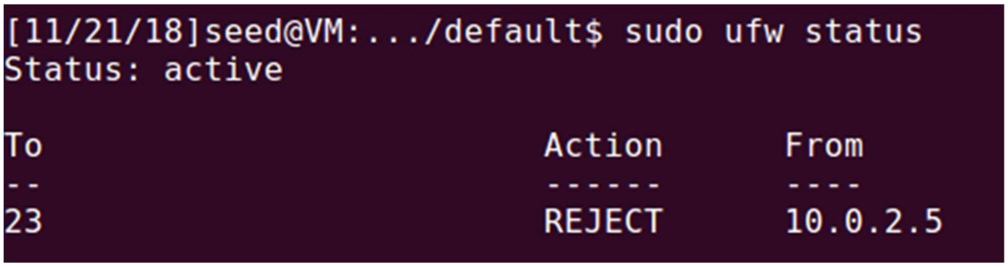
Linux Firewall Exploration Lab

(说明：A 机:10.0.2.4 B 机:10.0.2.5)

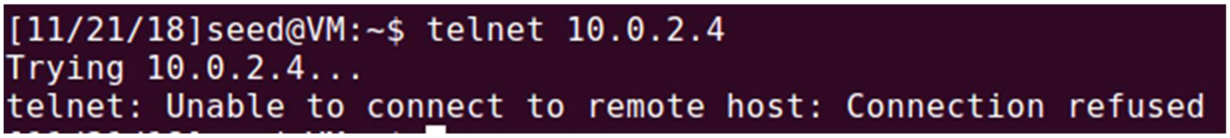
Task1: Using Firewall

Prevent B from doing telnet to Machine A.

命令：sudo ufw reject in from 10.0.2.5 to any port 23



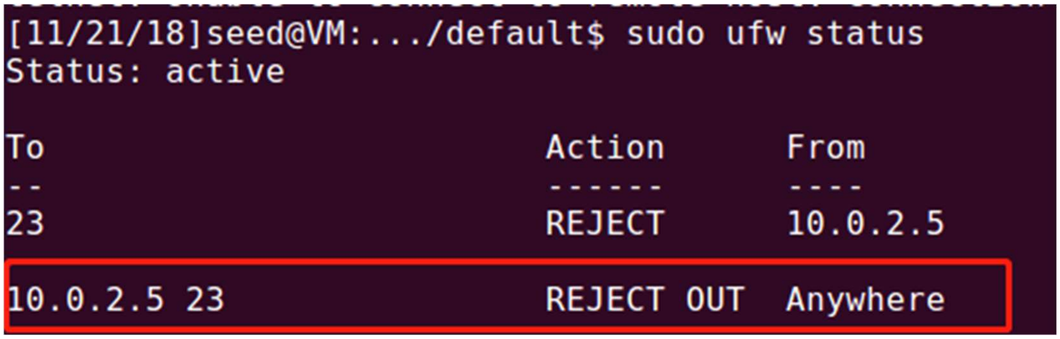
```
[11/21/18]seed@VM:.../default$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         REJECT      10.0.2.5
```



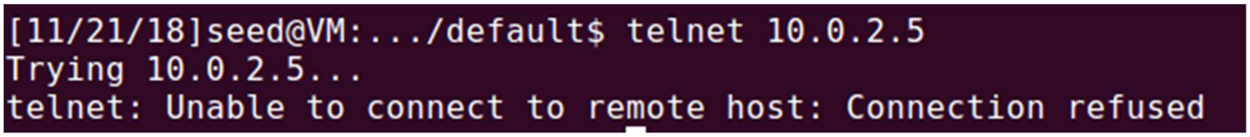
```
[11/21/18]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
telnet: Unable to connect to remote host: Connection refused
```

Prevent A from doing telnet to Machine B.

命令：sudo ufw reject out to 10.0.2.5 port 23



```
[11/21/18]seed@VM:.../default$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         REJECT      10.0.2.5

10.0.2.5 23                REJECT OUT  Anywhere
```

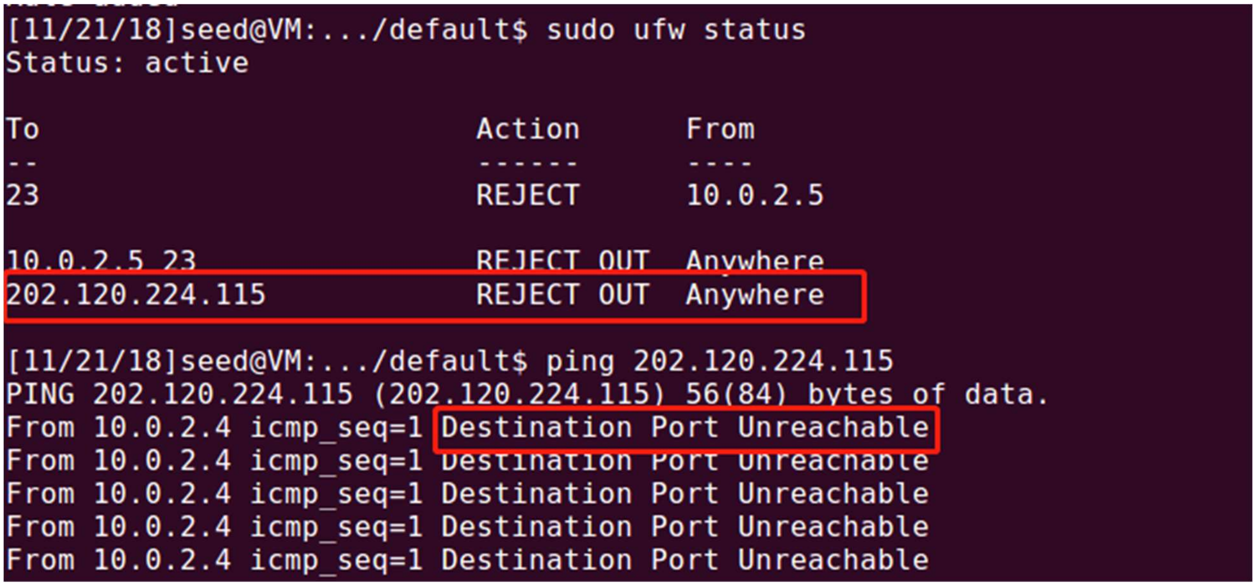


```
[11/21/18]seed@VM:.../default$ telnet 10.0.2.5
Trying 10.0.2.5...
telnet: Unable to connect to remote host: Connection refused
```

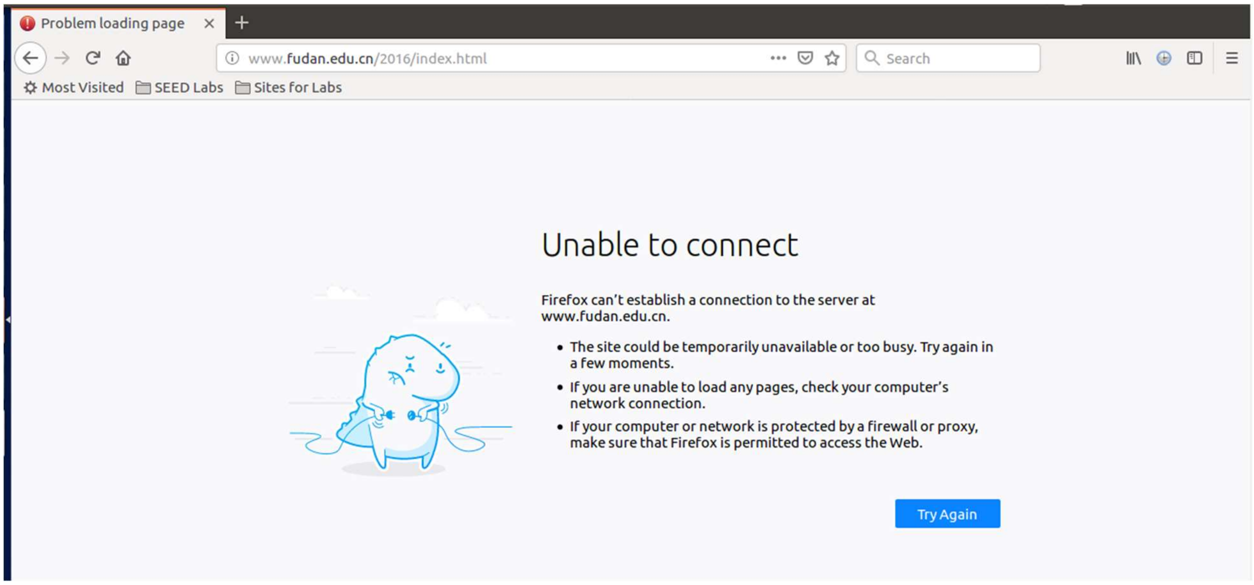
Prevent A from visiting an external web site. You can choose any web site that you like to block, but keep in mind, some web servers have multiple IP addresses.

