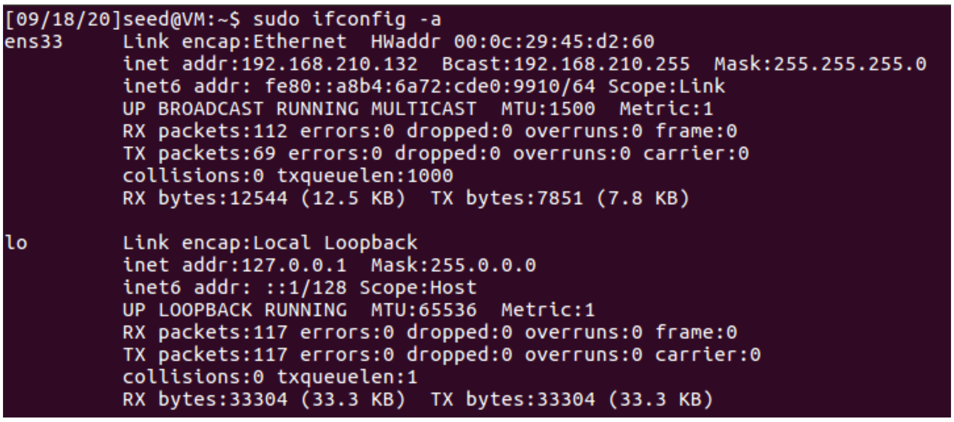
SEED LAB6

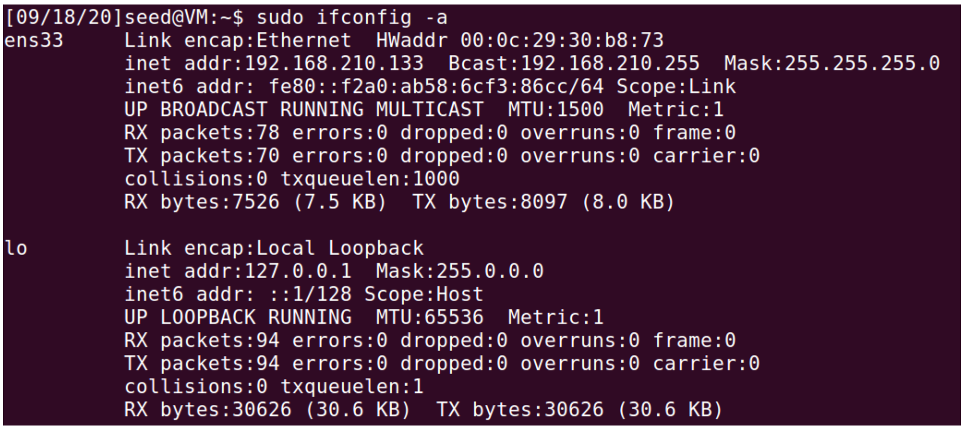
57117111 蒋涛

Linux Firewall Exploration Lab

Task1: Using Firewall



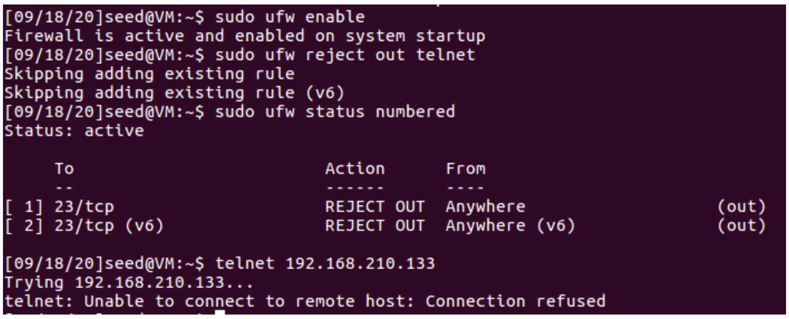
```
[09/18/20]seed@VM:~$ sudo ifconfig -a
ens33     Link encap:Ethernet  HWaddr 00:0c:29:45:d2:60
          inet addr:192.168.210.132  Bcast:192.168.210.255  Mask:255.255.255.0
          inet6 addr: fe80::a8b4:6a72:cde0:9910/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:112 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12544 (12.5 KB)  TX bytes:7851 (7.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:33304 (33.3 KB)  TX bytes:33304 (33.3 KB)
```



```
[09/18/20]seed@VM:~$ sudo ifconfig -a
ens33     Link encap:Ethernet  HWaddr 00:0c:29:30:b8:73
          inet addr:192.168.210.133  Bcast:192.168.210.255  Mask:255.255.255.0
          inet6 addr: fe80::f2a0:ab58:6cf3:86cc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7526 (7.5 KB)  TX bytes:8097 (8.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:30626 (30.6 KB)  TX bytes:30626 (30.6 KB)
```

