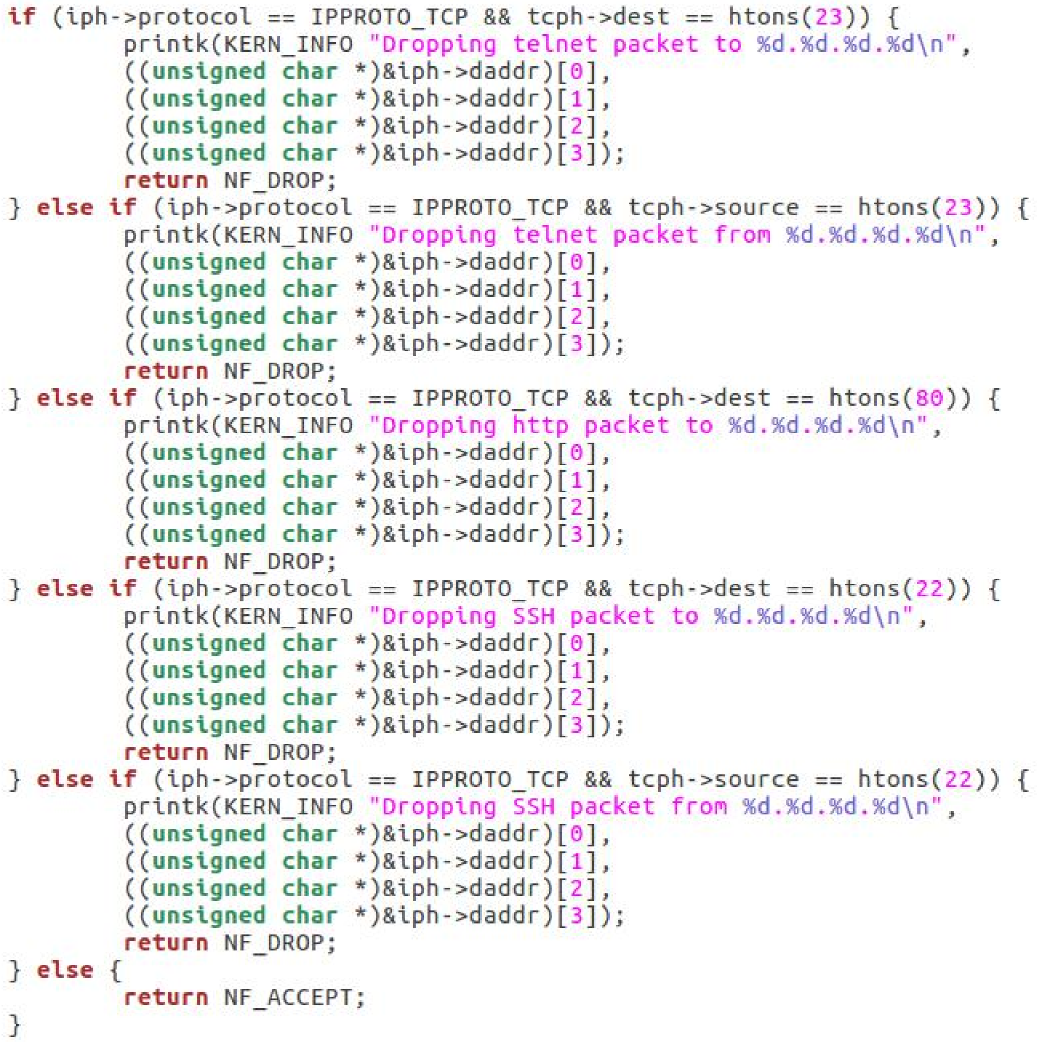
无法连接了



```
Rule added (v6)
[09/17/20]seed@VM-128:~$ curl www.google.com
curl: (7) Failed to connect to www.google.com port 80: Connection refused
```

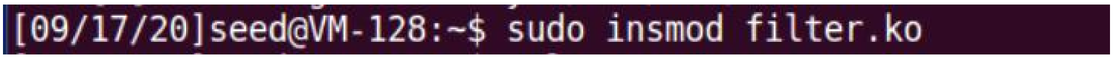
Task2：实现一个简单的防火墙

增添规则



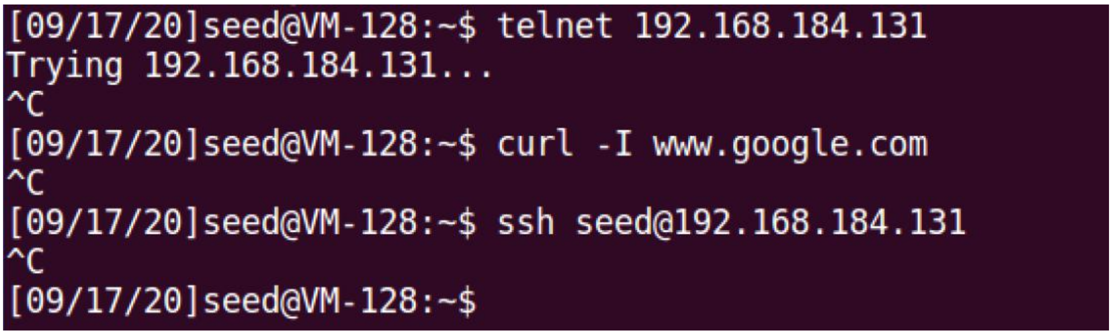
```
if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(23)) {
        printk(KERN_INFO "Dropping telnet packet to %d.%d.%d.%d\n",
        ((unsigned char *)&iph->daddr)[0],
        ((unsigned char *)&iph->daddr)[1],
        ((unsigned char *)&iph->daddr)[2],
        ((unsigned char *)&iph->daddr)[3]);
        return NF_DROP;
} else if (iph->protocol == IPPROTO_TCP && tcph->source == 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 if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(80)) {
        printk(KERN_INFO "Dropping http 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 if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(22)) {
        printk(KERN_INFO "Dropping SSH 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 if (iph->protocol == IPPROTO_TCP && tcph->source == htons(22)) {
        printk(KERN_INFO "Dropping SSH 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;
}
```