命令:sudo ufw reject out to 202.120.224.115

选择的是 www.fudan.edu.cn 网站



```
[11/21/18]seed@VM:.../default$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         REJECT      10.0.2.5

10.0.2.5 23                REJECT OUT  Anywhere
202.120.224.115            REJECT OUT  Anywhere

[11/21/18]seed@VM:.../default$ ping 202.120.224.115
PING 202.120.224.115 (202.120.224.115) 56(84) bytes of data.
From 10.0.2.4 icmp_seq=1 Destination Port Unreachable
From 10.0.2.4 icmp_seq=1 Destination Port Unreachable
From 10.0.2.4 icmp_seq=1 Destination Port Unreachable
From 10.0.2.4 icmp_seq=1 Destination Port Unreachable
From 10.0.2.4 icmp_seq=1 Destination Port Unreachable
```



Unable to connect

Firefox can't establish a connection to the server at www.fudan.edu.cn.

- 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.

Task2: Implementing a Simple Firewall

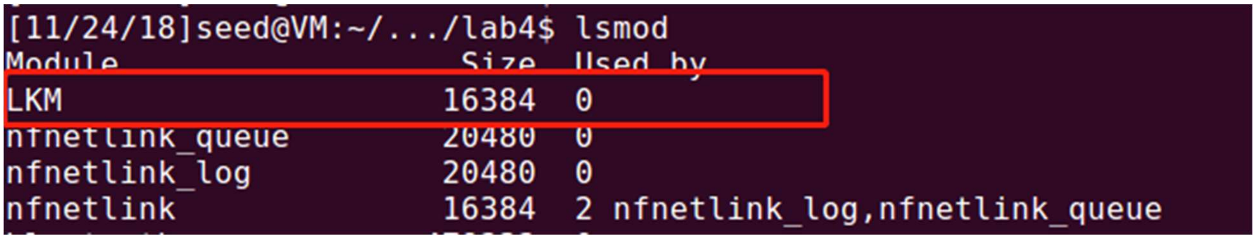
注：由于我升级内核的原因，所以有些代码与实验中给的并不一样。

其次，我发现在内部局域网之间，netfilter 并不能过滤 A 主机发出的包。

（注：实验代码：LKM.c 和 Makefile 内核版本：linux 4.15.0-39-generic）

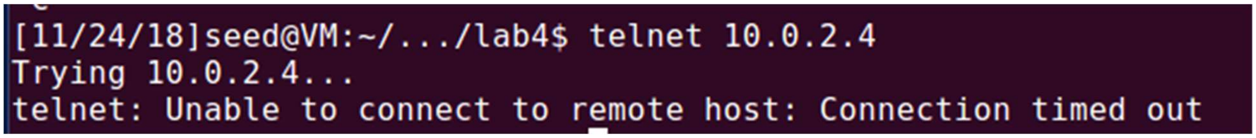
实验证据截图：

LKM module 的插入：



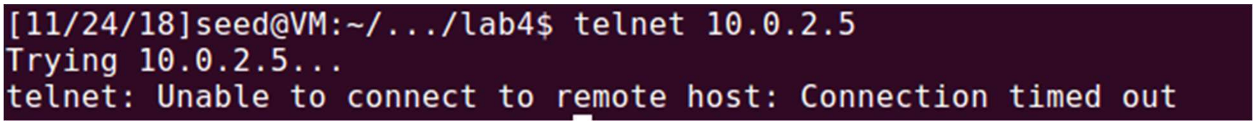
```
[11/24/18]seed@VM:~/.../lab4$ lsmod
Module                  Size  Used by
LKM                    16384  0
nfnetlink_queue        20480  0
nfnetlink_log          20480  0
nfnetlink              16384  2 nfnetlink_log,nfnetlink_queue
```

阻止 B 通过 telnet 连接 A：



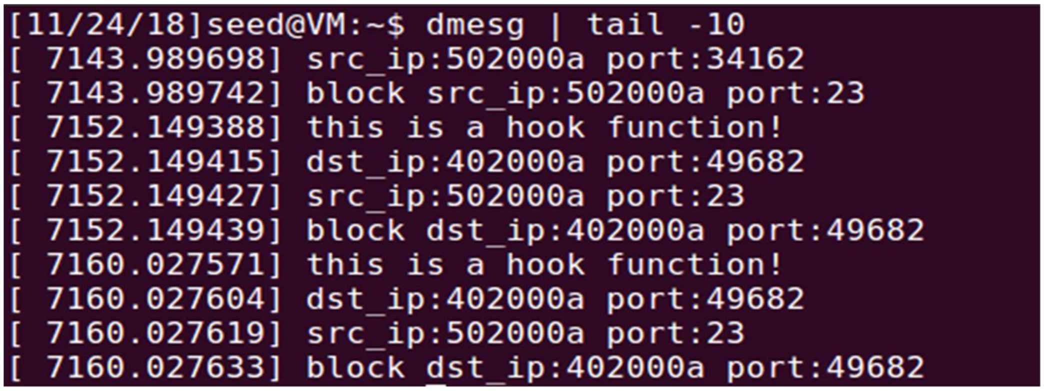
```
[11/24/18]seed@VM:~/.../lab4$ telnet 10.0.2.4
Trying 10.0.2.4...
telnet: Unable to connect to remote host: Connection timed out
```

阻止 A 通过 telnet 连接 B：

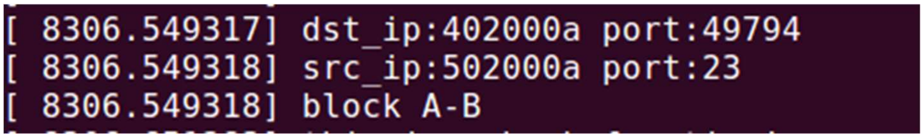


```
[11/24/18]seed@VM:~/.../lab4$ telnet 10.0.2.5
Trying 10.0.2.5...
telnet: Unable to connect to remote host: Connection timed out
```

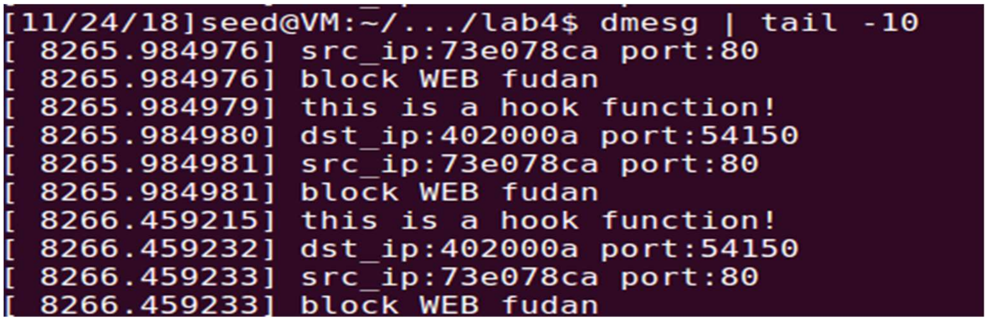
Printk 信息：



```
[11/24/18]seed@VM:~$ dmesg | tail -10
[ 7143.989698] src_ip:502000a port:34162
[ 7143.989742] block src_ip:502000a port:23
[ 7152.149388] this is a hook function!
[ 7152.149415] dst_ip:402000a port:49682
[ 7152.149427] src_ip:502000a port:23
[ 7152.149439] block dst_ip:402000a port:49682
[ 7160.027571] this is a hook function!
[ 7160.027604] dst_ip:402000a port:49682
[ 7160.027619] src_ip:502000a port:23
[ 7160.027633] block dst_ip:402000a port:49682
```