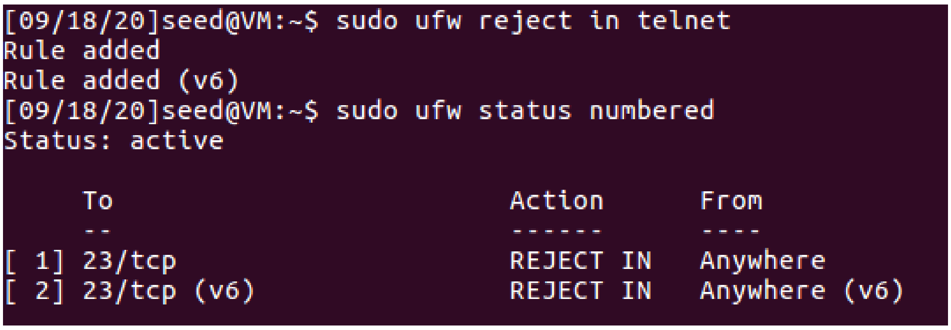
The IP address of A and B is 192.168.210.132 and 192.168.210.133 respectively.

- Prevent A from doing telnet to Machine B

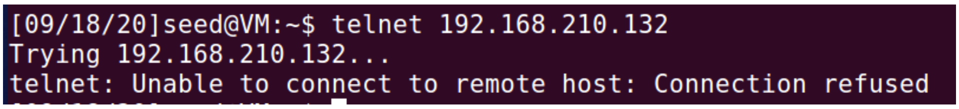


```
[09/18/20]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
[09/18/20]seed@VM:~$ sudo ufw reject out telnet
Skipping adding existing rule
Skipping adding existing rule (v6)
[09/18/20]seed@VM:~$ sudo ufw status numbered
Status: active

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

[09/18/20]seed@VM:~$ telnet 192.168.210.133
Trying 192.168.210.133...
telnet: Unable to connect to remote host: Connection refused
```

- Prevent B from doing telnet to Machine A

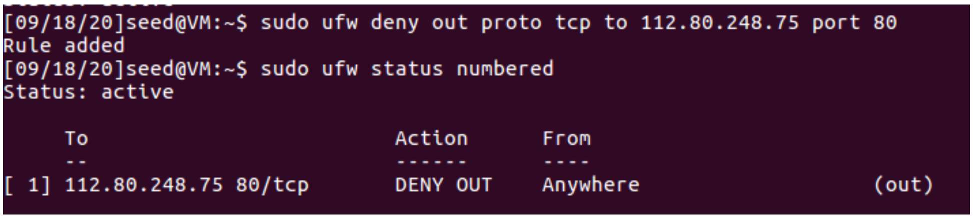


```
[09/18/20]seed@VM:~$ sudo ufw reject in telnet
Rule added
Rule added (v6)
[09/18/20]seed@VM:~$ sudo ufw status numbered
Status: active

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

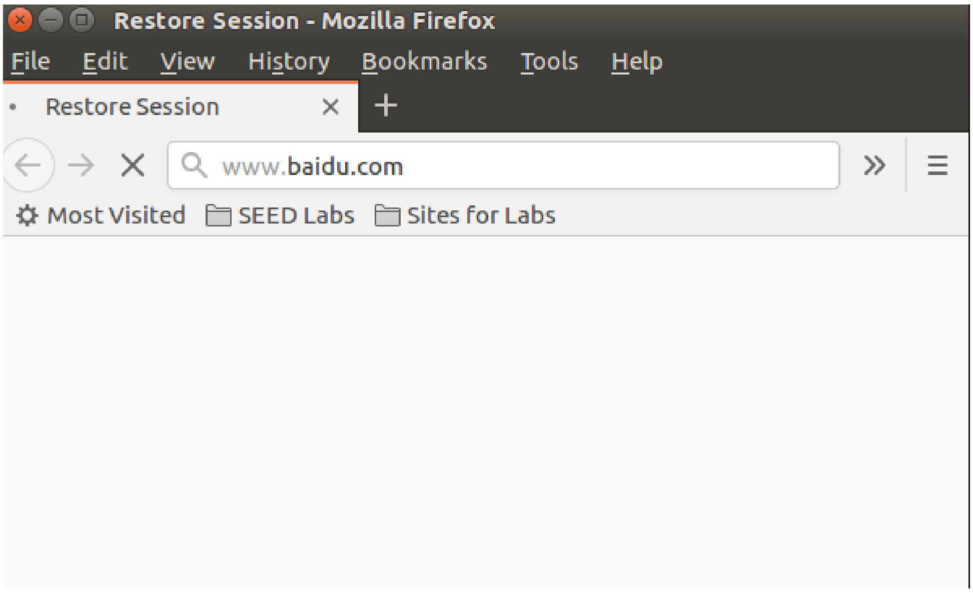