编译和并插入内核模块

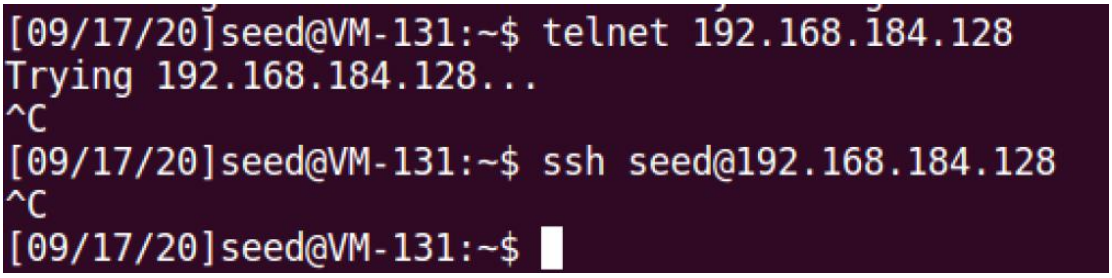


```
[09/17/20]seed@VM-128:~$ sudo insmod filter.ko
```

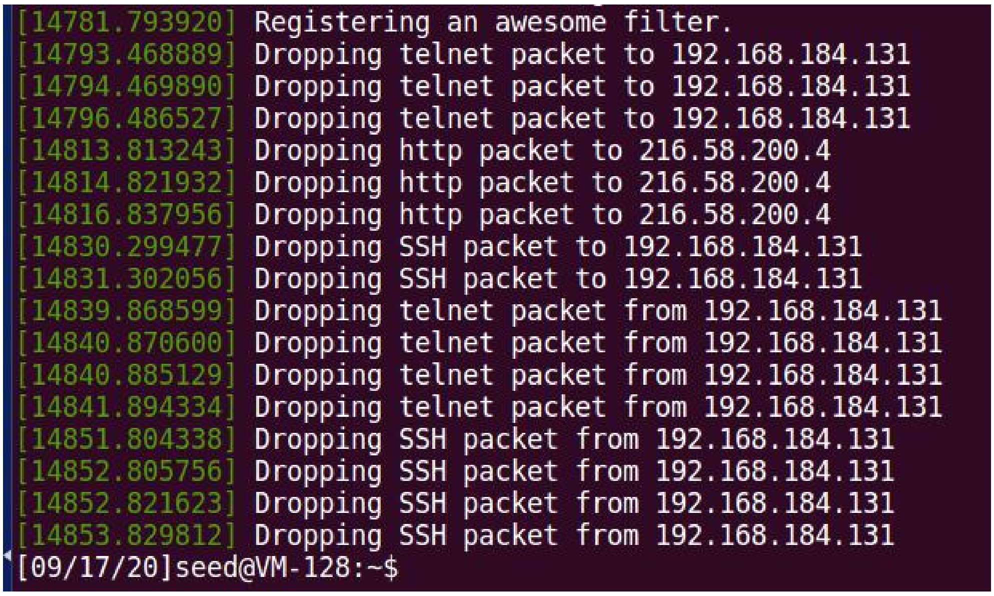
从日志中看到更新后的访问都被过滤了



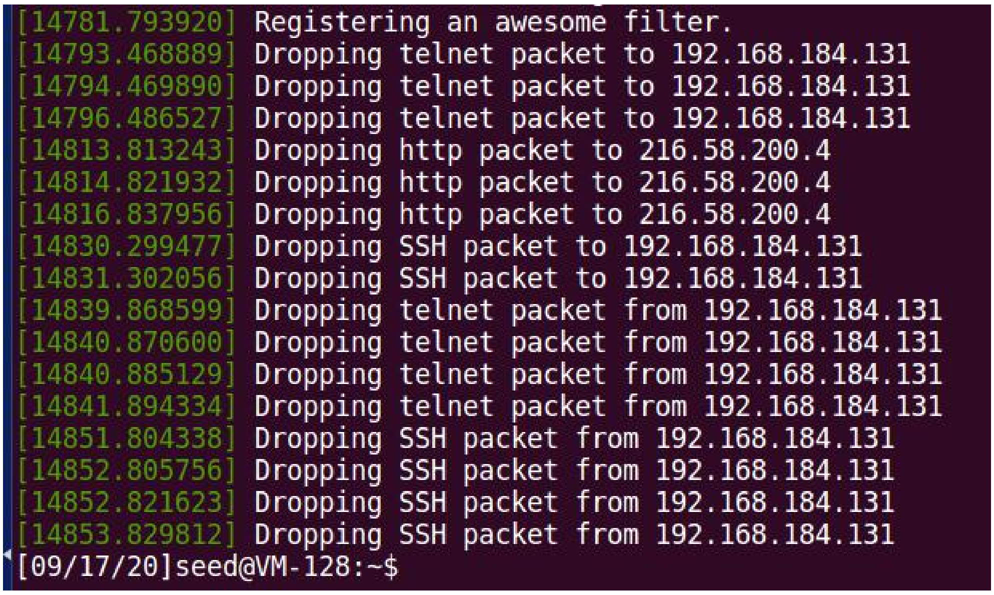
```
[09/17/20]seed@VM-128:~$ telnet 192.168.184.131
Trying 192.168.184.131...
^C
[09/17/20]seed@VM-128:~$ curl -I www.google.com
^C
[09/17/20]seed@VM-128:~$ ssh seed@192.168.184.131
^C
[09/17/20]seed@VM-128:~$
```



```
[09/17/20]seed@VM-131:~$ telnet 192.168.184.128
Trying 192.168.184.128...
^C
[09/17/20]seed@VM-131:~$ ssh seed@192.168.184.128
^C
[09/17/20]seed@VM-131:~$ 
```

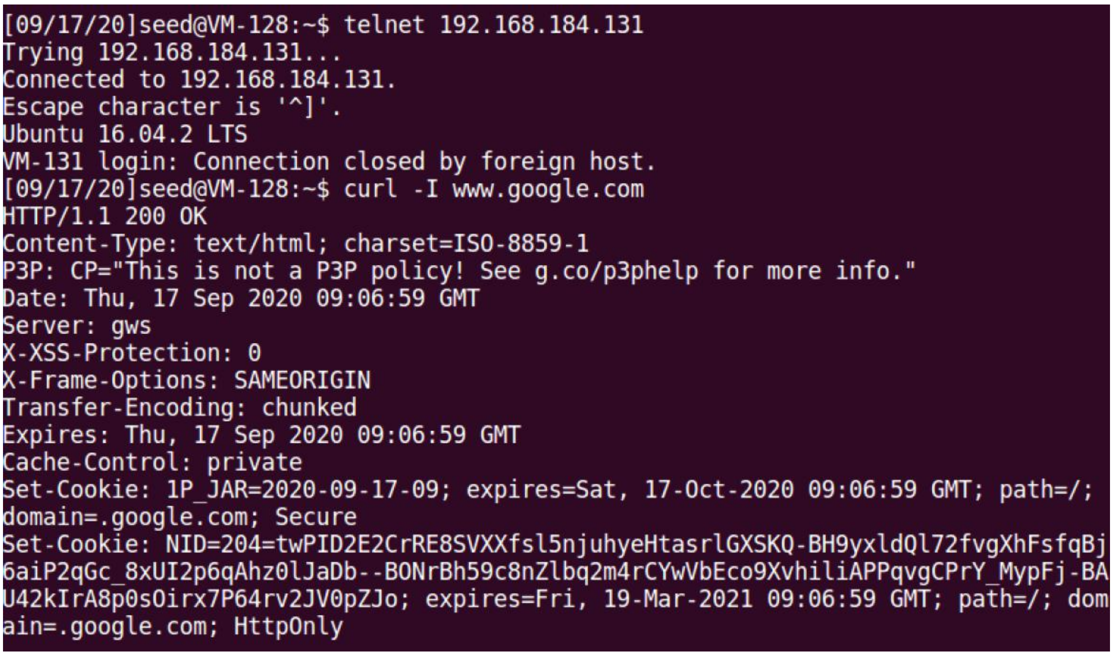


```
[14781.793920] Registering an awesome filter.
[14793.468889] Dropping telnet packet to 192.168.184.131
[14794.469890] Dropping telnet packet to 192.168.184.131
[14796.486527] Dropping telnet packet to 192.168.184.131
[14813.813243] Dropping http packet to 216.58.200.4
[14814.821932] Dropping http packet to 216.58.200.4
[14816.837956] Dropping http packet to 216.58.200.4
[14830.299477] Dropping SSH packet to 192.168.184.131
[14831.302056] Dropping SSH packet to 192.168.184.131
[14839.868599] Dropping telnet packet from 192.168.184.131
[14840.870600] Dropping telnet packet from 192.168.184.131
[14840.885129] Dropping telnet packet from 192.168.184.131