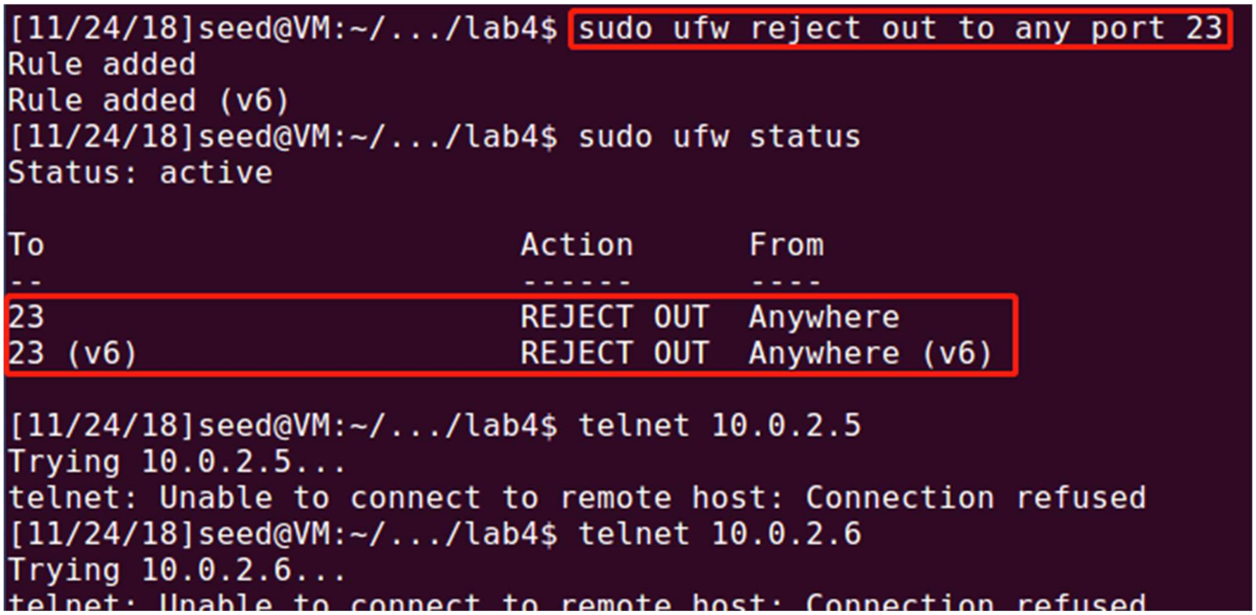
```
[ 8306.549317] dst_ip:402000a port:49794
[ 8306.549318] src_ip:502000a port:23
[ 8306.549318] block A-B
```



```
[11/24/18]seed@VM:~/.../lab4$ dmesg | tail -10
[ 8265.984976] src_ip:73e078ca port:80
[ 8265.984976] block WEB fudan
[ 8265.984979] this is a hook function!
[ 8265.984980] dst_ip:402000a port:54150
[ 8265.984981] src_ip:73e078ca port:80
[ 8265.984981] block WEB fudan
[ 8266.459215] this is a hook function!
[ 8266.459232] dst_ip:402000a port:54150
[ 8266.459233] src_ip:73e078ca port:80
[ 8266.459233] block WEB fudan
```

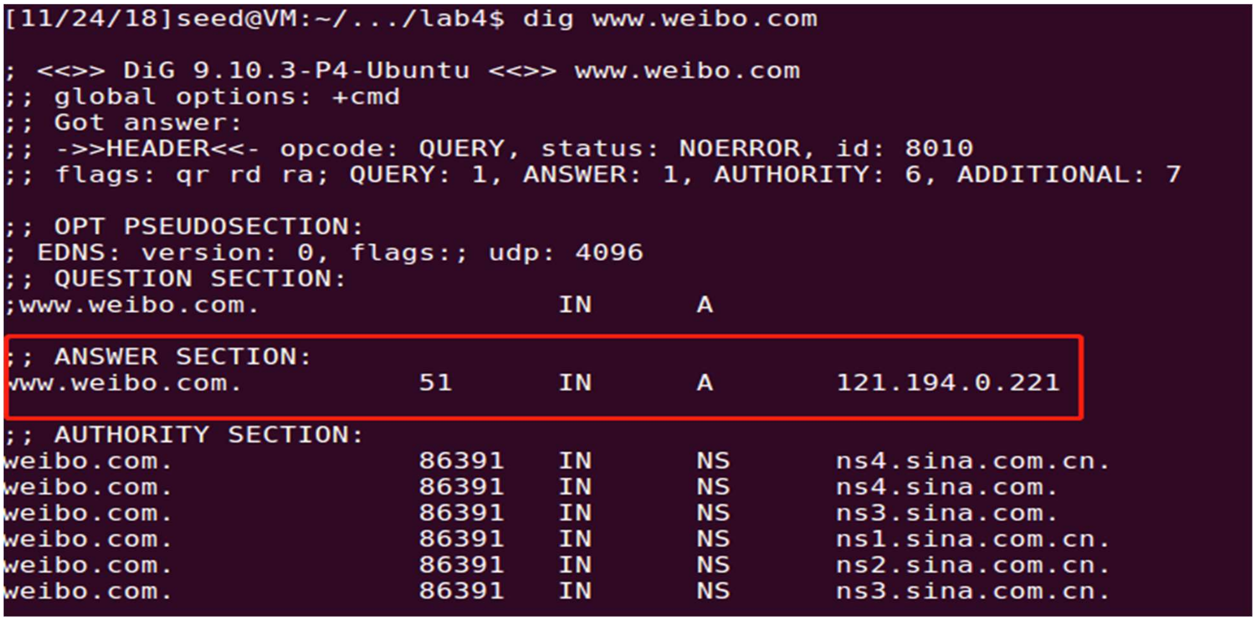
Task3: Evading Egress Filtering

为了阻断所有的 telnet，我丢弃了所有的 23 端口的输出包。

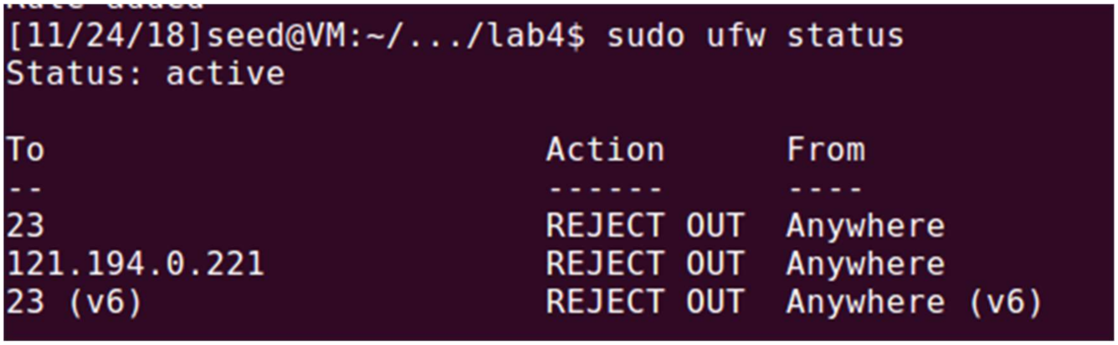


```
[11/24/18]seed@VM:~/.../lab4$ sudo ufw reject out to any port 23
Rule added
Rule added (v6)
[11/24/18]seed@VM:~/.../lab4$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         REJECT OUT  Anywhere
23 (v6)                    REJECT OUT  Anywhere (v6)

[11/24/18]seed@VM:~/.../lab4$ telnet 10.0.2.5
Trying 10.0.2.5...
telnet: Unable to connect to remote host: Connection refused
[11/24/18]seed@VM:~/.../lab4$ telnet 10.0.2.6
Trying 10.0.2.6...
telnet: Unable to connect to remote host: Connection refused
```

