

Firewall Exploration Lab Report

Lab Environment Setup

Machine A 10.0.2.4

Machine B 10.0.2.7

Task 1: Using Firewall

使用ufw代替iptables¹

```
[11/30/20]seed@VM:~$ sudo dpkg --get-selections | grep ufw
ufw                                install
[11/30/20]seed@VM:~$ sudo ufw status
Status: inactive
[11/30/20]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
[11/30/20]seed@VM:~$ sudo ufw default deny
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
[11/30/20]seed@VM:~$ sudo ufw status
Status: active
```

Prevent A from doing telnet to Machine B

```
$ sudo ufw deny out from 10.0.2.4 to 10.0.2.7 port 23
```

```
[11/30/20]seed@VM:~$ sudo ufw deny out from 10.0.2.7 to 10.0.2.4 port 23
Rule added
[11/30/20]seed@VM:~$ sudo ufw deny out from 10.0.2.4 to 10.0.2.7 port 23
Rule added
[11/30/20]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
```

Prevent B from doing telnet to Machine A

```
$ sudo ufw deny out from 10.0.2.7 to 10.0.2.4 port 23
```

```
[11/30/20]seed@VM:~$
[11/30/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
█
```

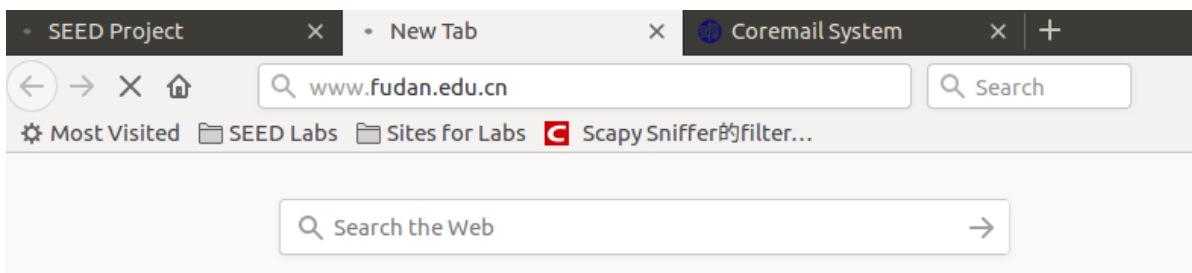
Prevent A from visiting an external web site

因为一般的商用网站都会有不止一个IP地址，所以这里用了学校官网作为外部网址。通过ping命令得到www.fudan.edu.cn的IP地址。

```
$ sudo ufw deny out from 10.0.2.4 to 202.120.224.81 port 80
```

```
[11/30/20]seed@VM:~$ ping www.fudan.edu.cn
PING www.fudan.edu.cn (202.120.224.81) 56(84) bytes of data.
64 bytes from 224.fudan.edu.cn (202.120.224.81): icmp_seq=1 ttl
=250 time=6.05 ms
64 bytes from 224.fudan.edu.cn (202.120.224.81): icmp_seq=2 ttl
=250 time=4.96 ms
^C
--- www.fudan.edu.cn ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 4.967/5.509/6.051/0.542 ms
[11/30/20]seed@VM:~$ sudo ufw deny out from 10.0.2.4 to 202.120
.224.81
Rule added
[11/30/20]seed@VM:~$
```

得到的结果如截图：www.fudan.edu.cn无法正常访问，但是其他网址如mail.fudan.edu.cn还是可以正常访问的。



Task 2: Implementing a Simple Firewall

首先重复以下命令来删除Task 1中用ufw添加的过滤规则

```
$ sudo ufw delete 1
```

```

[11/30/20]seed@VM:~$ sudo ufw delete 1
Deleting:
deny out from 10.0.2.7 to 10.0.2.4 port 23
Proceed with operation (y|n)? y
Rule deleted
[11/30/20]seed@VM:~$ sudo ufw delete 1
Deleting:
deny out from 10.0.2.4 to 10.0.2.7 port 23
Proceed with operation (y|n)? y
Rule deleted
[11/30/20]seed@VM:~$ sudo ufw delete 1
Deleting:
deny out from 10.0.2.4 to 202.120.224.81
Proceed with operation (y|n)? y
Rule deleted
[11/30/20]seed@VM:~$ sudo ufw delete 1
ERROR: Could not find rule '1'
[11/30/20]seed@VM:~$

