

Lab 6 Linux Firewall Exploration

Task 1: Using Firewall

虚拟机信息

虚拟机	IP
SEED	192.168.11.140
SEED 1	192.168.11.143

调整默认条目，防止被丢弃

```
9 # 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.
11 DEFAULT INPUT POLICY="ACCEPT"
```

首先观察双方可互相telnet

```
[09/17/20]seed@VM:~$ telnet 192.168.11.143
Trying 192.168.11.143...
Connected to 192.168.11.143.
Escape character is '^].
Ubuntu 16.04.2 LTS
VM login: seed
Password:
/usr/lib/update-notifier/update-motd-fsck-at-reboot[:59: integer expression
ion expected:          0
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.
```

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.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

```
[09/17/20]seed@VM:~$ ls
android      Desktop    examples.desktop  Music      source
bin          Documents   get-pip.py       Pictures   Templates
Customization Downloads  lib              Public    Videos
[09/17/20]seed@VM:~$ cd Desktop/
[09/17/20]seed@VM:~/Desktop$ ls
Server  VMwareTools-10.3.10-13959562.tar.gz  vmware-tools-distrib
[09/17/20]seed@VM:~/Desktop$ exit
logout
Connection closed by foreign host.
```

```
[09/17/20]seed@VM:~$ telnet 192.168.11.140
Trying 192.168.11.140...
Connected to 192.168.11.140.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Sep 17 05:56:42 EDT 2020 from 192.168.11.143 on pts/19
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:~$ exit
logout
Connection closed by foreign host.
```

- 阻止A对B发起telnet

```
1 | $ sudo iptables -A OUTPUT -p tcp --dport 23 -j DROP
```

```
[09/17/20]seed@VM:~$ sudo iptables -A OUTPUT -p tcp --dport 23 -j DROP
[09/17/20]seed@VM:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
target     prot opt source          destination

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
DROP      tcp   --  0.0.0.0/0        0.0.0.0/0          tcp  dpt:23
[09/17/20]seed@VM:~$ telnet 192.168.11.143
Trying 192.168.11.143...
telnet: Unable to connect to remote host: Connection timed out
```

```
1 | $ sudo ufw deny out proto tcp to any port 23
```

- 阻止B对A发起telnet

```
1 | $ sudo iptables -A INPUT -p tcp --dport 23 -j DROP
```

```
[09/17/20]seed@VM:~$ telnet 192.168.11.140
Trying 192.168.11.140...
telnet: Unable to connect to remote host: Connection timed out
[09/17/20]seed@VM:~$ telnet 192.168.11.140
Trying 192.168.11.140...
telnet: Unable to connect to remote host: Connection timed out
```

```
1 | $ sudo ufw 23
```

```
[09/17/20]seed@VM:~$ telnet 192.168.11.140
Trying 192.168.11.140...
telnet: Unable to connect to remote host: Connection timed out
```

- 阻止A访问外部网站

```
1 | $ sudo iptables -A OUTPUT -p tcp -d ***.***.***.*** --dport 80 -j DROP
```

```
1 | $ sudo ufw deny out proto tcp to ***.***.***.*** port 80
```

```
[09/17/20]seed@M:~$ sudo iptables -A OUTPUT -p tcp -d 220.181.38.148 --dport 80 -j DROP
[09/17/20]seed@M:~$ wget baidu.com
--2020-09-17 06:52:39 -- http://baidu.com/
Resolving baidu.com (baidu.com)... 39.156.69.79, 220.181.38.148
Connecting to baidu.com (baidu.com)|39.156.69.79|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 81 [text/html]
Saving to: 'index.html.4'

index.html.4          100%[=====]     81 --KB/s   in 0s
2020-09-17 06:52:39 (12.4 MB/s) - 'index.html.4' saved [81/81]

[09/17/20]seed@M:~$ sudo iptables -A OUTPUT -p tcp -d 39.156.69.79 --dport 80 -j DROP
[09/17/20]seed@M:~$ wget baidu.com
--2020-09-17 06:53:00 -- http://baidu.com/
Resolving baidu.com (baidu.com)... 220.181.38.148, 39.156.69.79
Connecting to baidu.com (baidu.com)|220.181.38.148|:80... failed: Connection timed out.
Connecting to baidu.com (baidu.com)|39.156.69.79|:80... failed: Connection timed out.
Retrying.

--2020-09-17 06:57:22-- (try: 2) http://baidu.com/
Connecting to baidu.com (baidu.com)|220.181.38.148|:80... ^C
[09/17/20]seed@M:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
Chain FORWARD (policy ACCEPT)
target    prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
DROP      tcp  --  0.0.0.0/0      180.101.49.12    tcp dpt:80
DROP      tcp  --  0.0.0.0/0      220.181.38.148  tcp dpt:80
DROP      tcp  --  0.0.0.0/0      39.156.69.79   tcp dpt:80
```