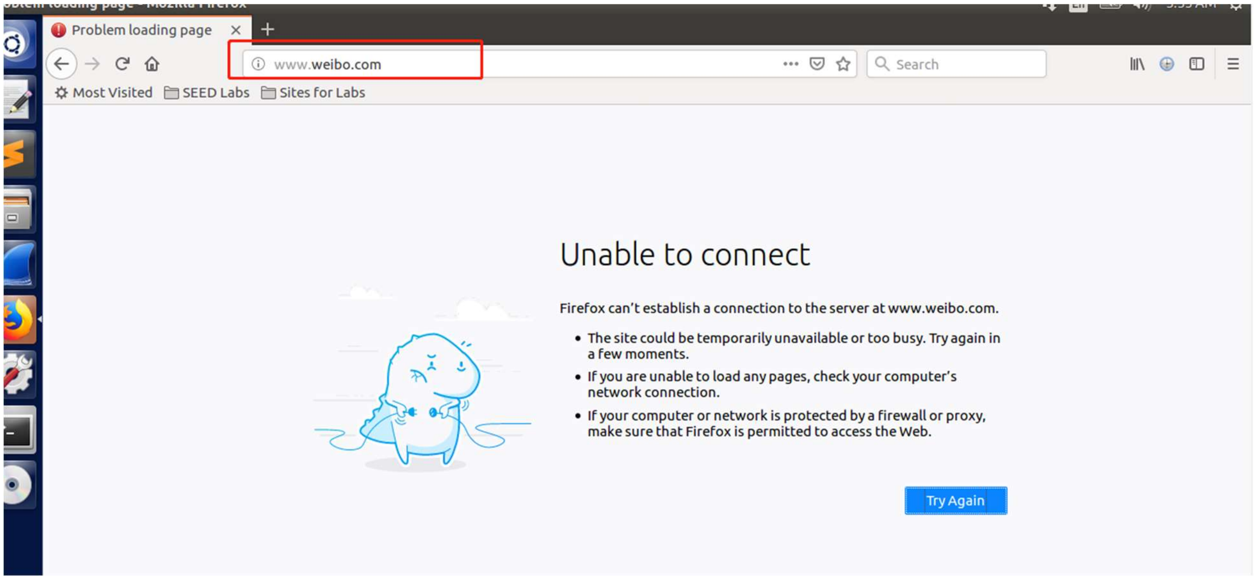
由于 facebook 不能访问，我将其改为 weibo



```
[11/24/18]seed@VM:~/.../lab4$ dig www.weibo.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.weibo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8010
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.weibo.com.                 IN      A

;; ANSWER SECTION:
www.weibo.com.          51      IN      A       121.194.0.221

;; AUTHORITY SECTION:
weibo.com.              86391   IN      NS      ns4.sina.com.cn.
weibo.com.              86391   IN      NS      ns4.sina.com.
weibo.com.              86391   IN      NS      ns3.sina.com.
weibo.com.              86391   IN      NS      ns1.sina.com.cn.
weibo.com.              86391   IN      NS      ns2.sina.com.cn.
weibo.com.              86391   IN      NS      ns3.sina.com.cn.
```



```
[11/24/18]seed@VM:~/.../lab4$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         REJECT OUT  Anywhere
121.194.0.221              REJECT OUT  Anywhere
23 (v6)                    REJECT OUT  Anywhere (v6)
```



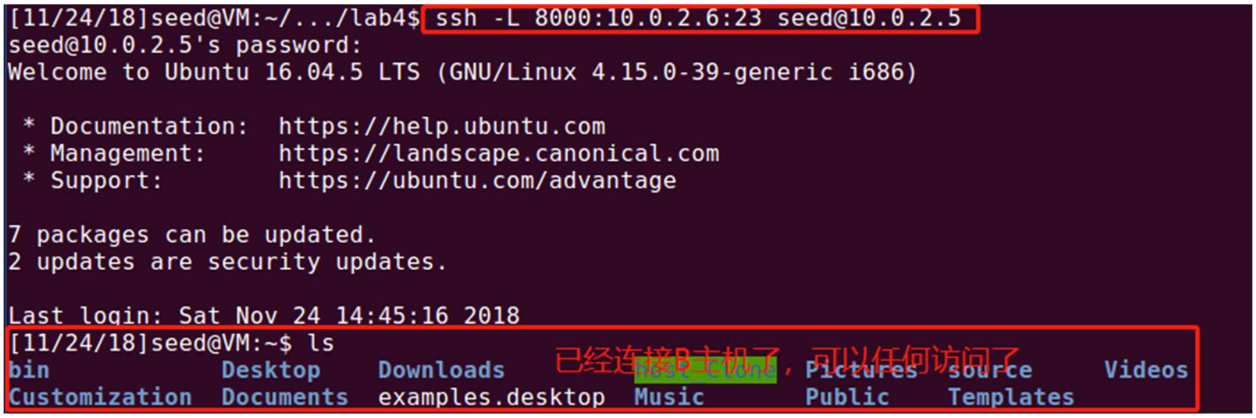
Unable to connect

Firefox can't establish a connection to the server at www.weibo.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.

Task 3.a: Telnet to Machine B through the firewall

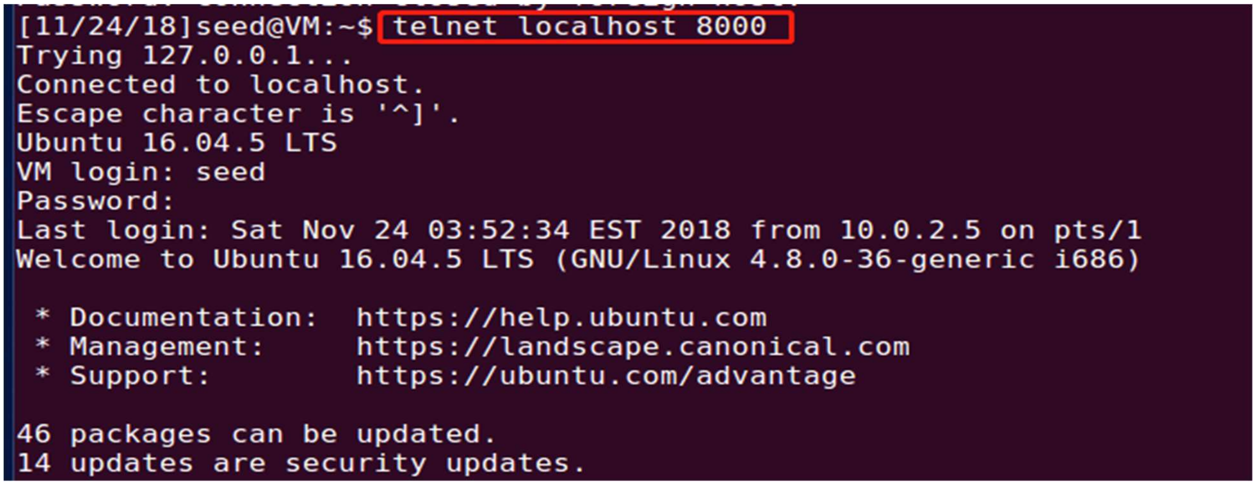
主机 C:10.0.2.6



```
[11/24/18]seed@VM:~/.../lab4$ ssh -L 8000:10.0.2.6:23 seed@10.0.2.5
seed@10.0.2.5's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-39-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

7 packages can be updated.
2 updates are security updates.

Last login: Sat Nov 24 14:45:16 2018
[11/24/18]seed@VM:~$ ls
bin            Desktop    Downloads         host_Clone  Pictures  source     Videos
Customization  Documents  examples.desktop  Music       Public    Templates
```

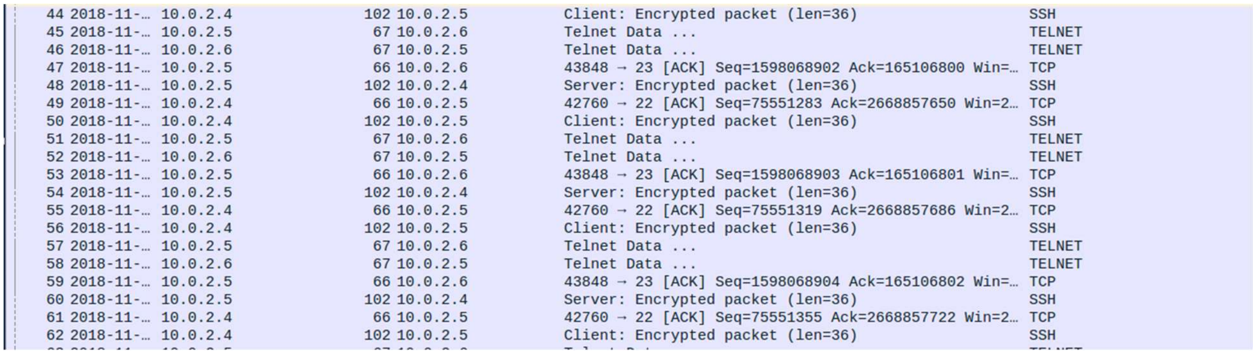
已经连接B主机了，可以任何访问了

重新打开一个 cmd 在主机 A



```
[11/24/18]seed@VM:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04.5 LTS
VM login: seed
Password:
Last login: Sat Nov 24 03:52:34 EST 2018 from 10.0.2.5 on pts/1
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

46 packages can be updated.
14 updates are security updates.
```