[14841.894334] Dropping telnet packet from 192.168.184.131
[14851.804338] Dropping SSH packet from 192.168.184.131
[14852.805756] Dropping SSH packet from 192.168.184.131
[14852.821623] Dropping SSH packet from 192.168.184.131
[14853.829812] Dropping SSH packet from 192.168.184.131
[09/17/20]seed@VM-128:~$
```



```
[14781.793920] Registering an awesome filter.
[14793.468889] Dropping telnet packet to 192.168.184.131
[14794.469890] Dropping telnet packet to 192.168.184.131
[14796.486527] Dropping telnet packet to 192.168.184.131
[14813.813243] Dropping http packet to 216.58.200.4
[14814.821932] Dropping http packet to 216.58.200.4
[14816.837956] Dropping http packet to 216.58.200.4
[14830.299477] Dropping SSH packet to 192.168.184.131
[14831.302056] Dropping SSH packet to 192.168.184.131
[14839.868599] Dropping telnet packet from 192.168.184.131
[14840.870600] Dropping telnet packet from 192.168.184.131
[14840.885129] Dropping telnet packet from 192.168.184.131
[14841.894334] Dropping telnet packet from 192.168.184.131
[14851.804338] Dropping SSH packet from 192.168.184.131
[14852.805756] Dropping SSH packet from 192.168.184.131
[14852.821623] Dropping SSH packet from 192.168.184.131
[14853.829812] Dropping SSH packet from 192.168.184.131
[09/17/20]seed@VM-128:~$
```

