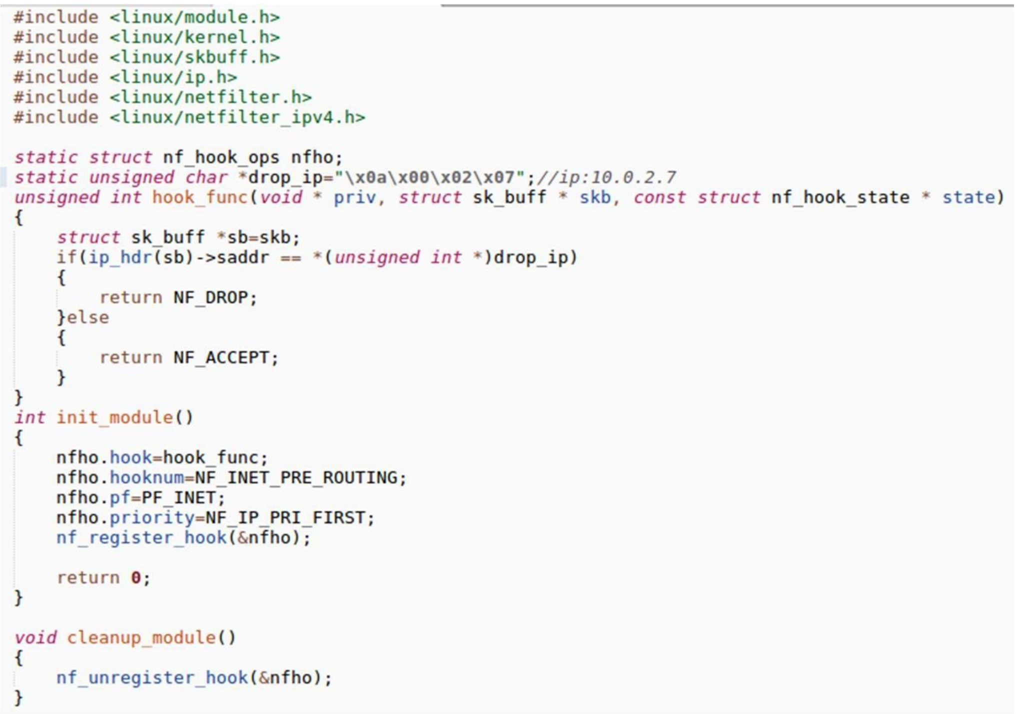
Firewall Exploration Lab

57118138 李嘉怡

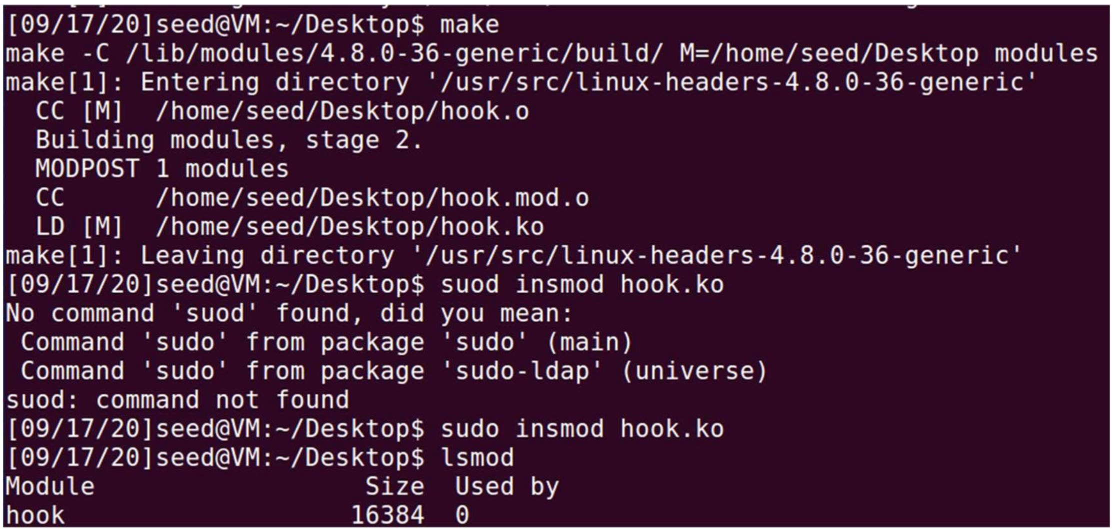
Task 1: Implementing a Simple Firewall

在主机 A 上，首先构造代码组织主机 B 的一切访问



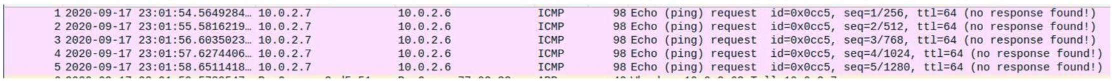
```
#include <linux/module.h>
#include <linux/kernel.h>
#include <linux/skbuff.h>
#include <linux/ip.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>

static struct nf_hook_ops nfho;
static unsigned char *drop_ip="\x0a\x00\x02\x07";//ip:10.0.2.7
unsigned int hook_func(void * priv, struct sk_buff * skb, const struct nf_hook_state * state)
{
    struct sk_buff *sb=skb;
    if(ip_hdr(sb)->saddr == *(unsigned int *)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;
}

void cleanup_module()
{
    nf_unregister_hook(&nfho);
}
```