通过观察 wireshark 抓的流量包：



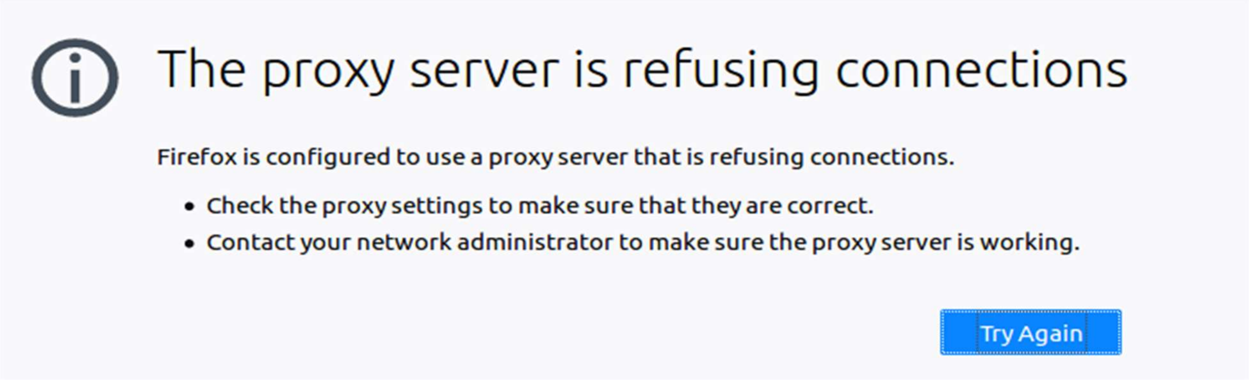
```
44 2018-11-… 10.0.2.4    102 10.0.2.5    Client: Encrypted packet (len=36)                       SSH
45 2018-11-… 10.0.2.5     67 10.0.2.6    Telnet Data ...                                         TELNET
46 2018-11-… 10.0.2.6     67 10.0.2.5    Telnet Data ...                                         TELNET
47 2018-11-… 10.0.2.5     66 10.0.2.6    43848 → 23 [ACK] Seq=1598068902 Ack=165106800 Win=…  TCP
48 2018-11-… 10.0.2.5    102 10.0.2.4    Server: Encrypted packet (len=36)                       SSH
49 2018-11-… 10.0.2.4     66 10.0.2.5    42760 → 22 [ACK] Seq=75551283 Ack=2668857650 Win=2…  TCP
50 2018-11-… 10.0.2.4    102 10.0.2.5    Client: Encrypted packet (len=36)                       SSH
51 2018-11-… 10.0.2.5     67 10.0.2.6    Telnet Data ...                                         TELNET
52 2018-11-… 10.0.2.6     67 10.0.2.5    Telnet Data ...                                         TELNET
53 2018-11-… 10.0.2.5     66 10.0.2.6    43848 → 23 [ACK] Seq=1598068903 Ack=165106801 Win=…  TCP
54 2018-11-… 10.0.2.5    102 10.0.2.4    Server: Encrypted packet (len=36)                       SSH
55 2018-11-… 10.0.2.4     66 10.0.2.5    42760 → 22 [ACK] Seq=75551319 Ack=2668857686 Win=2…  TCP
56 2018-11-… 10.0.2.4    102 10.0.2.5    Client: Encrypted packet (len=36)                       SSH
57 2018-11-… 10.0.2.5     67 10.0.2.6    Telnet Data ...                                         TELNET
58 2018-11-… 10.0.2.6     67 10.0.2.5    Telnet Data ...                                         TELNET
59 2018-11-… 10.0.2.5     66 10.0.2.6    43848 → 23 [ACK] Seq=1598068904 Ack=165106802 Win=…  TCP
60 2018-11-… 10.0.2.5    102 10.0.2.4    Server: Encrypted packet (len=36)                       SSH
61 2018-11-… 10.0.2.4     66 10.0.2.5    42760 → 22 [ACK] Seq=75551355 Ack=2668857722 Win=2…  TCP
62 2018-11-… 10.0.2.4    102 10.0.2.5    Client: Encrypted packet (len=36)                       SSH
```

首先，主机 A 使用 ssh 连接到主机 B，给 ssh 发送连接 C 的 telnet 指令，主机 B 连接主机 C 并将控制权在主机 A 里面，然后主机 A 就可以通过间接的 telnet 访问主机 C 了。原因：因为 ufw 设置的是防火墙只检测包头部信息，而且 ssh 是加密传输，他无法检测到具体的命令。

Task 3.b: Connect to Facebook using SSH Tunnel.

1、可以看到正常的 weibo 页面。

2、当关闭 SSH 通道后，无法看到 weibo 页面。显示代理服务拒绝连接。因为我们的代理服务已经关闭了。所以会有如下显示：



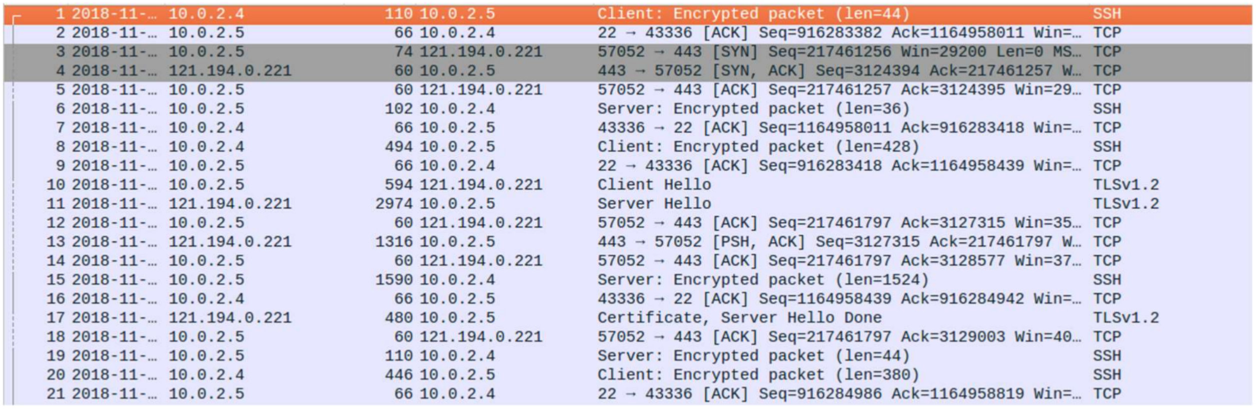
The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