```

Code

```

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

struct nf_hook_ops nfho_in;
struct nf_hook_ops nfho_out;

struct iphdr *ipHeader;
struct tcphdr *tcpHeader;
struct icmphdr *icmpHeader;

bool isAddressEqual(struct iphdr *ip, int srcORdst, int a, int b, int c, int d){
    bool res = true;
    if (srcORdst == 0) { // 判断src IP
        res &= ((ip->saddr & 0xff000000) >> 24 == d); // big endian
        res &= ((ip->saddr & 0x00ff0000) >> 16 == c);
        res &= ((ip->saddr & 0x0000ff00) >> 8 == b);
        res &= ((ip->saddr & 0x000000ff) == a);
    }
    else if (srcORdst == 1) { // 判断dst IP
        res &= ((ip->daddr & 0xff000000) >> 24 == d);
        res &= ((ip->daddr & 0x00ff0000) >> 16 == c);
        res &= ((ip->daddr & 0x0000ff00) >> 8 == b);
    }
}

```

```

        res &= ((ip->daddr & 0x000000ff) == a);
    }
    return res;
}

unsigned int hook_func_in(void *priv, struct sk_buff *skb, const struct
nf_book_state *state){
    ipHeader = (struct iphdr *)skb_network_header(skb);
    if (ipHeader->protocol == 6) { // TCP
        tcpHeader = (struct tcphdr *)((__u32 *)ipHeader + ipHeader->ihl);
        // ip + ip首部长度的
        unsigned int dst = (unsigned int)ntohs(tcpHeader->dest);

        // Filter 2: B telnet A
        if (dst == 23) { // telnet
            // check ip addr
            if (isAddressEqual(ipHeader,0,10,0,2,7) == false){
                printk(KERN_INFO "Filter 2: incorrect target src ip\n");
                return NF_ACCEPT;
            }
            if (isAddressEqual(ipHeader,1,10,0,2,4) == false){
                printk(KERN_INFO "Filter 2: incorrect target dst ip\n");
                return NF_ACCEPT;
            }
            printk(KERN_INFO "Filter 2: B telnet A\n");
            return NF_DROP;
        }
    }

    if (ipHeader->protocol == 1) { // ICMP
        icmpHeader = (struct icmp_hdr *)((__u32 *)ipHeader + ipHeader->ihl);
        // Filter 5: B ping A
        if (icmpHeader->type == 8){ // ping
            if (isAddressEqual(ipHeader,0,10,0,2,7) == false){
                printk(KERN_INFO "Filter 5: incorrect target src ip\n");
                return NF_ACCEPT;
            }
            if (isAddressEqual(ipHeader,1,10,0,2,4) == false){
                printk(KERN_INFO "Filter 5: incorrect target dst ip\n");
                return NF_ACCEPT;
            }
            printk(KERN_INFO "Filter 5: B ping A\n");
            return NF_DROP;
        }
    }
    return NF_ACCEPT;
}

unsigned int hook_func_out(void *priv, struct sk_buff *skb, const struct
nf_book_state *state){
    ipHeader = (struct iphdr *)skb_network_header(skb);
    if (ipHeader->protocol == 6) { // TCP
        tcpHeader = (struct tcphdr *)((__u32 *)ipHeader + ipHeader->ihl);
        unsigned int dst = (unsigned int)ntohs(tcpHeader->dest);

        // Filter 1: A telnet B
        if (dst == 23) { // telnet
            // check ip addr
            if (isAddressEqual(ipHeader,0,10,0,2,4) == false){