可以看到使用 make 在内核中添加了一块新的 hook：



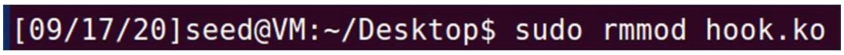
```
[09/17/20]seed@VM:~/Desktop$ make
make -C /lib/modules/4.8.0-36-generic/build/ M=/home/seed/Desktop modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  CC [M]  /home/seed/Desktop/hook.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/Desktop/hook.mod.o
  LD [M]  /home/seed/Desktop/hook.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[09/17/20]seed@VM:~/Desktop$ suod insmod hook.ko
No command 'suod' found, did you mean:
 Command 'sudo' from package 'sudo' (main)
 Command 'sudo' from package 'sudo-ldap' (universe)
suod: command not found
[09/17/20]seed@VM:~/Desktop$ sudo insmod hook.ko
[09/17/20]seed@VM:~/Desktop$ lsmod
Module                  Size  Used by
hook                   16384  0
```

这时主机 B 就无法访问到主机A 了。

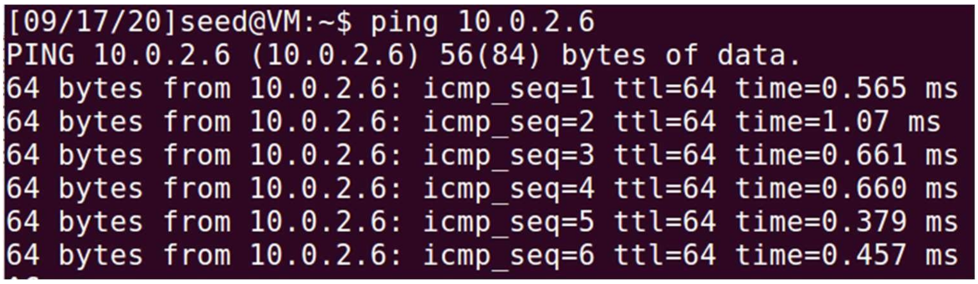


```
1 2020-09-17 23:01:54.5649284… 10.0.2.7    10.0.2.6    ICMP    98 Echo (ping) request  id=0x0cc5, seq=1/256, ttl=64 (no response found!)
2 2020-09-17 23:01:55.5816219… 10.0.2.7    10.0.2.6    ICMP    98 Echo (ping) request  id=0x0cc5, seq=2/512, ttl=64 (no response found!)
3 2020-09-17 23:01:56.6035023… 10.0.2.7    10.0.2.6    ICMP    98 Echo (ping) request  id=0x0cc5, seq=3/768, ttl=64 (no response found!)
4 2020-09-17 23:01:57.6274406… 10.0.2.7    10.0.2.6    ICMP    98 Echo (ping) request  id=0x0cc5, seq=4/1024, ttl=64 (no response found!)
5 2020-09-17 23:01:58.6511418… 10.0.2.7    10.0.2.6    ICMP    98 Echo (ping) request  id=0x0cc5, seq=5/1280, ttl=64 (no response found!)
```

移除掉 hook 后又可以正常访问主机A 了。



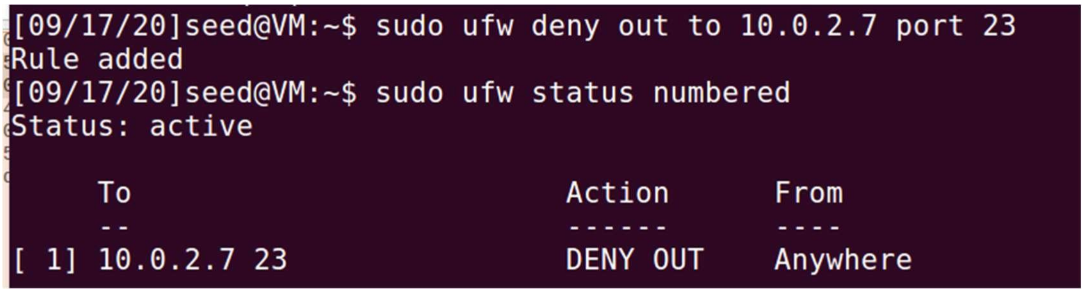
```
[09/17/20]seed@VM:~/Desktop$ sudo rmmod hook.ko
```



```
[09/17/20]seed@VM:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.565 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=1.07 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.661 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.660 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.379 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.457 ms
```