3、当建立 SSH 后，又可以继续看到正常的 weibo 页面。

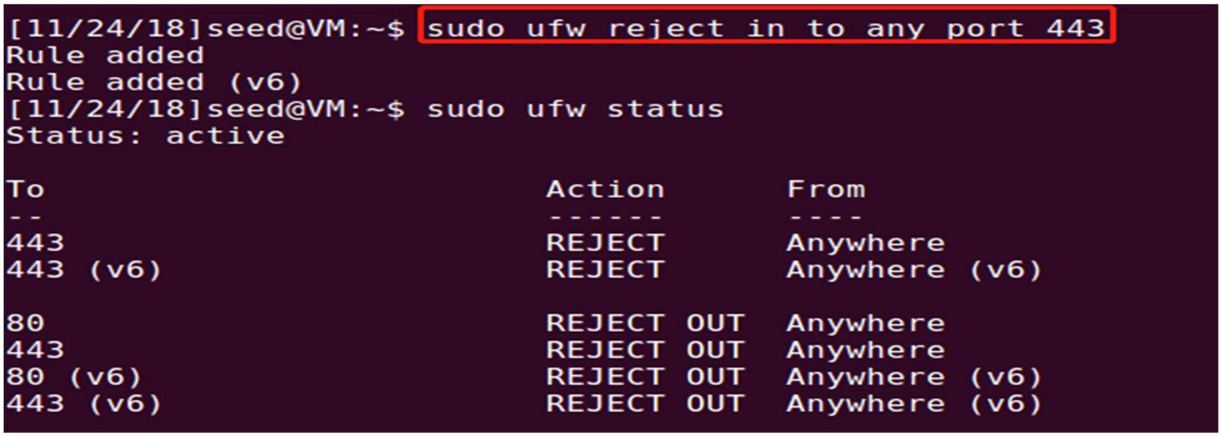
4、观察数据流，可以发现跟上面 telnet 类似，主机 B 起一个中间桥梁的作用，可以很好地避开防火墙的检测。墙内的主机 A 跟墙外的代理服务器主机 B，建立好 SSH 连接，并设定动态绑定。而此时墙内主机 A 上的 SSH 会监听本地的一个端口 9000，当 firefox 要对 weibo 发送数据包时，www.weibo.com:80 的请求告知 9000 端口的 SSH，SSH 将此请求通过 SSH 加密连接发送到墙外服务器主机 B 的 SSH 上，由于建立的动态绑定，服务器主机 B 会将 www.weibo.com:80 的请求发送给 www.weibo.com 上的 80 端口，并在收到回复后，通过原路返回给客户机主机 A 的 SSH，客户机 A 的 SSH 返回给应用程序 firefox。



```
 1 2018-11-… 10.0.2.4          110 10.0.2.5        Client: Encrypted packet (len=44)                       SSH
 2 2018-11-… 10.0.2.5           66 10.0.2.4        22 → 43336 [ACK] Seq=916283382 Ack=1164958011 Win=…    TCP
 3 2018-11-… 10.0.2.5           74 121.194.0.221   57052 → 443 [SYN] Seq=217461256 Win=29200 Len=0 MS…    TCP
 4 2018-11-… 121.194.0.221      60 10.0.2.5        443 → 57052 [SYN, ACK] Seq=3124394 Ack=217461257 W…    TCP
 5 2018-11-… 10.0.2.5           60 121.194.0.221   57052 → 443 [ACK] Seq=217461257 Ack=3124395 Win=29…    TCP
 6 2018-11-… 10.0.2.5          102 10.0.2.4        Server: Encrypted packet (len=36)                       SSH
 7 2018-11-… 10.0.2.4           66 10.0.2.5        43336 → 22 [ACK] Seq=1164958011 Ack=916283418 Win=…    TCP
 8 2018-11-… 10.0.2.4          494 10.0.2.5        Client: Encrypted packet (len=428)                      SSH
 9 2018-11-… 10.0.2.5           66 10.0.2.4        22 → 43336 [ACK] Seq=916283418 Ack=1164958439 Win=…    TCP
10 2018-11-… 10.0.2.5          594 121.194.0.221   Client Hello                                            TLSv1.2
11 2018-11-… 121.194.0.221    2974 10.0.2.5        Server Hello                                            TLSv1.2
12 2018-11-… 10.0.2.5           60 121.194.0.221   57052 → 443 [ACK] Seq=217461797 Ack=3127315 Win=35…    TCP
13 2018-11-… 121.194.0.221    1316 10.0.2.5        443 → 57052 [PSH, ACK] Seq=3127315 Ack=217461797 W…    TCP
14 2018-11-… 10.0.2.5           60 121.194.0.221   57052 → 443 [ACK] Seq=217461797 Ack=3128577 Win=37…    TCP
15 2018-11-… 10.0.2.5         1590 10.0.2.4        Server: Encrypted packet (len=1524)                     SSH
16 2018-11-… 10.0.2.4           66 10.0.2.5        43336 → 22 [ACK] Seq=1164958439 Ack=916284942 Win=…    TCP
17 2018-11-… 121.194.0.221     480 10.0.2.5        Certificate, Server Hello Done                          TLSv1.2
18 2018-11-… 10.0.2.5           60 121.194.0.221   57052 → 443 [ACK] Seq=217461797 Ack=3129003 Win=40…    TCP
19 2018-11-… 10.0.2.5          110 10.0.2.4        Server: Encrypted packet (len=44)                       SSH
20 2018-11-… 10.0.2.4          446 10.0.2.5        Client: Encrypted packet (len=380)                      SSH
21 2018-11-… 10.0.2.5           66 10.0.2.4        22 → 43336 [ACK] Seq=916284986 Ack=1164958819 Win=…    TCP
```

Task4: Evading Ingress Filtering

首先为了简单实验过程，不用构建一个网络服务器，所以首先我将主机 B 的 80 和 443 端口（因为现在多数网络连接是 SSL）的包全部丢弃掉，通过主机 A 访问网页。

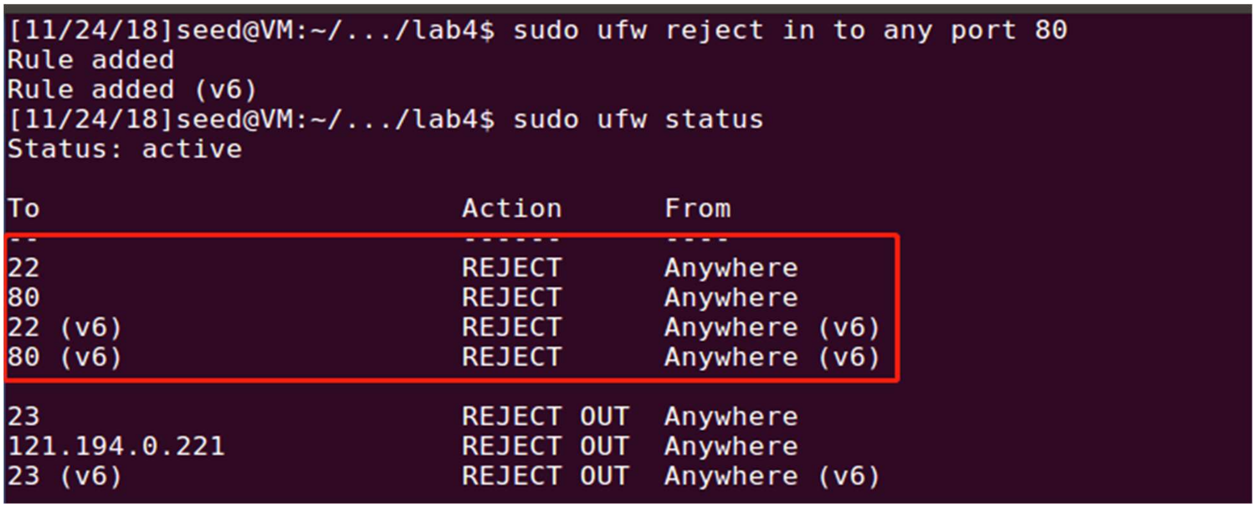


```
[11/24/18]seed@VM:~$ sudo ufw reject in to any port 443
Rule added
Rule added (v6)
[11/24/18]seed@VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
443                        REJECT      Anywhere
443 (v6)                   REJECT      Anywhere (v6)

80                         REJECT OUT  Anywhere
443                        REJECT OUT  Anywhere
80 (v6)                    REJECT OUT  Anywhere (v6)
443 (v6)                   REJECT OUT  Anywhere (v6)
```

这相当于主机 A 的 web 服务器外部网络的主机 B 不能直接访问。

开始实验过程：

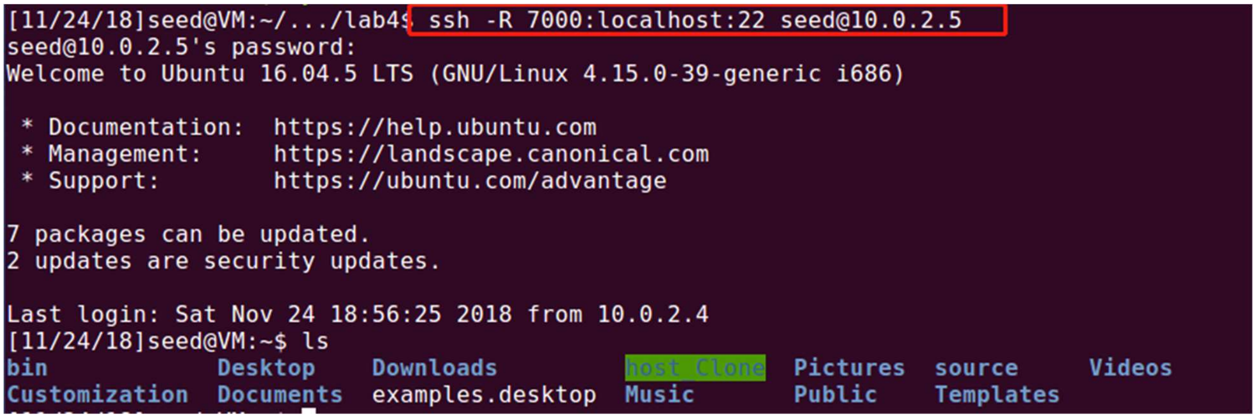
首先将主机 A 的外部链接 SSH 通道关闭：



```
[11/24/18]seed@VM:~/.../lab4$ sudo ufw reject in to any port 80
Rule added
Rule added (v6)
[11/24/18]seed@VM:~/.../lab4$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         REJECT      Anywhere
80                         REJECT      Anywhere
22 (v6)                    REJECT      Anywhere (v6)
80 (v6)                    REJECT      Anywhere (v6)

23                         REJECT OUT  Anywhere
121.194.0.221              REJECT OUT  Anywhere
23 (v6)                    REJECT OUT  Anywhere (v6)
```