```

```

        printk(KERN_INFO "Filter 1: incorrect target src ip\n");
        return NF_ACCEPT;
    }
    if (isAddressEqual(ipHeader,1,10,0,2,7) == false){
        printk(KERN_INFO "Filter 1: incorrect target dst ip\n");
        return NF_ACCEPT;
    }
    printk(KERN_INFO "Filter 1: A telnet B\n");
    return NF_DROP;
}

// Filter 3: A http www.fudan.edu.cn
if (dst == 80) { // http
    // check ip addr
    if (isAddressEqual(ipHeader,0,10,0,2,4) == false){
        printk(KERN_INFO "Filter 3: incorrect target src ip\n");
        return NF_ACCEPT;
    }
    if (isAddressEqual(ipHeader,1,202,120,224,81) == false){
        printk(KERN_INFO "Filter 3: incorrect target dst ip\n");
        return NF_ACCEPT;
    }
    printk(KERN_INFO "Filter 3: A http www.fudan.edu.cn\n");
    return NF_DROP;
}
}

if (ipHeader->protocol == 1) { // ICMP
    icmpHeader = (struct icmphdr *)((__u32 *)ipHeader + ipHeader->ihl);
    // Filter 4: A ping B
    if (icmpHeader->type == 8){ // ping
        if (isAddressEqual(ipHeader,0,10,0,2,4) == false){
            printk(KERN_INFO "Filter 4: incorrect target src ip\n");
            return NF_ACCEPT;
        }
        if (isAddressEqual(ipHeader,1,10,0,2,7) == false){
            printk(KERN_INFO "Filter 4: incorrect target dst ip\n");
            return NF_ACCEPT;
        }
        printk(KERN_INFO "Filter 4: A ping B\n");
        return NF_DROP;
    }
}

return NF_ACCEPT;
}

int init_module(){
    nfho_in.hook = (void *)hook_func_in;
    nfho_in.hooknum = NF_INET_PRE_ROUTING; // 收到的数据包
    nfho_in.pf = PF_INET;
    nfho_in.priority = NF_IP_PRI_FIRST;

    nf_register_hook(&nfho_in);

    nfho_out.hook = (void *)hook_func_out;
    nfho_out.hooknum = NF_INET_POST_ROUTING; // 转发的或者是本地发出的数据包
    nfho_out.pf = PF_INET;
    nfho_out.priority = NF_IP_PRI_FIRST;
}

```

```

    nf_register_hook(&nfho_out);
    printk(KERN_INFO "Welcome~\n");
    return 0;
}

void cleanup_module(){
    printk(KERN_INFO "See u~\n");
    nf_unregister_hook(&nfho_in);
    nf_unregister_hook(&nfho_out);
}

```

Filter 1: A telnet B

```

[12/03/20]seed@VM:~$
[12/03/20]seed@VM:~$
[12/03/20]seed@VM:~$
[12/03/20]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
[12/03/20]seed@VM:~/Desktop$ dmesg | tail -10
[ 365.422075] Filter 1: A telnet B
[ 373.618429] Filter 1: A telnet B
[ 409.586869] See u~
[ 409.612215] Welcome~
[ 415.504186] Filter 1: A telnet B
[ 416.520118] Filter 1: A telnet B
[ 418.536936] Filter 1: A telnet B
[ 422.795593] Filter 1: A telnet B
[ 430.991395] Filter 1: A telnet B
[ 447.127064] Filter 1: A telnet B
[12/03/20]seed@VM:~/Desktop$
[12/03/20]seed@VM:~/Desktop$
[12/03/20]seed@VM:~/Desktop$
[12/03/20]seed@VM:~/Desktop$
[12/03/20]seed@VM:~/Desktop$

```

Filter 2: B telnet A

```

[12/03/20]seed@VM:~/Desktop$ dmesg | tail -10
[ 743.551470] Filter 3: incorrect target dst ip
[ 743.551477] Filter 3: incorrect target dst ip
[ 743.551482] Filter 3: incorrect target dst ip
[ 815.316350] Filter 2: B telnet A
[ 816.321570] Filter 2: B telnet A
[ 818.338066] Filter 2: B telnet A
[ 822.596167] Filter 2: B telnet A
[ 835.954746] Filter 2: B telnet A
[ 836.971250] Filter 2: B telnet A
[ 838.988617] Filter 2: B telnet A
[12/03/20]seed@VM:~/Desktop$
[12/03/20]seed@VM:~$
[12/03/20]seed@VM:~$
[12/03/20]seed@VM:~$
[12/03/20]seed@VM:~$
[12/03/20]seed@VM:~$
[12/03/20]seed@VM:~$
[12/03/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
^C
[12/03/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...