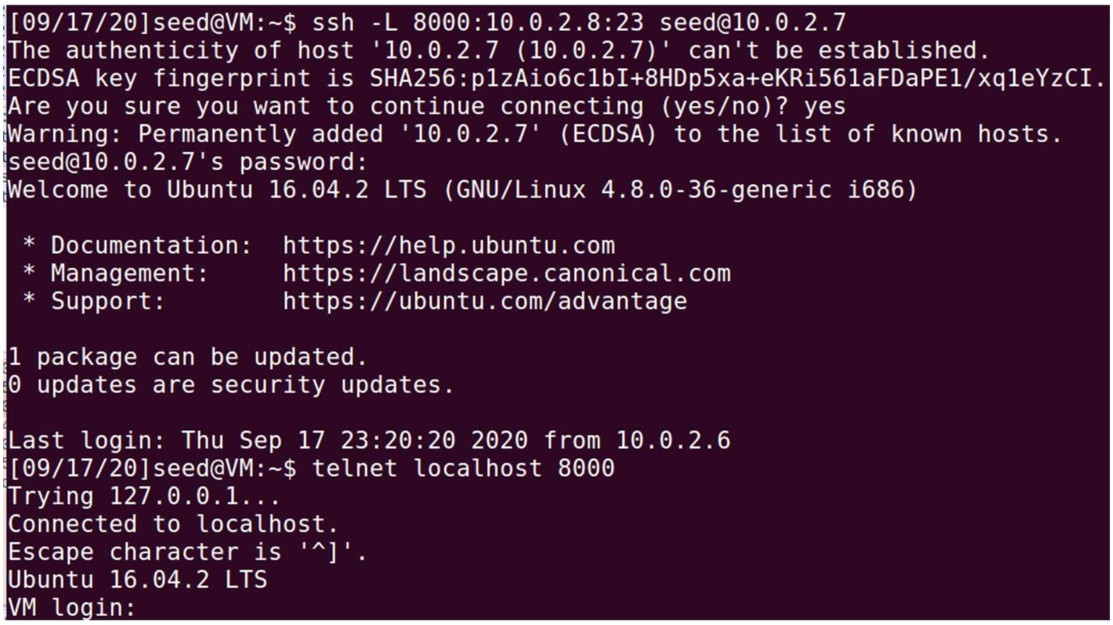
Task 2: Experimenting with Stateless Firewall Rules

建立防火墙阻止 telnet 访问主机 B:

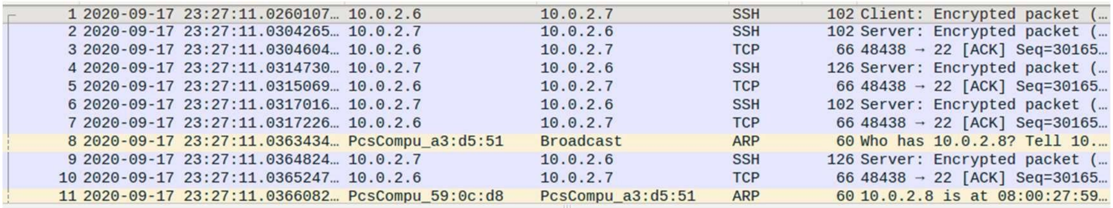


```
[09/17/20]seed@VM:~$ sudo ufw deny out to 10.0.2.7 port 23
Rule added
[09/17/20]seed@VM:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 10.0.2.7 23                DENY OUT    Anywhere
```

建立隧道:



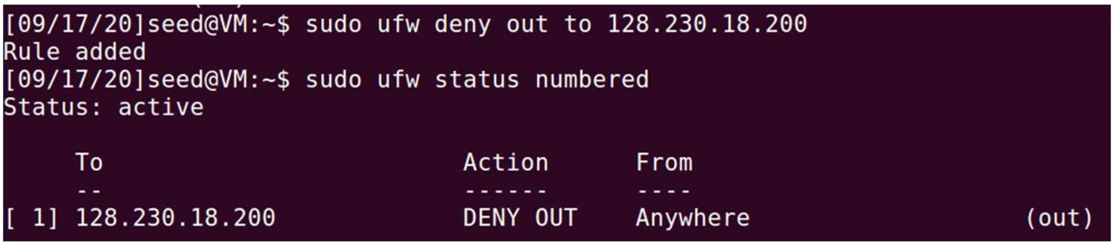
```
[09/17/20]seed@VM:~$ ssh -L 8000:10.0.2.8:23 seed@10.0.2.7
The authenticity of host '10.0.2.7 (10.0.2.7)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.7' (ECDSA) to the list of known hosts.
seed@10.0.2.7'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 23:20:20 2020 from 10.0.2.6
[09/17/20]seed@VM:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login:
```