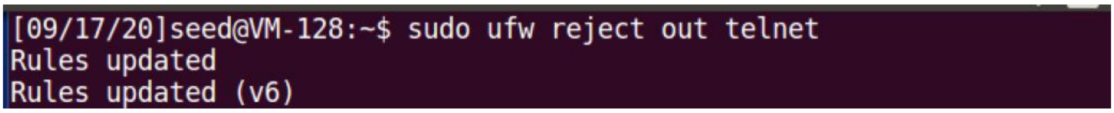
移除模块，又恢复正常了



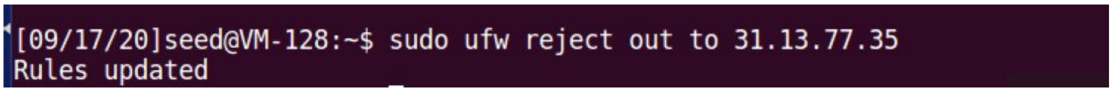
```
[09/17/20]seed@VM-128:~$ telnet 192.168.184.131
Trying 192.168.184.131...
Connected to 192.168.184.131.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM-131 login: Connection closed by foreign host.
[09/17/20]seed@VM-128:~$ curl -I www.google.com
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Thu, 17 Sep 2020 09:06:59 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Transfer-Encoding: chunked
Expires: Thu, 17 Sep 2020 09:06:59 GMT
Cache-Control: private
Set-Cookie: 1P_JAR=2020-09-17-09; expires=Sat, 17-Oct-2020 09:06:59 GMT; path=/;
domain=.google.com; Secure
Set-Cookie: NID=204=twPID2E2CrRE8SVXXfsl5njuhyeHtasrlGXSKQ-BH9yxldQl72fvgXhFsfqBj
6aiP2qGc_8xUI2p6qAhz0lJaDb--BONrBh59c8nZlbq2m4rCYwVbEco9XvhiliAPPqvgCPrY_MypFj-BA
U42kIrA8p0sOirx7P64rv2JV0pZJo; expires=Fri, 19-Mar-2021 09:06:59 GMT; path=/; dom
ain=.google.com; HttpOnly
```

Task3:

配置由内而外的拒绝远程登陆和脸谱

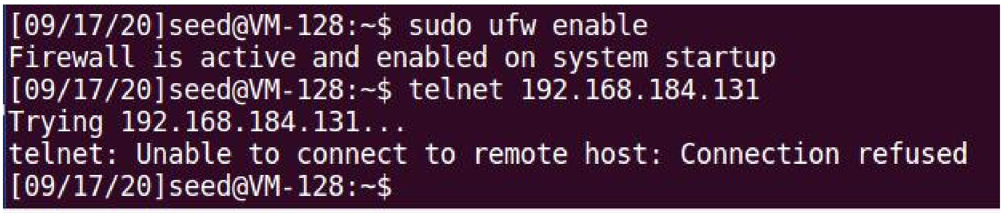


```
[09/17/20]seed@VM-128:~$ sudo ufw reject out telnet
Rules updated
Rules updated (v6)
```