```

Filter 3: A http www.fudan.edu.cn

```

File Edit View History Bookmarks Tools Help
New Tab x +
www.fudan.edu.cn
Most Visited SEED Labs Sites for Labs Scapy Sniffer's filter...
[ 670.873914] Filter 3: incorrect target dst ip
[ 677.021490] Filter 3: A http www.fudan.edu.cn
[ 678.026665] Filter 3: A http www.fudan.edu.cn
[12/03/20]seed@VM:~/Desktop$ dmesg | tail -10
[ 676.361879] Filter 3: incorrect target dst ip
[ 676.617689] Filter 3: incorrect target dst ip
[ 676.617711] Filter 3: incorrect target dst ip
[ 676.873914] Filter 3: incorrect target dst ip
[ 677.021490] Filter 3: A http www.fudan.edu.cn
[ 678.026665] Filter 3: A http www.fudan.edu.cn
[ 679.691616] Filter 3: A http www.fudan.edu.cn
[ 680.043553] Filter 3: A http www.fudan.edu.cn
[ 680.059623] Filter 3: incorrect target dst ip
[ 680.159831] Filter 3: incorrect target dst ip
[12/03/20]seed@VM:~/Desktop$

```

Filter 4: A ping B

```
[12/03/20]seed@VM:~$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 10.0.2.7 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 0.000 ms
[12/03/20]seed@VM:~$
```

```
[12/03/20]seed@VM:~/Desktop$
[12/03/20]seed@VM:~/Desktop$ dmesg | tail -10
[ 568.596144] Filter 4: A ping B
[ 569.620619] Filter 4: A ping B
[ 570.644756] Filter 4: A ping B
[ 571.669728] Filter 4: A ping B
[ 572.694130] Filter 4: A ping B
[ 573.718398] Filter 4: A ping B
[ 574.742789] Filter 4: A ping B
[ 575.767240] Filter 4: A ping B
[ 576.792329] Filter 4: A ping B
[ 577.816485] Filter 4: A ping B
[12/03/20]seed@VM:~/Desktop$
```

Filter 5: B ping A

```
[12/03/20]seed@VM:~/Desktop$ dmesg | tail -10
[ 897.161421] Filter 5: B ping A
[ 891.015053] Filter 5: B ping A
[ 892.039301] Filter 5: B ping A
[ 893.063335] Filter 5: B ping A
[ 894.088335] Filter 5: B ping A
[ 895.112455] Filter 5: B ping A
[12/03/20]seed@VM:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
^C
--- 10.0.2.4 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 0.000 ms
[12/03/20]seed@VM:~$
```

Task 3: Evading Egress Filtering

由于www.facebook.com由于一些众所周知的原因已经被block了，所以还是使用www.fudan.edu.cn代替

```
# Block all the outgoing traffic to external telnet servers
$ sudo ufw deny out from 10.0.2.4 to any port 23
# Block all the outgoing traffic to www.fudan.edu.cn
$ sudo ufw deny out from 10.0.2.4 to 202.120.224.81
```

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

这一步需要先关闭10.0.2.7的防火墙

```
$ sudo ufw disable
```

```
$ ssh -L 8000:10.0.2.7:23 seed@10.0.2.7
$ telnet localhost 8000
```