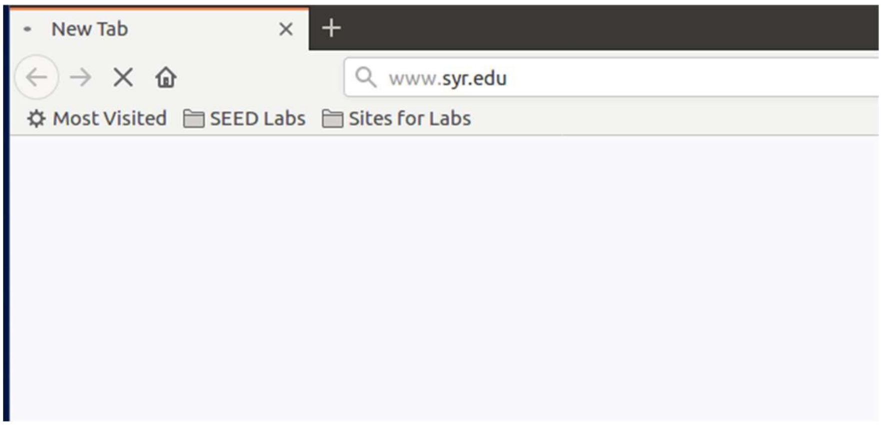
```
 1 2020-09-17 23:27:11.0260107… 10.0.2.6           10.0.2.7           SSH    102 Client: Encrypted packet (…
 2 2020-09-17 23:27:11.0304265… 10.0.2.7           10.0.2.6           SSH    102 Server: Encrypted packet (…
 3 2020-09-17 23:27:11.0304604… 10.0.2.6           10.0.2.7           TCP     66 48438 → 22 [ACK] Seq=30165…
 4 2020-09-17 23:27:11.0314730… 10.0.2.7           10.0.2.6           SSH    126 Server: Encrypted packet (…
 5 2020-09-17 23:27:11.0315069… 10.0.2.6           10.0.2.7           TCP     66 48438 → 22 [ACK] Seq=30165…
 6 2020-09-17 23:27:11.0317016… 10.0.2.7           10.0.2.6           SSH    102 Server: Encrypted packet (…
 7 2020-09-17 23:27:11.0317226… 10.0.2.6           10.0.2.7           TCP     66 48438 → 22 [ACK] Seq=30165…
 8 2020-09-17 23:27:11.0363434… PcsCompu_a3:d5:51  Broadcast          ARP     60 Who has 10.0.2.8? Tell 10.…
 9 2020-09-17 23:27:11.0364824… 10.0.2.7           10.0.2.6           SSH    126 Server: Encrypted packet (…
10 2020-09-17 23:27:11.0365247… 10.0.2.6           10.0.2.7           TCP     66 48438 → 22 [ACK] Seq=30165…
11 2020-09-17 23:27:11.0366082… PcsCompu_59:0c:d8  PcsCompu_a3:d5:51  ARP     60 10.0.2.8 is at 08:00:27:59…
```

可以看到穿越防火墙访问主机C 和 B 了。

建立防火墙规则禁止访问www.syr.edu：

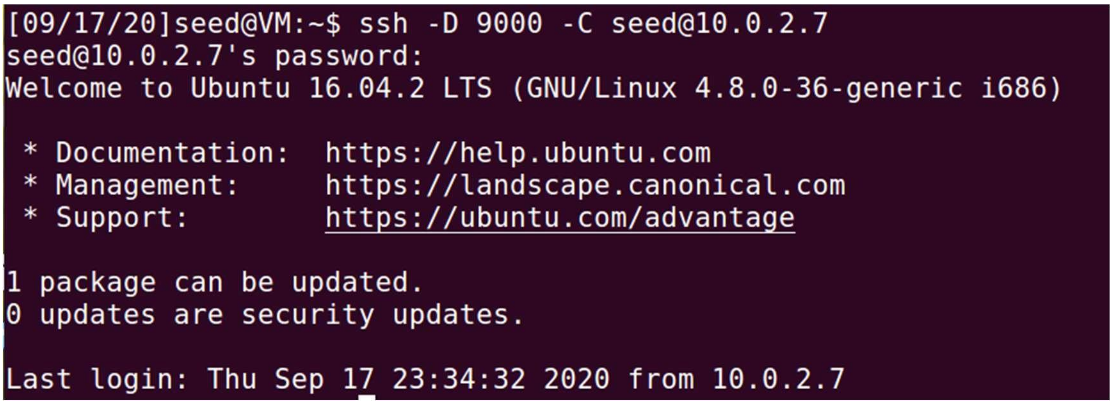


```
[09/17/20]seed@VM:~$ sudo ufw deny out to 128.230.18.200
Rule added
[09/17/20]seed@VM:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 128.230.18.200             DENY OUT    Anywhere                   (out)
```