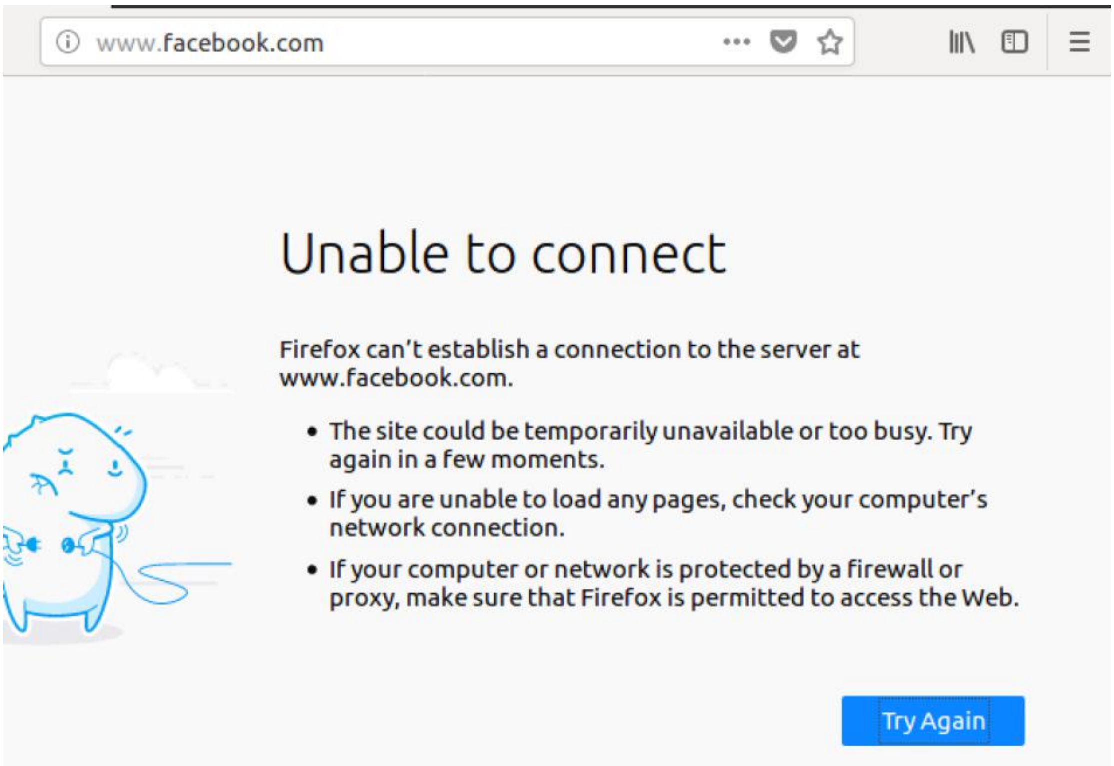


```
[09/17/20]seed@VM-128:~$ sudo ufw reject out to 31.13.77.35
Rules updated
```

检验



```
[09/17/20]seed@VM-128:~$ sudo ufw enable
Firewall is active and enabled on system startup
[09/17/20]seed@VM-128:~$ telnet 192.168.184.131
Trying 192.168.184.131...
telnet: Unable to connect to remote host: Connection refused
[09/17/20]seed@VM-128:~$
```



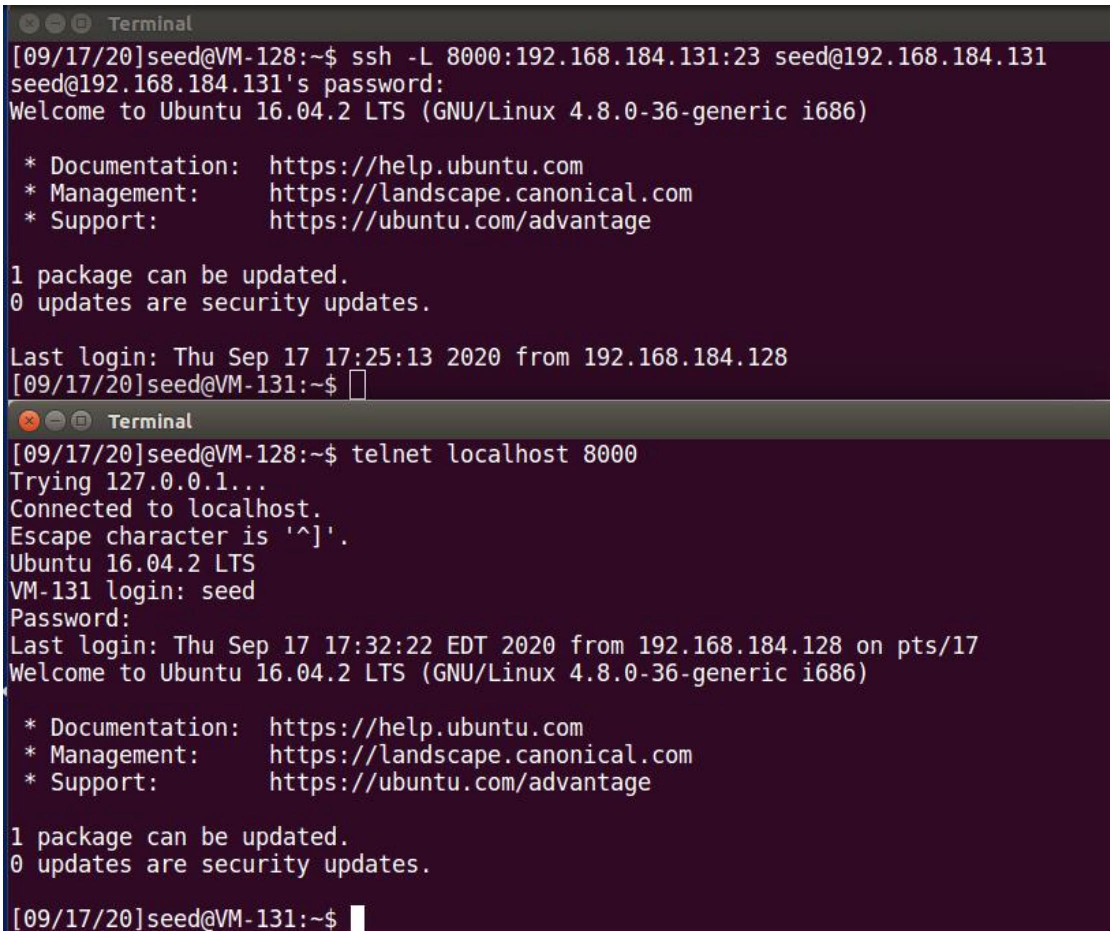
www.facebook.com

Unable to connect

Firefox can’t establish a connection to the server at www.facebook.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer’s network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