Time	Source	Destination	Protocol	Length	Info
262	2020-12-03 05:54:54.4371549...	10.0.2.7	TCP	60	Telnet Data ...
263	2020-12-03 05:54:54.4371691...	10.0.2.7	TCP	60	23 -> 37534 [ACK] Seq=242783126 Ack=79859800 Win=43776 Len=0 TSval=45011856 TSecr=45011856
264	2020-12-03 05:54:54.6392752...	10.0.2.7	SSH	104	Client: Encrypted packet (len=36)
265	2020-12-03 05:54:54.6393189...	10.0.2.7	TCP	60	22 -> 49722 [ACK] Seq=2851978142 Ack=3760935213 Win=270 Len=0 TSval=45011906 TSecr=2354744
266	2020-12-03 05:54:54.6395124...	10.0.2.7	TCP	60	Telnet Data ...
267	2020-12-03 05:54:54.6395205...	10.0.2.7	TCP	60	23 -> 37534 [ACK] Seq=242783126 Ack=79859801 Win=43776 Len=0 TSval=45011907 TSecr=45011907
268	2020-12-03 05:54:54.8269728...	10.0.2.4	SSH	104	Client: Encrypted packet (len=36)
269	2020-12-03 05:54:54.8269985...	10.0.2.7	TCP	60	22 -> 49722 [ACK] Seq=2851978142 Ack=3760935249 Win=270 Len=0 TSval=45011953 TSecr=2354791
270	2020-12-03 05:54:54.8271298...	10.0.2.7	TCP	60	Telnet Data ...
271	2020-12-03 05:54:54.8271344...	10.0.2.7	TCP	60	23 -> 37534 [ACK] Seq=242783126 Ack=79859802 Win=43776 Len=0 TSval=45011953 TSecr=45011953
272	2020-12-03 05:54:55.4095519...	10.0.2.4	SSH	104	Client: Encrypted packet (len=36)
273	2020-12-03 05:54:55.4095818...	10.0.2.7	TCP	60	22 -> 49722 [ACK] Seq=2851978142 Ack=3760935285 Win=270 Len=0 TSval=45012099 TSecr=2354936
274	2020-12-03 05:54:55.4096763...	10.0.2.7	TCP	60	Telnet Data ...
275	2020-12-03 05:54:55.4096828...	10.0.2.7	TCP	60	23 -> 37534 [ACK] Seq=242783126 Ack=79859803 Win=43776 Len=0 TSval=45012099 TSecr=45012099
276	2020-12-03 05:54:55.7583262...	10.0.2.4	SSH	104	Client: Encrypted packet (len=36)
277	2020-12-03 05:54:55.7583521...	10.0.2.7	TCP	60	22 -> 49722 [ACK] Seq=2851978142 Ack=3760935321 Win=270 Len=0 TSval=45012186 TSecr=2355024
278	2020-12-03 05:54:55.7584856...	10.0.2.7	TCP	70	Telnet Data ...
279	2020-12-03 05:54:55.7584898...	10.0.2.7	TCP	60	23 -> 37534 [ACK] Seq=242783126 Ack=79859805 Win=43776 Len=0 TSval=45012186 TSecr=45012186