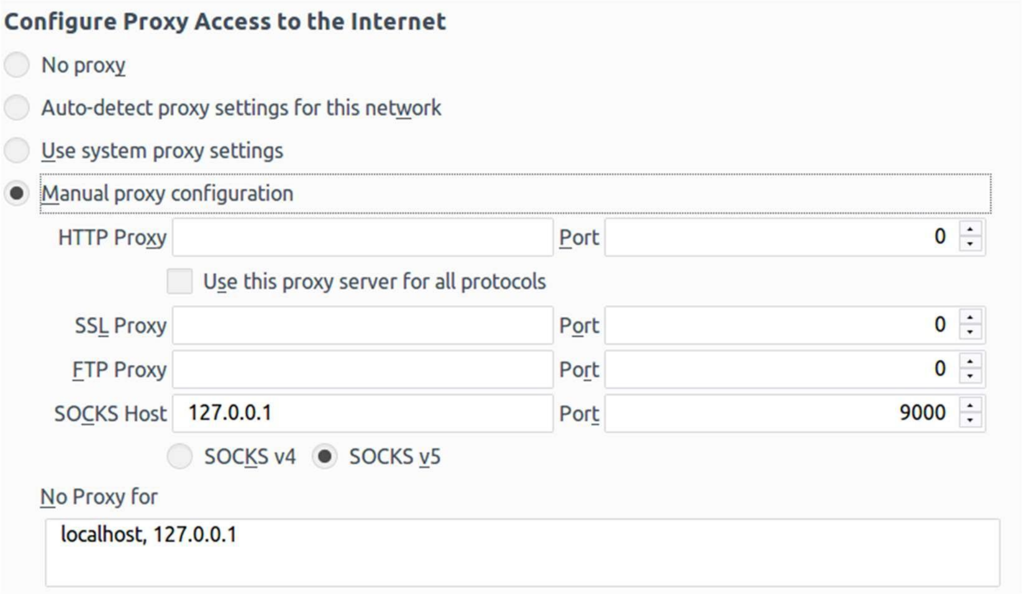


无法正常访问网站。

在配置完ssh 和网页代理后：



```
[09/17/20]seed@VM:~$ ssh -D 9000 -C seed@10.0.2.7
seed@10.0.2.7'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 23:34:32 2020 from 10.0.2.7
```



Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy Port 0

□ Use this proxy server for all protocols

SSL Proxy Port 0

FTP Proxy Port 0

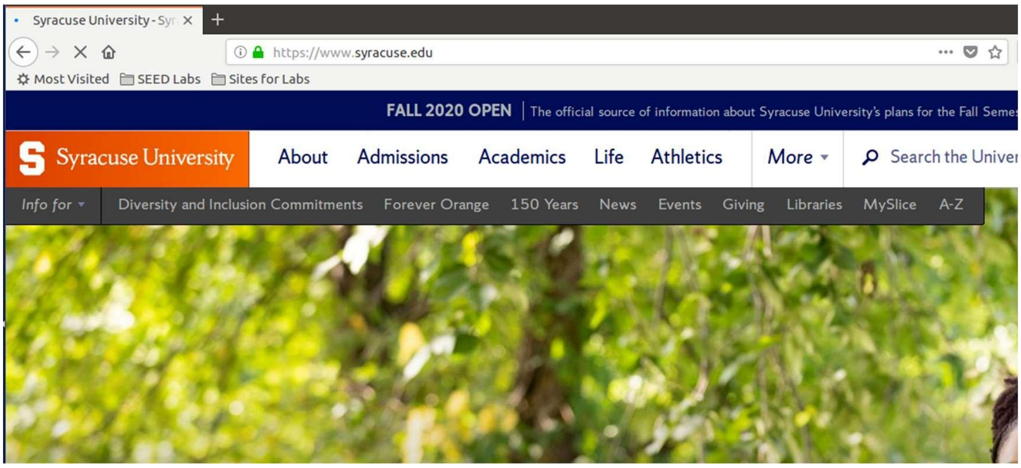
SOCKS Host 127.0.0.1 Port 9000

○ SOCKS v4 ● SOCKS v5

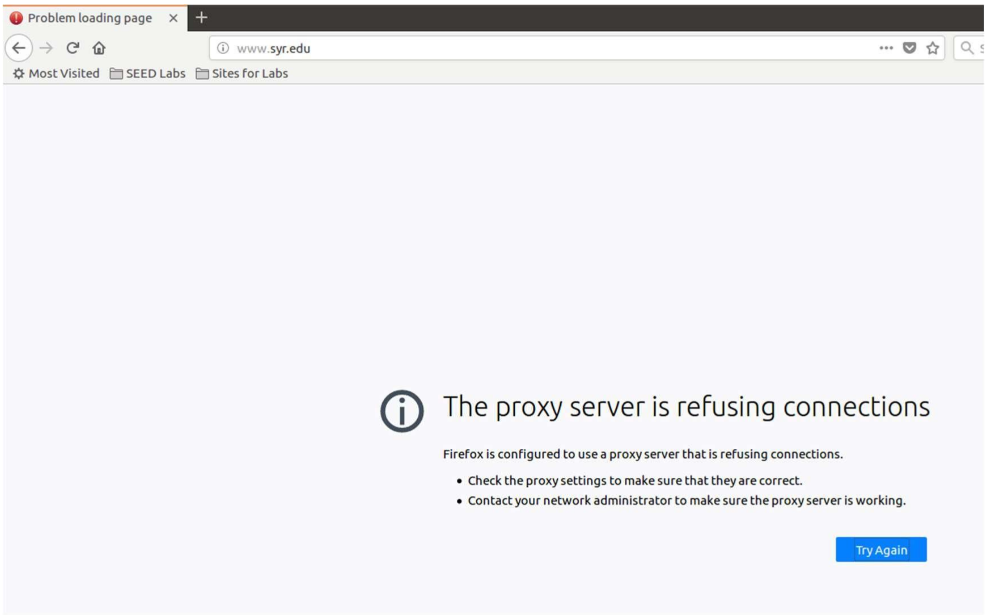
No Proxy for

localhost, 127.0.0.1

可以正常访问网站。



断开连接并清除掉缓存后再次访问网页则无法正常打开：

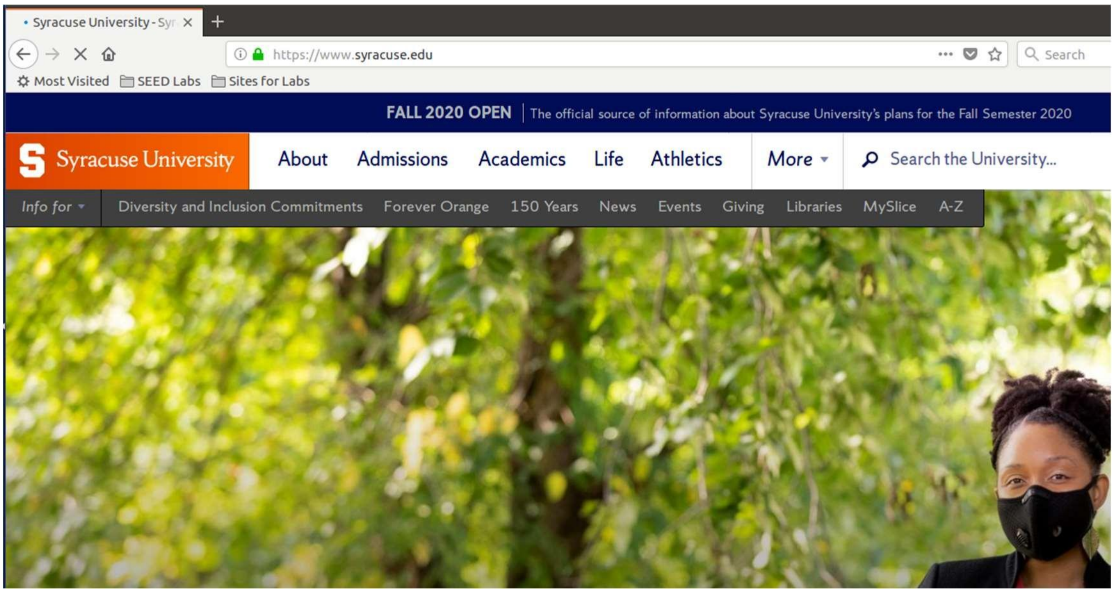


The proxy server is refusing connections

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

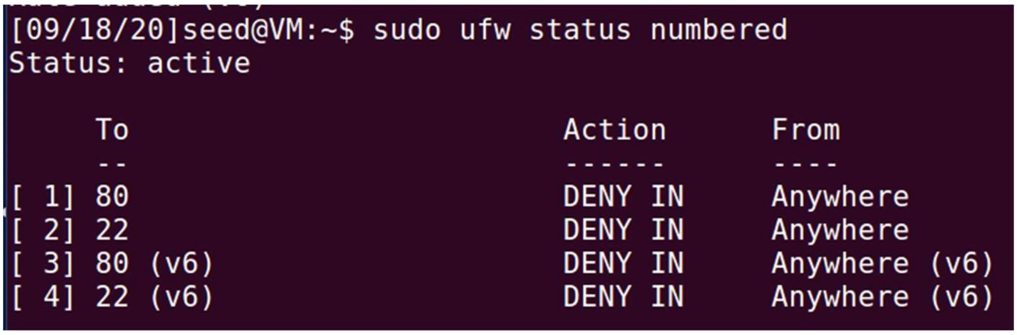
- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

重新连接后又可以正常访问：



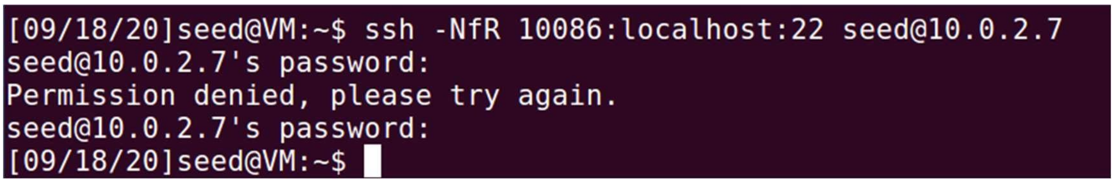
Task 3: Connection Tracking and Stateful Firewall