使用 SSH 隧道访问 B

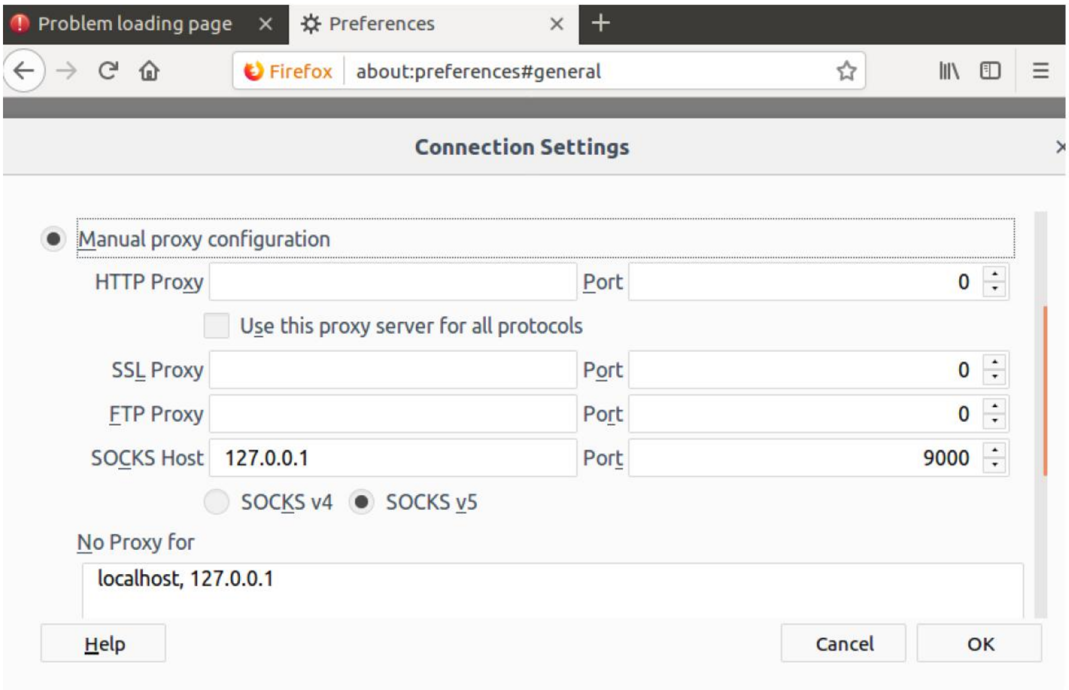


```
[09/17/20]seed@VM-128:~$ ssh -L 8000:192.168.184.131:23 seed@192.168.184.131
seed@192.168.184.131's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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 17:25:13 2020 from 192.168.184.128
[09/17/20]seed@VM-131:~$ 
```

```
[09/17/20]seed@VM-128:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM-131 login: seed
Password:
Last login: Thu Sep 17 17:32:22 EDT 2020 from 192.168.184.128 on pts/17
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-131:~$ 
```