Task 2: Implementing a Simple Firewall

- nf.c

```
1 #include <linux/module.h>
2 #include <linux/kernel.h>
3 #include <linux/netfilter.h>
4 #include <linux/netfilter_ipv4.h>
5 #include <linux/ip.h>
6 #include <linux/tcp.h>
7 #include <linux/skbuff.h>
8 #include <linux/icmp.h>
9 #include <linux/udp.h>
10
11 /* This is the structure we shall use to register our function */
12 static struct nf_hook_ops nfho;
13 /* This is the hook function itself */
14 unsigned int hook_func(void *priv, struct sk_buff *skb, const struct
15 nf_hook_state *state)
16 {
17     /* This is where you can inspect the packet contained in
18      * the structure pointed by skb, and decide whether to accept
19      * or drop it. You can even modify the packet */
20     // In this example, we simply drop all packets
21     // return NF_DROP; /* Drop ALL packets */
22     struct iphdr *iph;
23     struct tcphdr *tcph;
24
25     iph = ip_hdr(skb);
26     tcph = (void *)iph+iph->ihl*4;
27
28     if (
29         (iph->protocol == IPPROTO_TCP && tcph->dest == htons(23))
30         || (iph->protocol == IPPROTO_TCP && tcph->dest == htons(80))
31         || (iph->protocol == IPPROTO_TCP && tcph->dest == htons(8080))
32         || (iph->protocol == IPPROTO_TCP && tcph->dest == htons(22))
33         || (iph->protocol == IPPROTO_TCP && tcph->dest == htons(443))
34     )
```

```

34 {
35     printk(KERN_INFO "Dropping tcp packet to %d.%d.%d.%d\n",
36             ((unsigned char *) &iph->daddr)[0],
37             ((unsigned char *) &iph->daddr)[1],
38             ((unsigned char *) &iph->daddr)[2],
39             ((unsigned char *) &iph->daddr)[3]);
40     return NF_DROP;
41 }else{
42     printk("I got it.");
43     return NF_ACCEPT;
44 }
45 }
46 /* Initialization routine */
47 int setUpFilter(void)
48 { /* Fill in our hook structure */
49     printk("Hello, Groot.");
50     nfho.hook = hook_func; /* Handler function */
51     nfho.hooknum = NF_INET_POST_ROUTING; /* First hook for IPv4 */
52     nfho.pf = PF_INET;
53     nfho.priority = NF_IP_PRI_FIRST; /* Make our function first */
54
55     nf_register_hook(&nfho);
56     return 0;
57 }
58 /* Cleanup routine */
59 void removeFilter(void)
60 {
61     printk("So long, Groot.");
62     nf_unregister_hook(&nfho);
63 }
64
65 module_init(setUpFilter);
66 module_exit(removeFilter);

```

- Makefile

```

1 obj-m += nf.o
2 all:
3     make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules
4 clean:
5     make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean

```

make后执行命令可在dmesg中看到printk的结果

```

1 $ sudo insmod mymod.ko      (inserting a module)
2 $ lsmod                      (list all modules)
3 $ sudo rmmod mymod.ko        (remove the module)

```

```

[ 2310.952198] Hello, Groot
[ 2963.702993] So long, Groot.