设置防火墙规则：



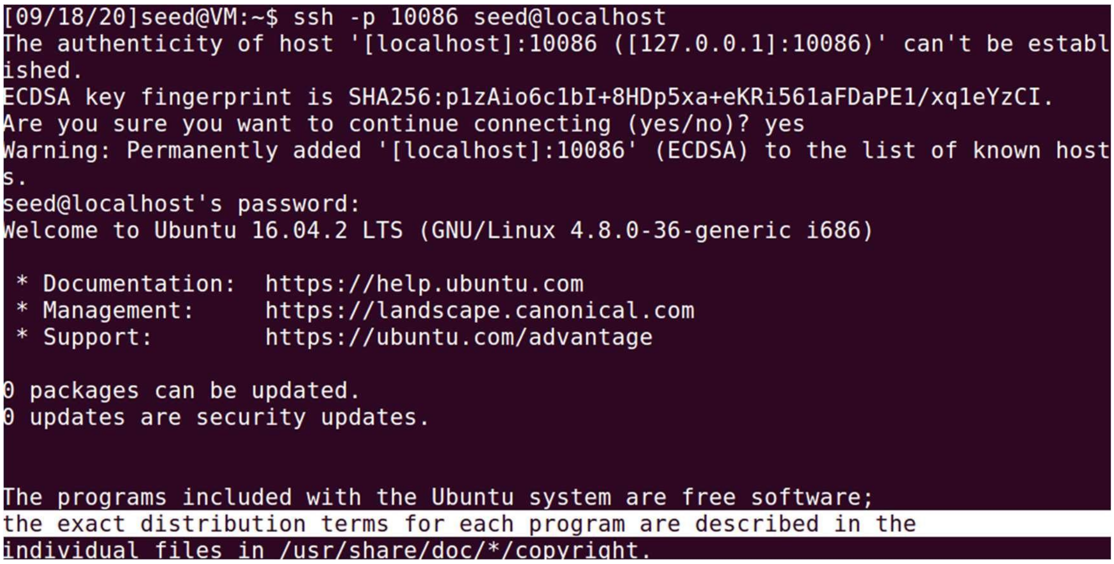
```
[09/18/20]seed@VM:~$ sudo ufw status numbered
Status: active

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

在主机 A 上建立反向 ssh：



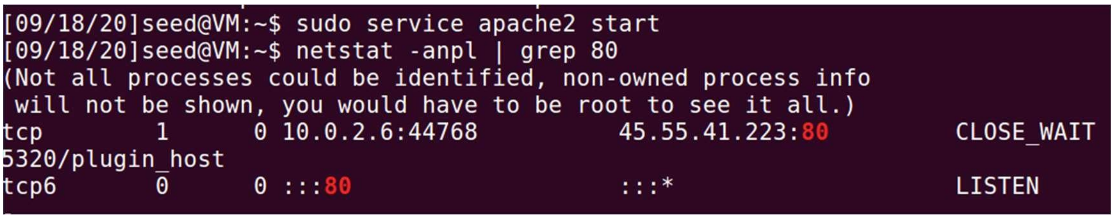
```
[09/18/20]seed@VM:~$ ssh -NfR 10086:localhost:22 seed@10.0.2.7
seed@10.0.2.7's password:
Permission denied, please try again.
seed@10.0.2.7's password:
[09/18/20]seed@VM:~$ 
```

在主机 B 上ssh 连接到主机 A:



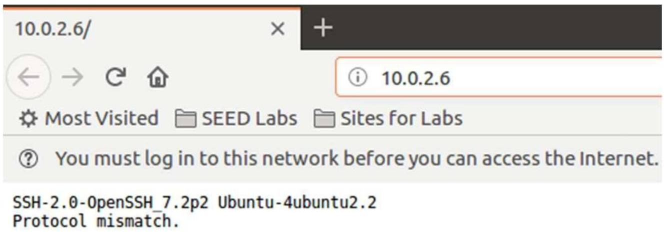
```
[09/18/20]seed@VM:~$ ssh -p 10086 seed@localhost
The authenticity of host '[localhost]:10086 ([127.0.0.1]:10086)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:10086' (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

0 packages 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.
```

在主机 A 上开启 web 服务器:



```
[09/18/20]seed@VM:~$ sudo service apache2 start
[09/18/20]seed@VM:~$ netstat -anpl | grep 80
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        1      0 10.0.2.6:44768          45.55.41.223:80         CLOSE_WAIT
5320/plugin_host
tcp6       0      0 :::80                   :::*                    LISTEN
```

可以看到在主机 B 上能够访问 80 端口，内网穿透成功。

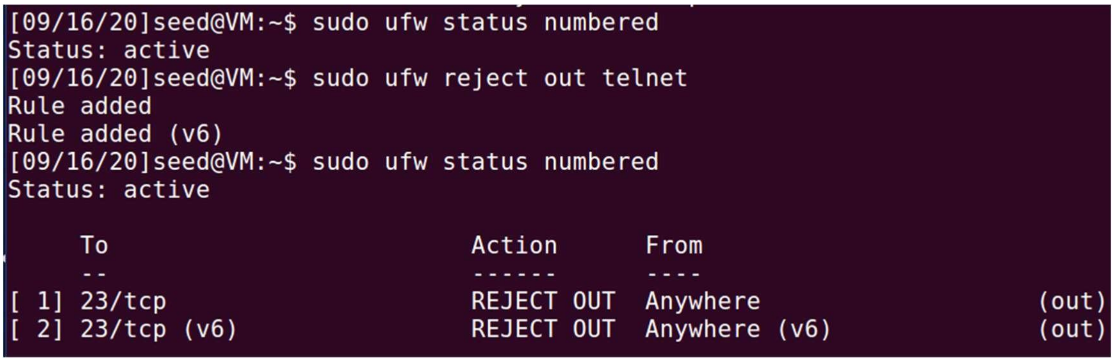


You must log in to this network before you can access the Internet.