使用 SSH 访问脸书

配置代理



Connection Settings

● Manual proxy configuration

HTTP Proxy: (empty) Port: 0

□ Use this proxy server for all protocols

SSL Proxy: (empty) Port: 0

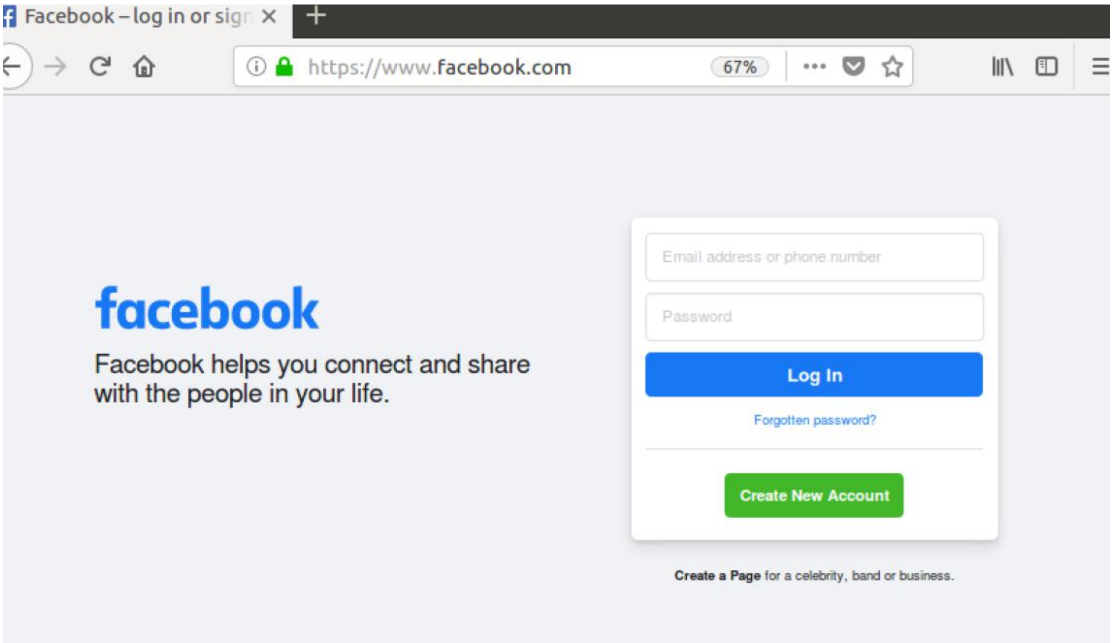
FTP Proxy: (empty) Port: 0

SOCKS Host: 127.0.0.1 Port: 9000

○ SOCKS v4 ● SOCKS v5

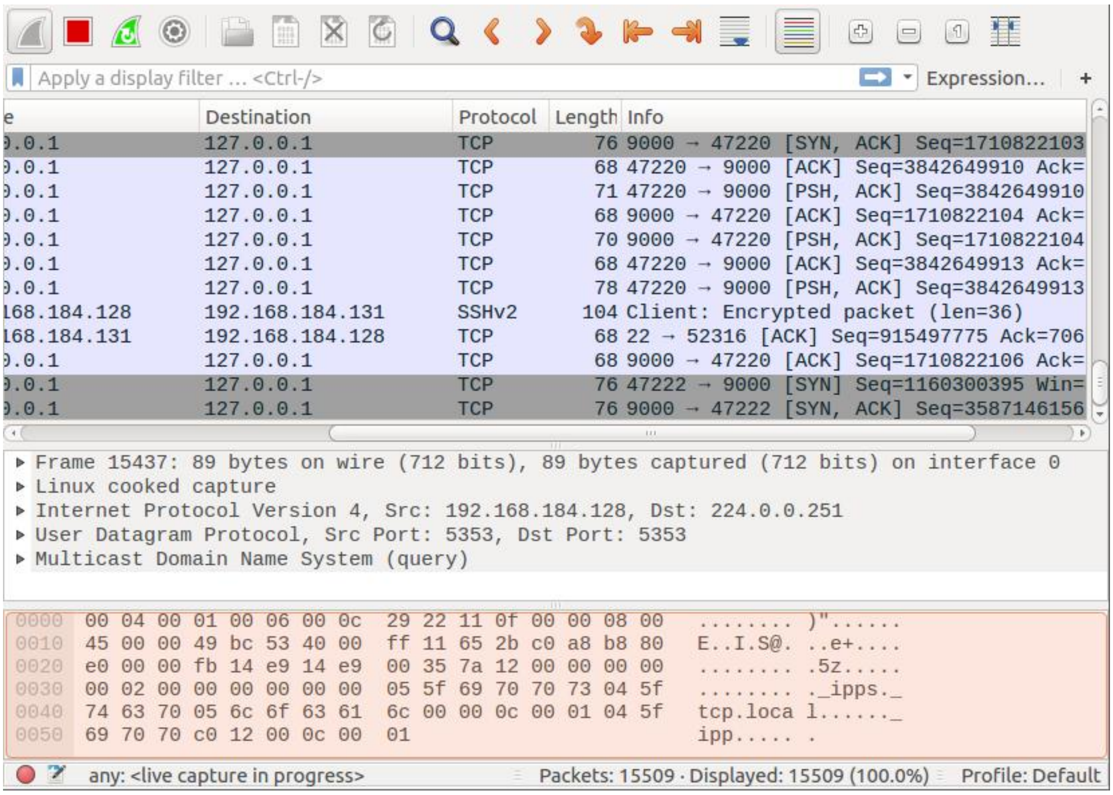
No Proxy for

localhost, 127.0.0.1


Facebook – log in or sign
https://www.facebook.com
67%
facebook
Facebook helps you connect and share with the people in your life.
Email address or phone number
Password
Log In
Forgotten password?
Create New Account
Create a Page for a celebrity, band or business.

停用 SSH，访问又失败了，具体图片同上

从 wireshark 上看到主机在和外部网络通信，浏览器绕过了防火墙



```
e                 Destination            Protocol  Length  Info
).0.1             127.0.0.1              TCP           76 9000 → 47220 [SYN, ACK] Seq=1710822103
).0.1             127.0.0.1              TCP           68 47220 → 9000 [ACK] Seq=3842649910 Ack=
).0.1             127.0.0.1              TCP           71 47220 → 9000 [PSH, ACK] Seq=3842649910
).0.1             127.0.0.1              TCP           68 9000 → 47220 [ACK] Seq=1710822104 Ack=
).0.1             127.0.0.1              TCP           70 9000 → 47220 [PSH, ACK] Seq=1710822104
).0.1             127.0.0.1              TCP           68 47220 → 9000 [ACK] Seq=3842649913 Ack=
).0.1             127.0.0.1              TCP           78 47220 → 9000 [PSH, ACK] Seq=3842649913
168.184.128       192.168.184.131        SSHv2        104 Client: Encrypted packet (len=36)
168.184.131       192.168.184.128        TCP           68 22 → 52316 [ACK] Seq=915497775 Ack=706
).0.1             127.0.0.1              TCP           68 9000 → 47220 [ACK] Seq=1710822106 Ack=
).0.1             127.0.0.1              TCP           76 47222 → 9000 [SYN] Seq=1160300395 Win=
).0.1             127.0.0.1              TCP           76 9000 → 47222 [SYN, ACK] Seq=3587146156
```