```

限制生效，并用dmesg查看

```

[09/17/20]seed@VM:~/.../PF$ telnet 192.168.11.143
Trying 192.168.11.143...
telnet: Unable to connect to remote host: Connection timed out

```

```
[ 5993.876140] Hello, Groot.  
[ 6006.861179] Dropping tcp packet to 192.168.11.143  
[ 6007.877068] Dropping tcp packet to 192.168.11.143  
[ 6009.892446] Dropping tcp packet to 192.168.11.143  
[ 6013.924630] Dropping tcp packet to 192.168.11.143  
[ 6022.117129] Dropping tcp packet to 192.168.11.143  
[ 6038.244602] Dropping tcp packet to 192.168.11.143  
[ 6071.269074] Dropping tcp packet to 192.168.11.143
```

```
[09/17/20]seed@VM:~/.../PF$ wget www.baidu.com  
--2020-09-17 13:55:03-- http://www.baidu.com/  
Resolving www.baidu.com (www.baidu.com)... 180.101.49.12, 180.101.49.11  
Connecting to www.baidu.com (www.baidu.com)|180.101.49.12|:80... ■
```

```
[ 6415.953208] Dropping tcp packet to 180.101.49.12  
[ 6416.964546] Dropping tcp packet to 180.101.49.12  
[ 6418.980304] Dropping tcp packet to 180.101.49.12  
[ 6423.012423] Dropping tcp packet to 180.101.49.12  
[ 6431.204739] Dropping tcp packet to 180.101.49.12  
[ 6447.332504] Dropping tcp packet to 180.101.49.12
```

Task 3: Evading Egress Filtering

添加ufw规则

```
1 | $ sudo ufw deny out proto tcp to any port 23  
2 | $ sudo ufw deny out proto tcp to 220.181.38.148
```

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

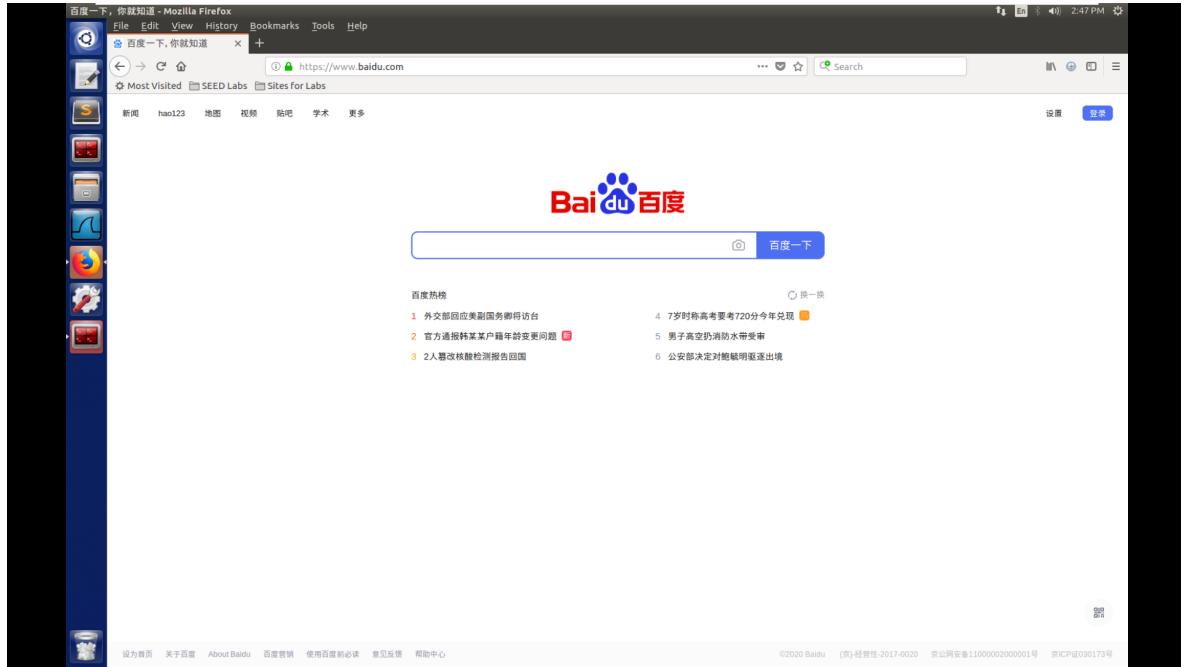
利用SSH连接Server 192.168.11.143，并telnet localhost，成功绕过

```
[09/17/20]seed@VM:~/.../PF$ ssh -L 8000:192.168.11.140:23 seed@192.168.11.  
.143  
seed@192.168.11.143'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 14:07:45 2020 from 192.168.11.140  
[09/17/20]seed@VM:~$ cd Desktop/  
[09/17/20]seed@VM:~/Desktop$ ls  
Server VMwareTools-10.3.10-13959562.tar.gz vmware-tools-distrib  
[09/17/20]seed@VM:~/Desktop$ telnet 192.168.11.143 8000  
Trying 192.168.11.143...  
telnet: Unable to connect to remote host: Connection refused  
[09/17/20]seed@VM:~/Desktop$ telnet 192.168.11.143  
Trying 192.168.11.143...  
Connected to 192.168.11.143.  
Escape character is '^]'.  
Ubuntu 16.04.2 LTS  
VM login: seed  
Password:  
Last login: Thu Sep 17 14:22:57 EDT 2020 from 192.168.11.143 on pts/19  
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.
```