在Wireshark中抓到的数据包可以看到ssh连接是作为真正的telnet连接（10.0.2.4<-->10.0.2.7）的桥梁（10.0.2.4<-->10.0.2.7(acting as ssh server, "apollo")<-->10.0.2.7）

```
rtt min/avg/max/mdev = 0.321/0.450/0.612/0.131 ms
[12/03/20]seed@VM:~/Desktop$ ssh -L 8000:10.0.2.7:23 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 Dec  3 04:44:22 2020 from 10.0.2.4
[12/03/20]seed@VM:~$
```

```
VM login: seed
Password:
Last login: Thu Dec  3 04:45:23 EST 2020 from 10.0.2.4 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

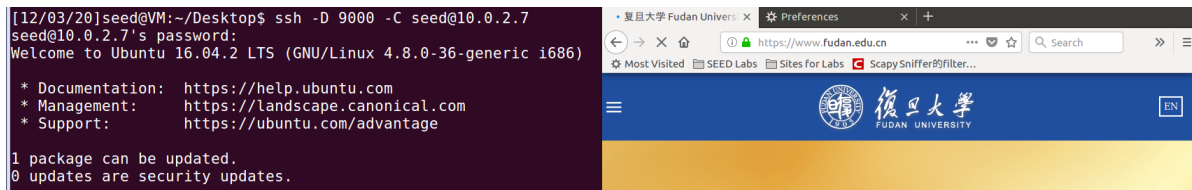
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

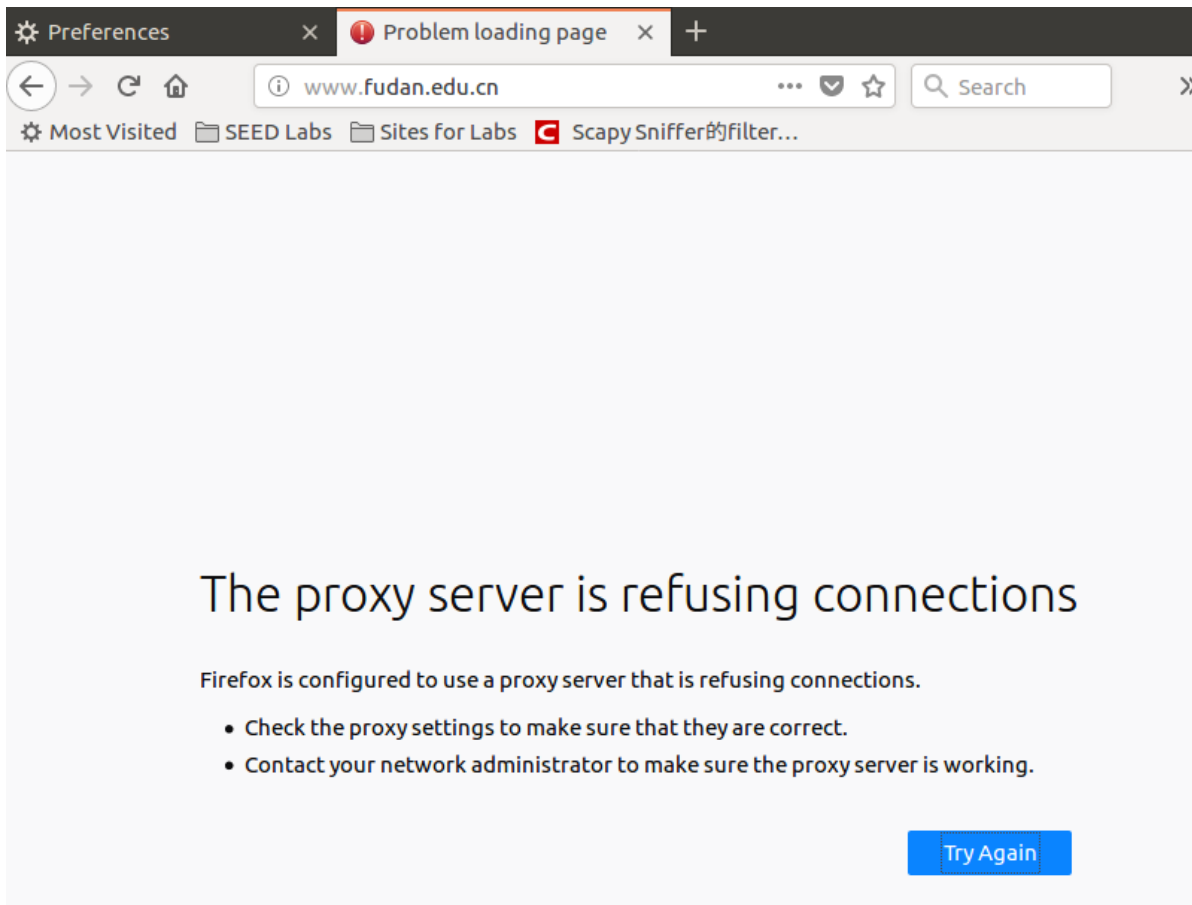
[12/03/20]seed@VM:~$
```


Task 3.b: Connect to Facebook using SSH Tunnel

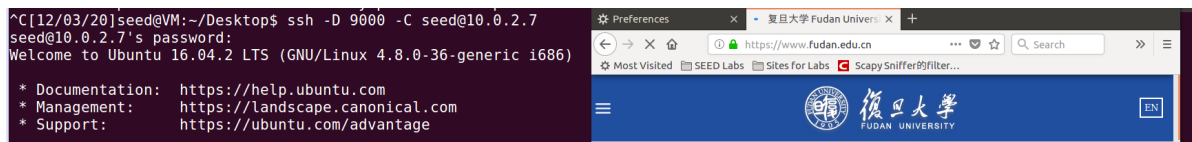
```
$ ssh -D 9000 -C seed@10.0.2.7
# -D 绑定端口
# -C 请求压缩所有数据
```



断开ssh连接并清空浏览器的cache之后:



再次建立ssh连接之后刷新浏览器页面:



在这个过程中10.0.2.7充当了proxy的角色。实际上是由10.0.2.7向www.fudan.edu.cn发送请求并将收到的响应通过建立的ssh连接发给10.0.2.4。