```
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
Protocol mismatch.
```

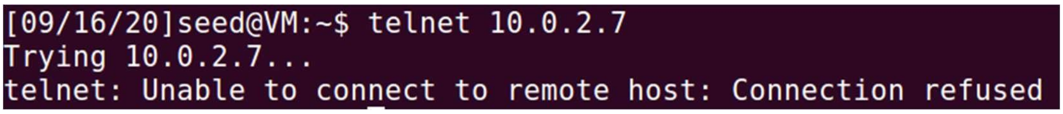
Task 4: Limiting Network Traffific

主机A 的IP：10.0.2.6
主机 B 的 IP：10.0.2.7
在主机 A 上设置如下命令：



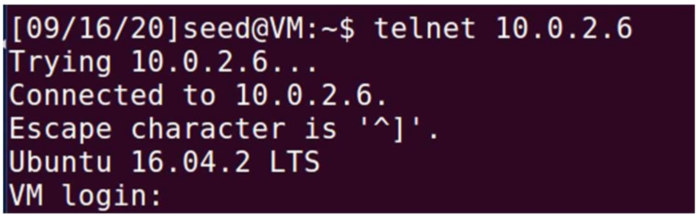
```
[09/16/20]seed@VM:~$ sudo ufw status numbered
Status: active
[09/16/20]seed@VM:~$ sudo ufw reject out telnet
Rule added
Rule added (v6)
[09/16/20]seed@VM:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23/tcp                     REJECT OUT  Anywhere                   (out)
[ 2] 23/tcp (v6)                REJECT OUT  Anywhere (v6)              (out)
```

这是在主机 A 上访问不了主机 B：



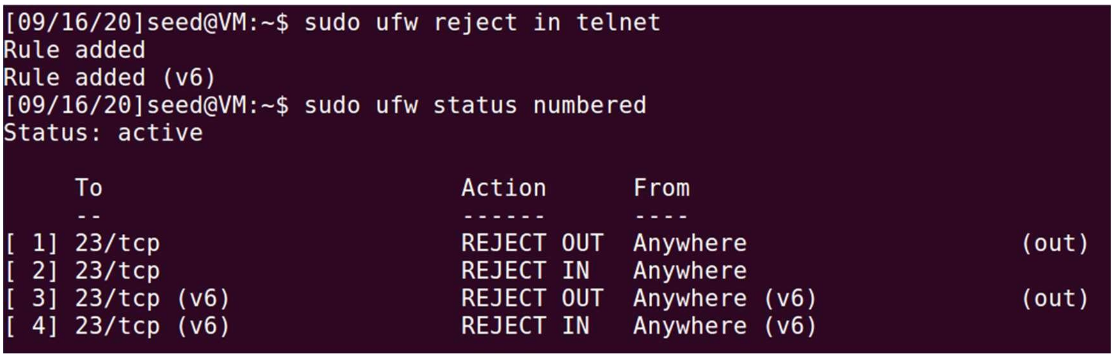
```
[09/16/20]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
telnet: Unable to connect to remote host: Connection refused
```

但是主机 B 可以访问主机A：



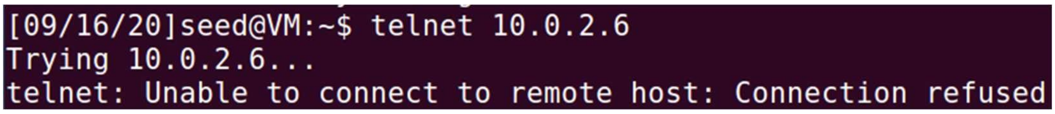
```
[09/16/20]seed@VM:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login:
```

在主机 A 上加上另一个命令：



```
[09/16/20]seed@VM:~$ sudo ufw reject in telnet
Rule added
Rule added (v6)
[09/16/20]seed@VM:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23/tcp                     REJECT OUT  Anywhere                   (out)
[ 2] 23/tcp                     REJECT IN   Anywhere
[ 3] 23/tcp (v6)                REJECT OUT  Anywhere (v6)              (out)
[ 4] 23/tcp (v6)                REJECT IN   Anywhere (v6)
```

这时主机 B 无法访问主机A了。



```
[09/16/20]seed@VM:~$ telnet 10.0.2.6
Trying 10.0.2.6...
telnet: Unable to connect to remote host: Connection refused
```

未设置防火墙规则时可以正常ping 通 seedsecuritylabs.org