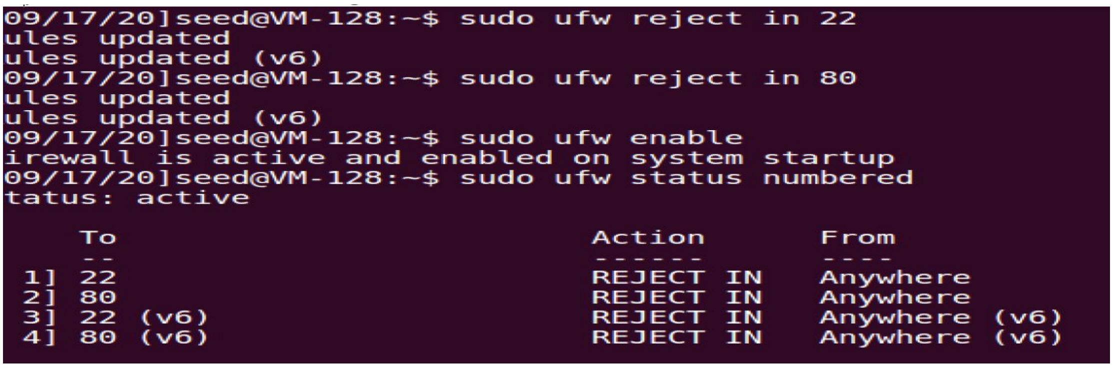
```
▸ Frame 15437: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.184.128, Dst: 224.0.0.251
▸ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▸ Multicast Domain Name System (query)
```

```
0000  00 04 00 01 00 06 00 0c  29 22 11 0f 00 00 08 00   ........ )"......
0010  45 00 00 49 bc 53 40 00  ff 11 65 2b c0 a8 b8 80   E..I.S@. ..e+....
0020  e0 00 00 fb 14 e9 14 e9  00 35 7a 12 00 00 00 00   ........ .5z.....
0030  00 02 00 00 00 00 00 00  05 5f 69 70 70 73 04 5f   ........ ._ipps._
0040  74 63 70 05 6c 6f 63 61  6c 00 00 0c 00 01 04 5f   tcp.loca l......_
0050  69 70 70 c0 12 00 0c 00  01                        ipp..... .
```

any: <live capture in progress>   Packets: 15509 · Displayed: 15509 (100.0%)   Profile: Default

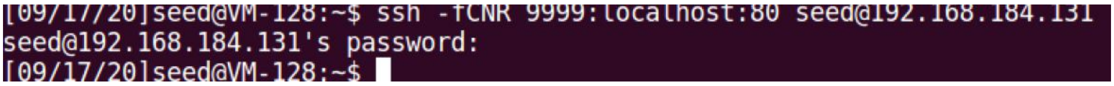
Task4：

配置规则，阻止由外而内的 SSH 和 HTTP 访问



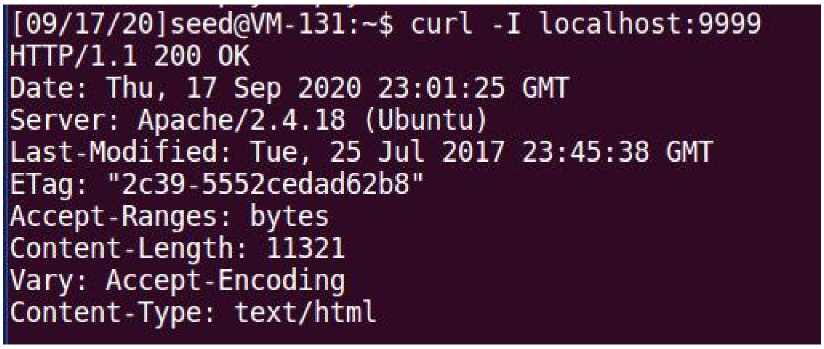
```
09/17/20]seed@VM-128:~$ sudo ufw reject in 22
ules updated
ules updated (v6)
09/17/20]seed@VM-128:~$ sudo ufw reject in 80
ules updated
ules updated (v6)
09/17/20]seed@VM-128:~$ sudo ufw enable
irewall is active and enabled on system startup
09/17/20]seed@VM-128:~$ sudo ufw status numbered
tatus: active

     To                         Action      From
     --                         ------      ----
  1] 22                         REJECT IN   Anywhere
  2] 80                         REJECT IN   Anywhere
  3] 22 (v6)                    REJECT IN   Anywhere (v6)
  4] 80 (v6)                    REJECT IN   Anywhere (v6)
```

设置逆向代理



```
[09/17/20]seed@VM-128:~$ ssh -fCNR 9999:localhost:80 seed@192.168.184.131
seed@192.168.184.131's password:
[09/17/20]seed@VM-128:~$ 
```

通过 SSH 隧道收到了来自 A 的 HTTP 应答



```
[09/17/20]seed@VM-131:~$ curl -I localhost:9999
HTTP/1.1 200 OK
Date: Thu, 17 Sep 2020 23:01:25 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Tue, 25 Jul 2017 23:45:38 GMT
ETag: "2c39-5552cedad62b8"
Accept-Ranges: bytes
Content-Length: 11321
Vary: Accept-Encoding
Content-Type: text/html
```