Task 3.b: Connect to Baidu using SSH Tunnel

因为Facebook.com是不存在的网址，SEU官网有异常，所以改用baidu.com的IP：220.181.38.148

虚拟机A 192.168.11.140不能正常访问百度，虚拟机B 192.168.11.143可以正常访问百度



建立A->B的SSH连接

```
1 | $ ssh -D 9000 -C seed@machine_B
```

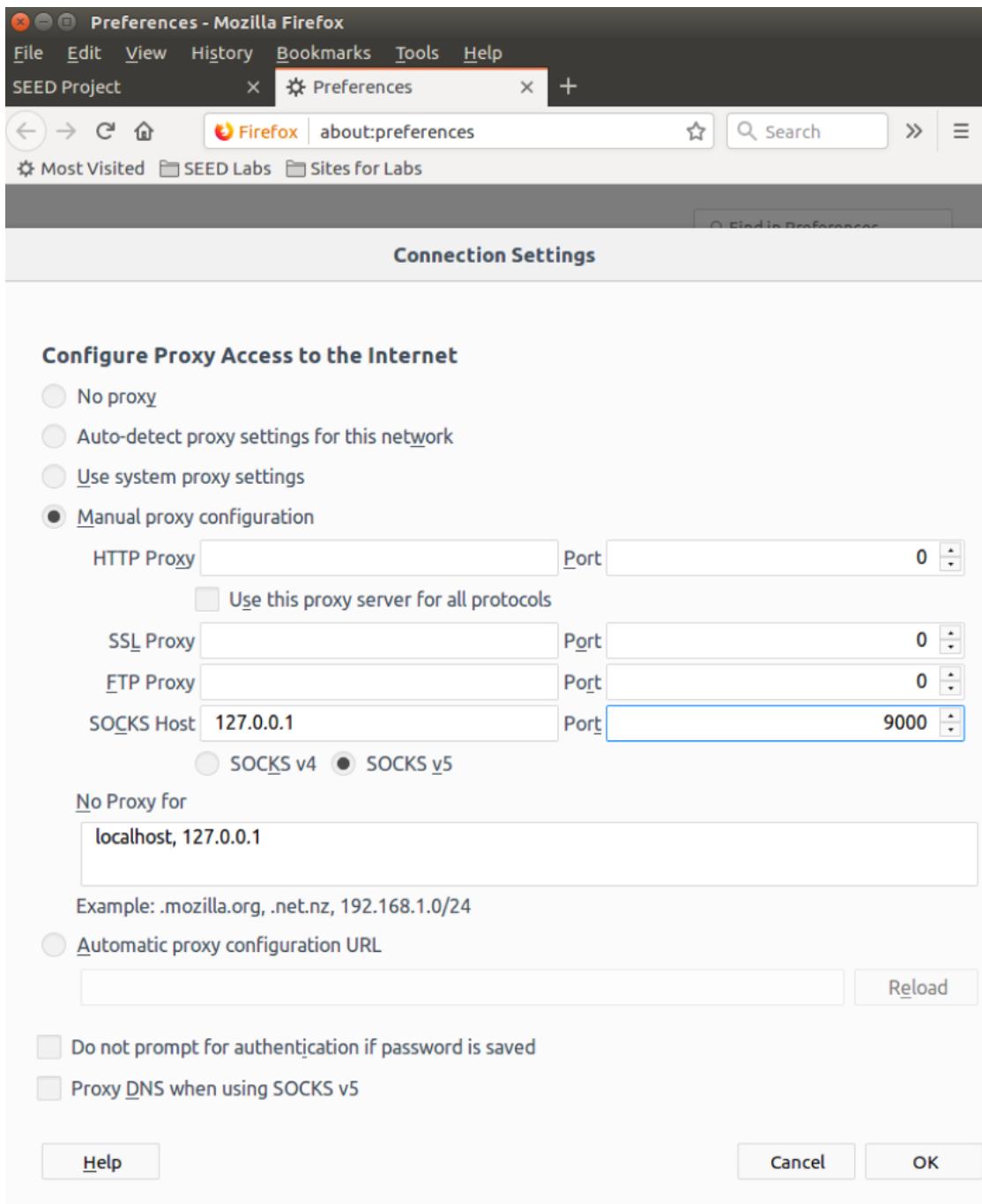
```
[09/17/20]seed@VM:~/.../PF$ ssh -D 9000 -C seed@192.168.11.143
seed@192.168.11.143's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