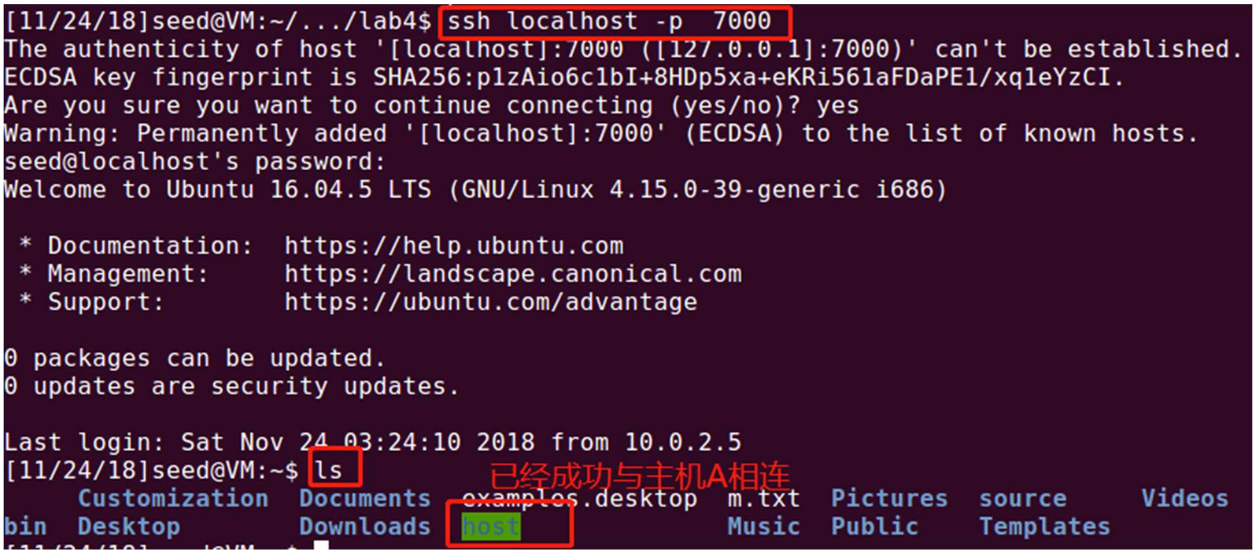
这样外部无法通过 SSH 连接主机 A。

接着在主机 A 上设置 SSH 的反射通道。



```
[11/24/18]seed@VM:~/.../lab4$ ssh -R 7000:localhost:22 seed@10.0.2.5
seed@10.0.2.5's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-39-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

7 packages can be updated.
2 updates are security updates.

Last login: Sat Nov 24 18:56:25 2018 from 10.0.2.4
[11/24/18]seed@VM:~$ ls
bin            Desktop    Downloads         host Clone  Pictures  source     Videos
Customization  Documents  examples.desktop  Music       Public    Templates
```

现在在主机 B 上测试 SSH 反向通道：

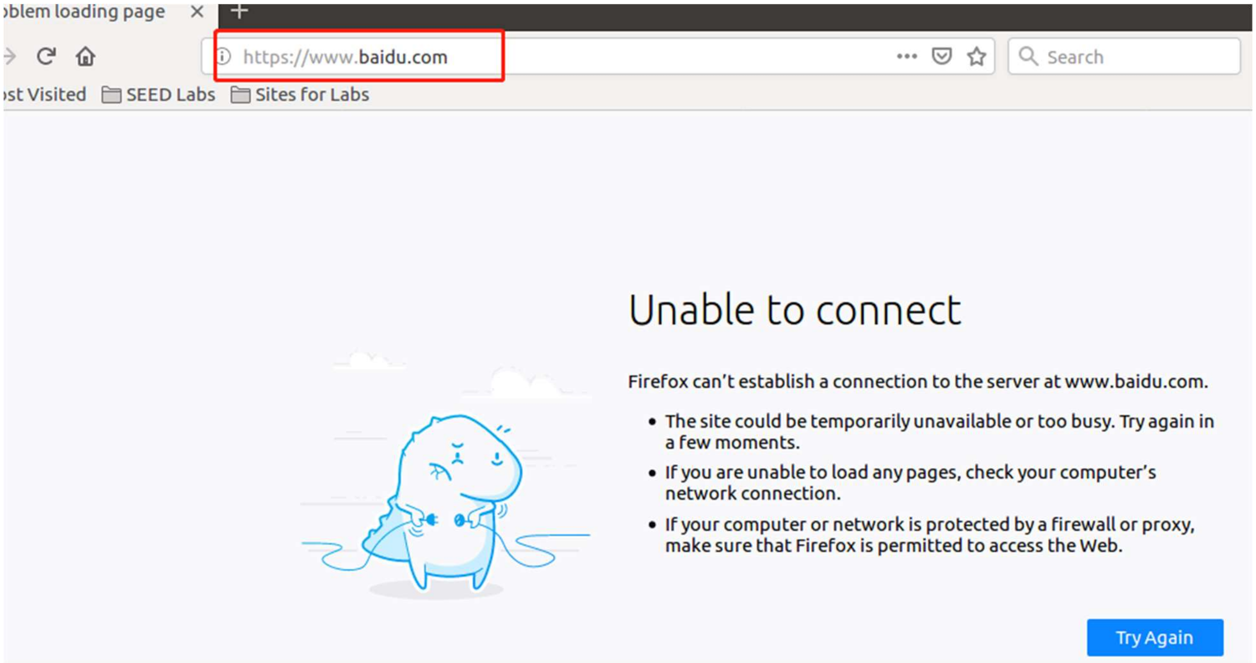


```
[11/24/18]seed@VM:~/.../lab4$ ssh localhost -p  7000
The authenticity of host '[localhost]:7000 ([127.0.0.1]:7000)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:7000' (ECDSA) to the list of known hosts.
seed@localhost's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-39-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Sat Nov 24 03:24:10 2018 from 10.0.2.5
[11/24/18]seed@VM:~$ ls
     Customization  Documents  examples.desktop  m.txt  Pictures  source     Videos
bin  Desktop        Downloads  host              Music  Public    Templates
```

已经成功与主机A相连

所以说明已经可以与主机 A 相连，可以做主机 A 可以做的任何工作，反射 SSH 建立成功。

为了能过运行 web 服务器，首先运行 firefox 打开 www.baidu.com 发现：

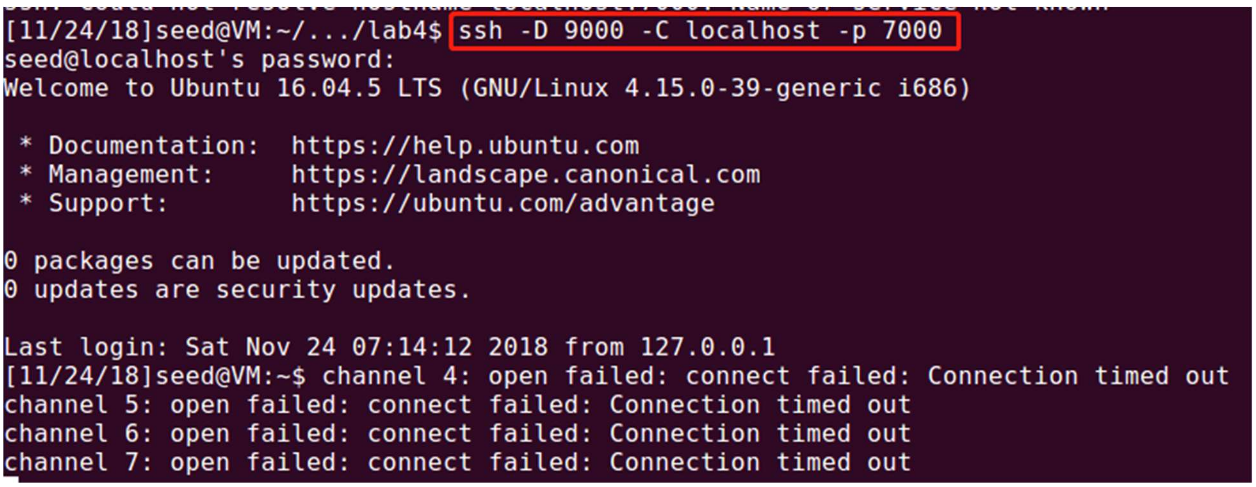


Unable to connect

Firefox can't establish a connection to the server at www.baidu.com.