4	2020-12-03 05:02:08.1237350...	10.0.2.4	SSH	118 Client: Encrypted packet (len=52)
5	2020-12-03 05:02:08.1240623...	10.0.2.7	TCP	66 22 -> 49594 [ACK] Seq=1175174051 Ack=2848152770 Win=1332 Len=0 TSval=44219866 TSecr=1562697
6	2020-12-03 05:02:08.1242149...	10.0.2.7	TCP	74 53746 -> 443 [SYN] Seq=1032029628 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=44219866 TSecr=0 WS=128
7	2020-12-03 05:02:08.1306463...	202.120.224.81	TCP	60 443 -> 53746 [SYN, ACK] Seq=11053535 Ack=1032029629 Win=32768 Len=0 MSS=1460
8	2020-12-03 05:02:08.1363637...	10.0.2.7	TCP	60 53746 -> 443 [ACK] Seq=1032029629 Ack=11053536 Win=29200 Len=0
9	2020-12-03 05:02:08.1363888...	10.0.2.4	SSH	102 Server: Encrypted packet (len=36)
10	2020-12-03 05:02:08.1421393...	10.0.2.7	SSH	310 Client: Encrypted packet (len=244)
11	2020-12-03 05:02:08.1427023...	10.0.2.7	TLSv1.2	571 Client Hello
12	2020-12-03 05:02:08.1836193...	10.0.2.4	TCP	66 22 -> 49594 [ACK] Seq=1175174087 Ack=2848153014 Win=1332 Len=0 TSval=44219881 TSecr=1562701
13	2020-12-03 05:02:08.2077814...	202.120.224.81	TLSv1.2	195 Server Hello, Change Cipher Spec, Encrypted Handshake Message
14	2020-12-03 05:02:08.2080602...	10.0.2.7	TCP	60 53746 -> 443 [ACK] Seq=1032030146 Ack=11053677 Win=30016 Len=0
15	2020-12-03 05:02:08.2089959...	10.0.2.4	SSH	238 Server: Encrypted packet (len=172)
16	2020-12-03 05:02:08.2092951...	10.0.2.7	SSH	134 Client: Encrypted packet (len=68)
17	2020-12-03 05:02:08.2097505...	10.0.2.4	TCP	66 22 -> 49594 [ACK] Seq=1175174259 Ack=2848153082 Win=1332 Len=0 TSval=44219887 TSecr=1562718
18	2020-12-03 05:02:08.2097624...	10.0.2.7	TLSv1.2	105 Change Cipher Spec, Hello Request, Hello Request
19	2020-12-03 05:02:08.2103633...	10.0.2.4	SSH	278 Client: Encrypted packet (len=212)
20	2020-12-03 05:02:08.2107029...	10.0.2.7	TCP	66 22 -> 49594 [ACK] Seq=1175174259 Ack=2848153294 Win=1332 Len=0 TSval=44219887 TSecr=1562718
21	2020-12-03 05:02:08.2107972...	10.0.2.7	TLSv1.2	231 Application Data

Task 4: Evading Ingress Filtering

```
# 删除之前的task设置的防火墙规则
$ sudo ufw delete 1
# block Machine B from accessing its port 80 (web server) and 22 (SSH server)
$ sudo ufw deny out from 10.0.2.7 to 10.0.2.4 port 80
$ sudo ufw deny out from 10.0.2.7 to 10.0.2.4 port 22
```

首先在10.0.2.4上开启反向连接隧道²：

```
$ ssh -f -N -R 10000:localhost:22 seed@10.0.2.7
# -f 后台执行ssh指令
# -N 不执行远程指令
# -R listen-port:host:port 指派远程上的 port 到本地地址上的 port
```

然后在10.0.2.7上通过10000端口就可以成功建立ssh连接：

```
$ ssh seed@localhost -p 10000
```

```
[12/03/20]seed@VM:~$ ssh seed@localhost -p 10000
The authenticity of host '[localhost]:10000 ([127.0.0.1]:10000)'
can't be established.
ECDSA key fingerprint is SHA256:plzAio6c1bI+8HDp5xa+eKRi561aFDaPE
1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:10000' (ECDSA) to the lis
t 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.

Last login: Thu Oct 22 16:50:06 2020 from 192.168.60.5
[12/03/20]seed@VM:~$ cd Desktop
[12/03/20]seed@VM:~/Desktop$ ls
Cyber Security  Module.symvers  task2.ko        task2.o
Makefile        System Security task2.mod.c
modules.order   task2.c         task2.mod.o
```

1. <https://www.cnblogs.com/EasonJim/p/6851241.html> [↗](#)

2. https://www.cnblogs.com/x_wukong/p/5997872.html [↗](#)