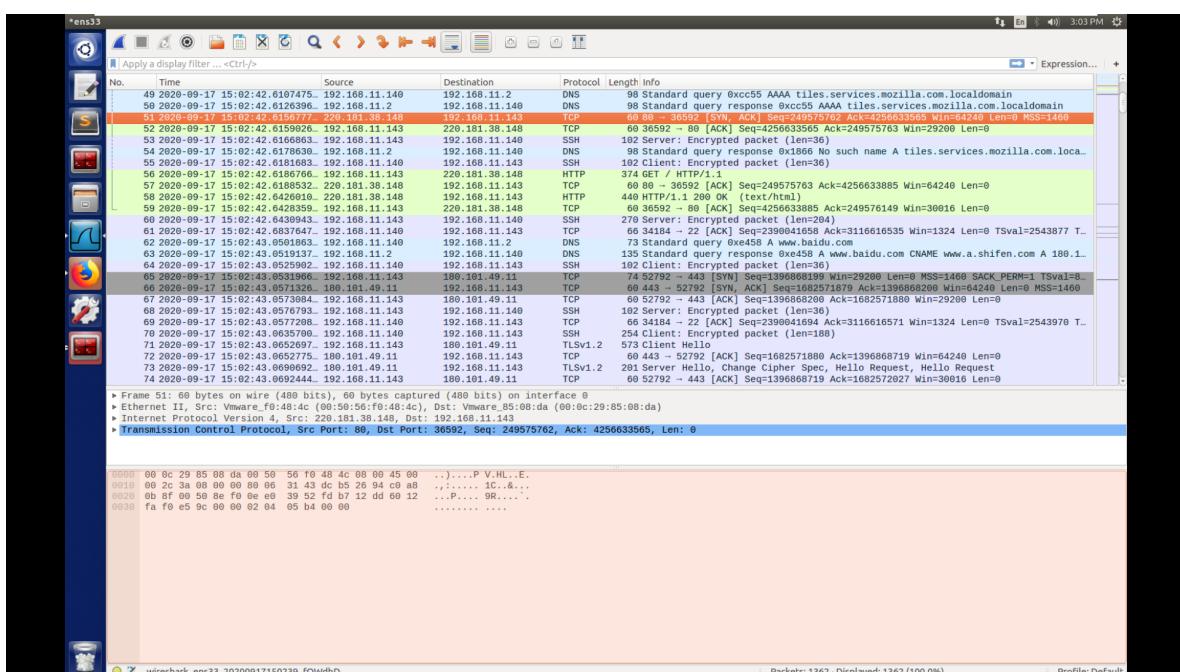
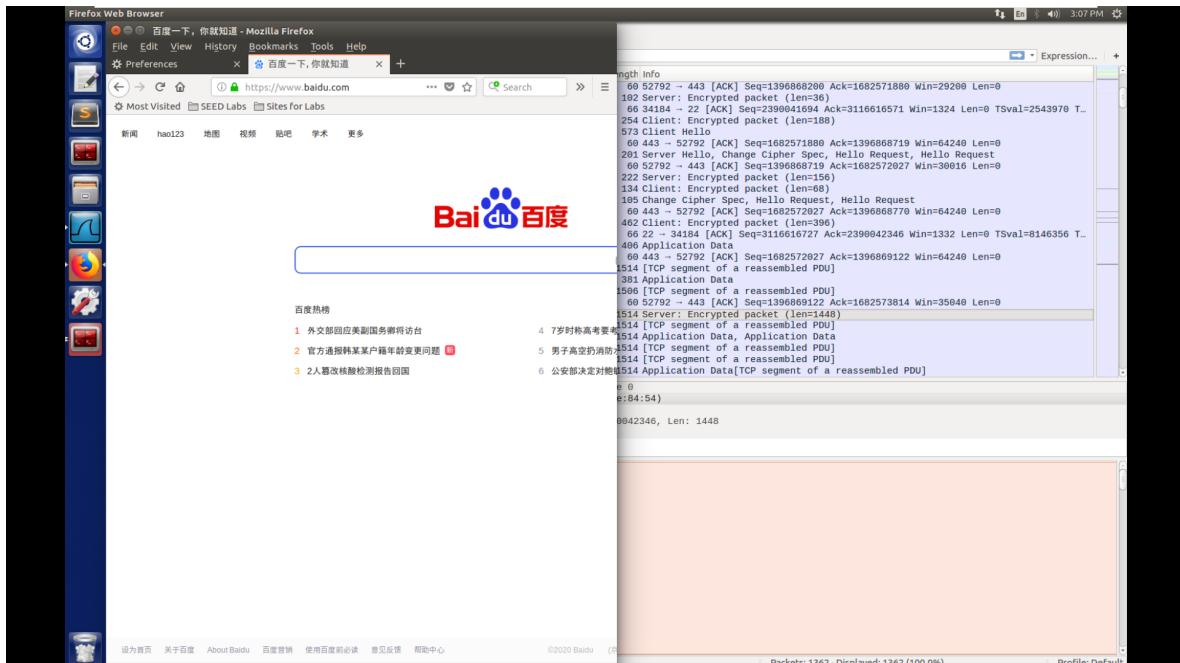
1 package can be updated.
0 updates are security updates.

Last login: Thu Sep 17 14:49:39 2020 from 192.168.11.143
[09/17/20]seed@VM:~$
```