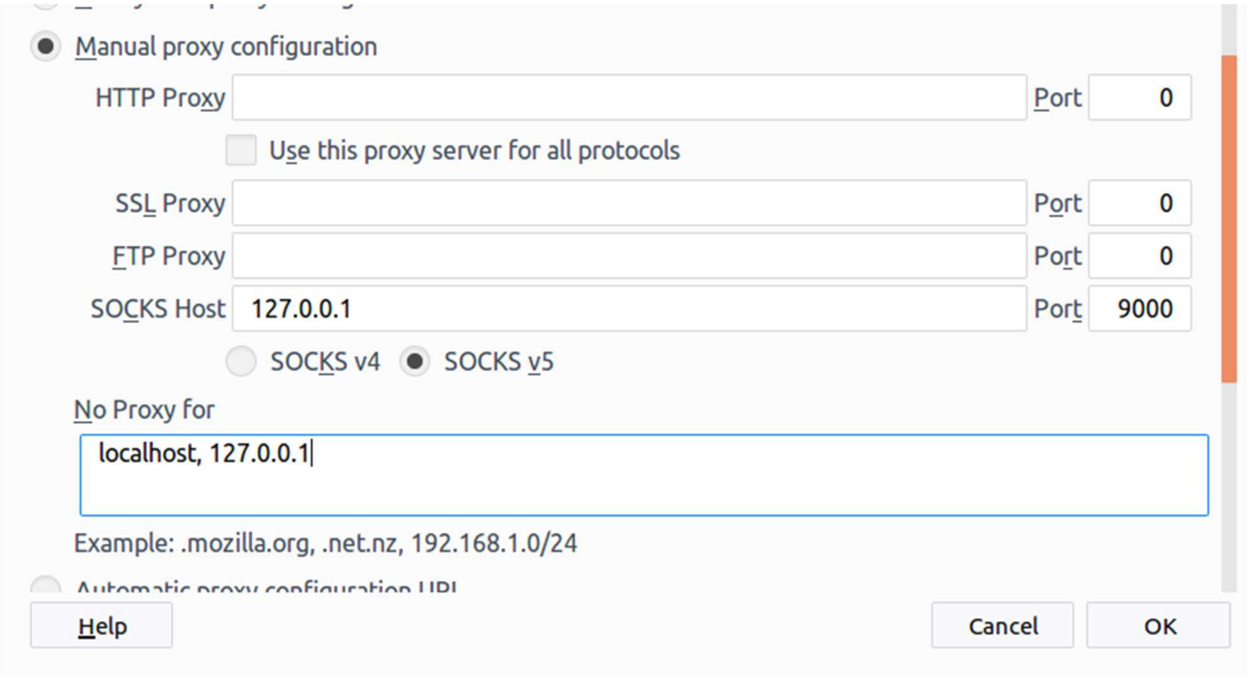
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

接着在主机 B 设置端口的动态绑定到 9000 端口：



```
ssh: Could not resolve hostname localhost:7000: Name or service not known
[11/24/18]seed@VM:~/.../lab4$ ssh -D 9000 -C localhost -p 7000
seed@localhost's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-39-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Sat Nov 24 07:14:12 2018 from 127.0.0.1
[11/24/18]seed@VM:~$ channel 4: open failed: connect failed: Connection timed out
channel 5: open failed: connect failed: Connection timed out
channel 6: open failed: connect failed: Connection timed out
channel 7: open failed: connect failed: Connection timed out
```

接着设置 firefox 的代理：



● Manual proxy configuration

HTTP Proxy: ____ Port: 0

□ Use this proxy server for all protocols

SSL Proxy: ____ Port: 0

FTP Proxy: ____ Port: 0

SOCKS Host: 127.0.0.1 Port: 9000

○ SOCKS v4 ● SOCKS v5

No Proxy for

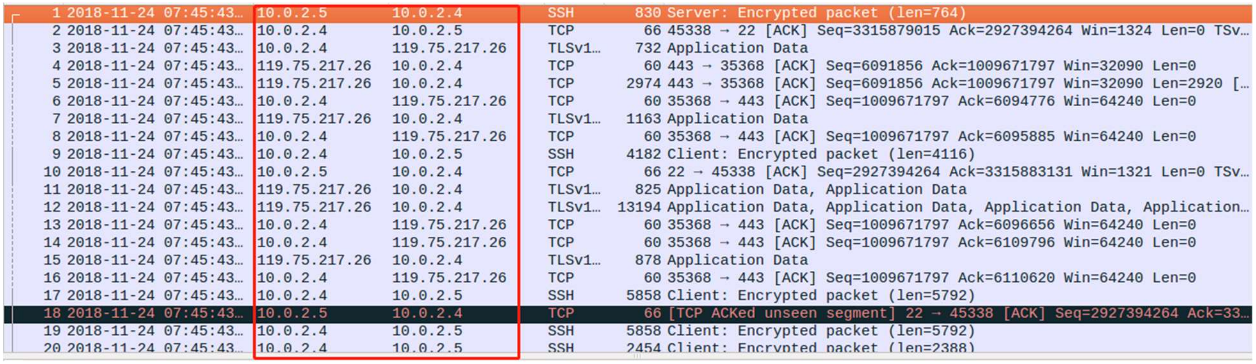
localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL

最后重新运行 firefox 打开 www.baidu.com 发现可以正常访问。

观察数据流，如同 task 3 b 工作一样：主机 A 起到一个桥梁作用。



```
 1 2018-11-24 07:45:43… 10.0.2.5       10.0.2.4       SSH       830 Server: Encrypted packet (len=764)
 2 2018-11-24 07:45:43… 10.0.2.4       10.0.2.5       TCP        66 45338 → 22 [ACK] Seq=3315879015 Ack=2927394264 Win=1324 Len=0 TSv…
 3 2018-11-24 07:45:43… 10.0.2.4       119.75.217.26  TLSv1…    732 Application Data
 4 2018-11-24 07:45:43… 119.75.217.26  10.0.2.4       TCP        60 443 → 35368 [ACK] Seq=6091856 Ack=1009671797 Win=32090 Len=0
 5 2018-11-24 07:45:43… 119.75.217.26  10.0.2.4       TCP      2974 443 → 35368 [ACK] Seq=6091856 Ack=1009671797 Win=32090 Len=2920 […
 6 2018-11-24 07:45:43… 10.0.2.4       119.75.217.26  TCP        60 35368 → 443 [ACK] Seq=1009671797 Ack=6094776 Win=64240 Len=0
 7 2018-11-24 07:45:43… 119.75.217.26  10.0.2.4       TLSv1…   1163 Application Data
 8 2018-11-24 07:45:43… 10.0.2.4       119.75.217.26  TCP        60 35368 → 443 [ACK] Seq=1009671797 Ack=6095885 Win=64240 Len=0
 9 2018-11-24 07:45:43… 10.0.2.4       10.0.2.5       SSH      4182 Client: Encrypted packet (len=4116)
10 2018-11-24 07:45:43… 10.0.2.5       10.0.2.4       TCP        66 22 → 45338 [ACK] Seq=2927394264 Ack=3315883131 Win=1321 Len=0 TSv…
11 2018-11-24 07:45:43… 119.75.217.26  10.0.2.4       TLSv1…    825 Application Data, Application Data
12 2018-11-24 07:45:43… 119.75.217.26  10.0.2.4       TLSv1…  13194 Application Data, Application Data, Application Data, Application…
13 2018-11-24 07:45:43… 10.0.2.4       119.75.217.26  TCP        60 35368 → 443 [ACK] Seq=1009671797 Ack=6096656 Win=64240 Len=0
14 2018-11-24 07:45:43… 10.0.2.4       119.75.217.26  TCP        60 35368 → 443 [ACK] Seq=1009671797 Ack=6109796 Win=64240 Len=0
15 2018-11-24 07:45:43… 119.75.217.26  10.0.2.4       TLSv1…    878 Application Data
16 2018-11-24 07:45:43… 10.0.2.4       119.75.217.26  TCP        60 35368 → 443 [ACK] Seq=1009671797 Ack=6110620 Win=64240 Len=0
17 2018-11-24 07:45:43… 10.0.2.4       10.0.2.5       SSH      5858 Client: Encrypted packet (len=5792)
18 2018-11-24 07:45:43… 10.0.2.5       10.0.2.4       TCP        66 [TCP ACKed unseen segment] 22 → 45338 [ACK] Seq=2927394264 Ack=33…
19 2018-11-24 07:45:43… 10.0.2.4       10.0.2.5       SSH      5858 Client: Encrypted packet (len=5792)
20 2018-11-24 07:45:43… 10.0.2.4       10.0.2.5       SSH      2454 Client: Encrypted packet (len=2388)
```

观察端口号，并没有使用主机 A(10.0.2.4)的 SSH 端口 22。（其中 119.75.217.26 为 www.baidu.com 的 IP）