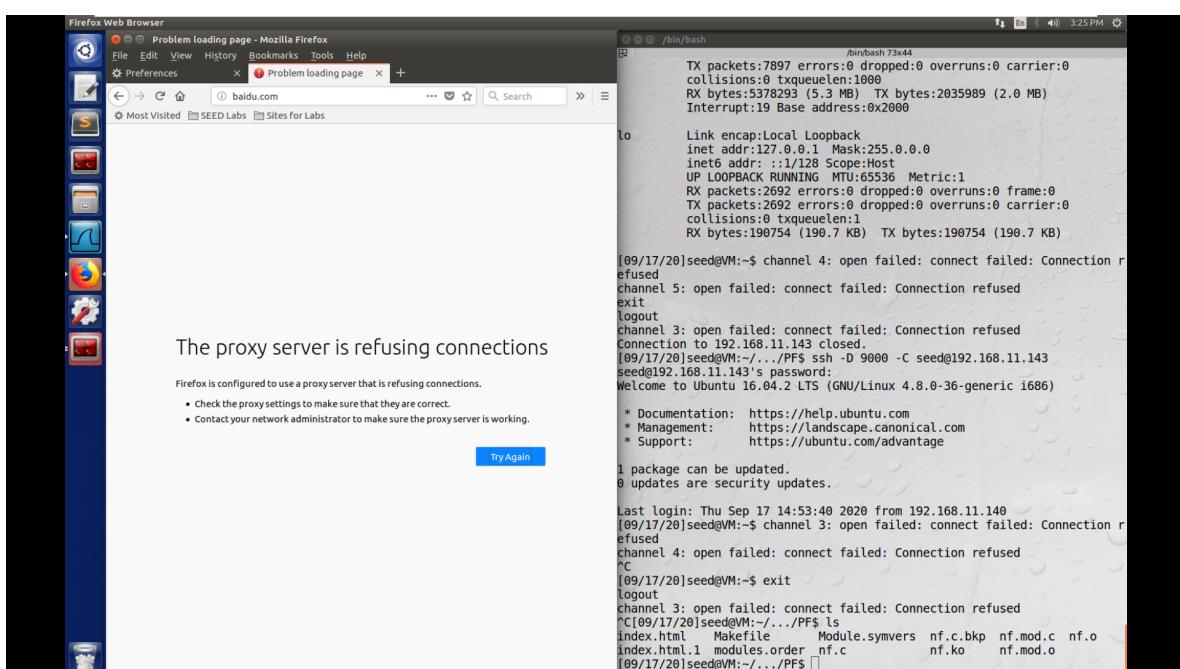
Firefox设置代理



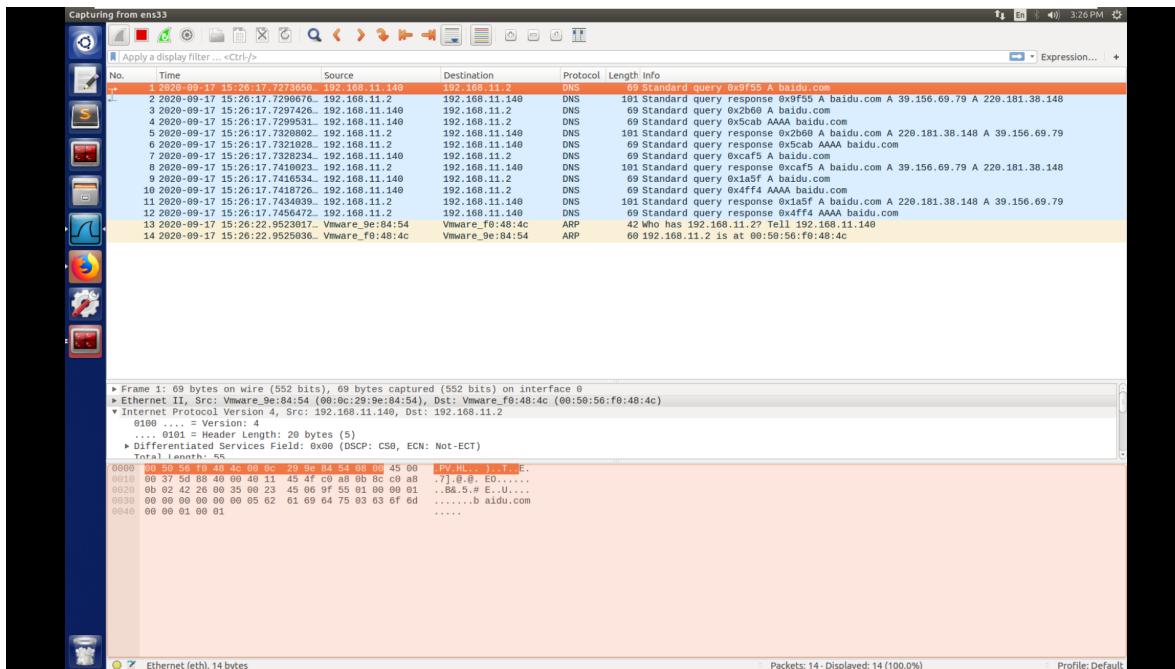
代理后可以正常访问百度，利用Wireshark可以发现，虚拟机A(192.168.11.140)与百度(220.181.38.148)之间是通过虚拟机B(192.168.11.143)进行转发的



清除Cache并断开SSH后，又不能正常访问百度



在Wireshark中没有发现发往外网的报文，认为是ufw将报文拦截



恢复SSH后看到又能够正常访问百度，证明了可以通过SSH连接防火墙外部主机进而间接绕过防火墙的拦截