```
[09/18/20]seed@VM:~$ telnet 192.168.210.132
Trying 192.168.210.132...
telnet: Unable to connect to remote host: Connection refused
```

- Prevent A from visiting an external web site



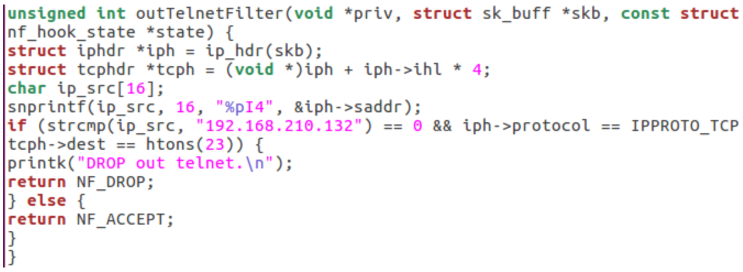
```
[09/18/20]seed@VM:~$ sudo ufw deny out proto tcp to 112.80.248.75 port 80
Rule added
[09/18/20]seed@VM:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 112.80.248.75 80/tcp       DENY OUT    Anywhere                   (out)
```


Restore Session - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Restore Session
www.baidu.com
Most Visited
SEED Labs
Sites for Labs

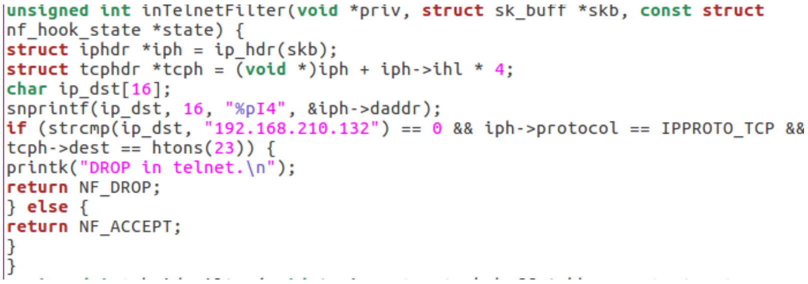
Block www.baidu.com successfully.

Task2: Implementing a Simple Firewall

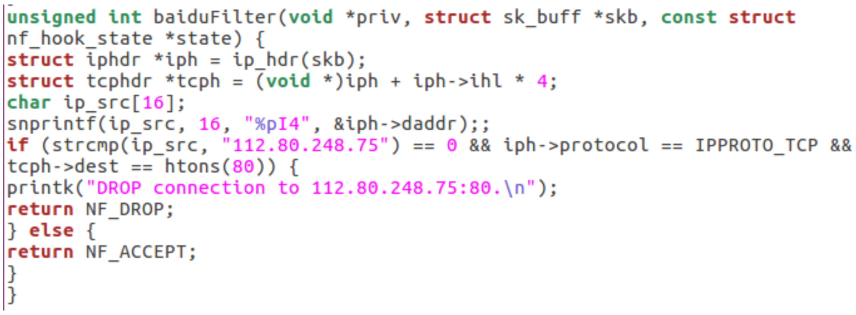
- Block in & out telnet and visiting www.baidu.com



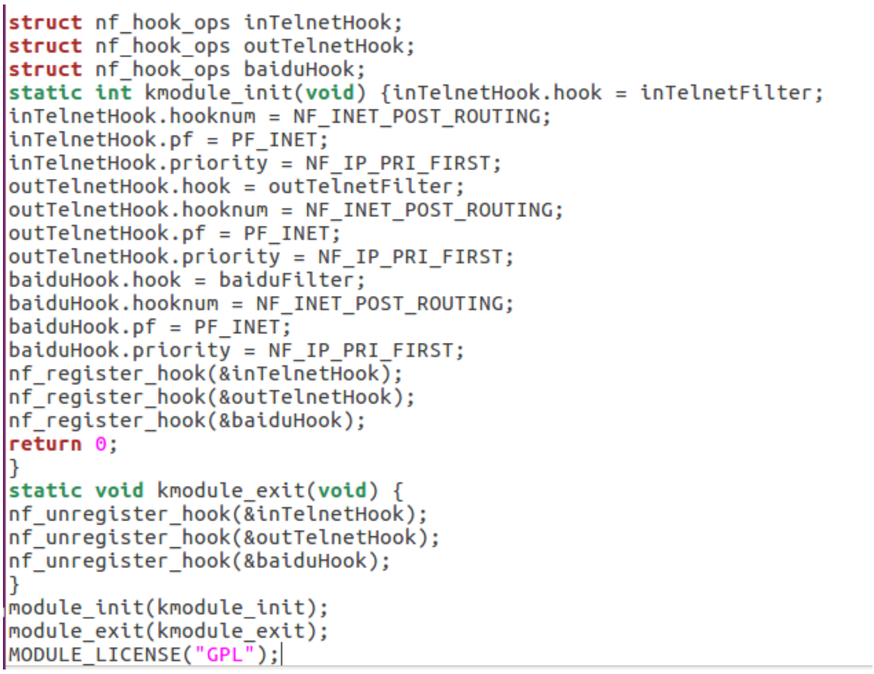
```
unsigned int outTelnetFilter(void *priv, struct sk_buff *skb, const struct
nf_hook_state *state) {
struct iphdr *iph = ip_hdr(skb);
struct tcphdr *tcph = (void *)iph + iph->ihl * 4;
char ip_src[16];
snprintf(ip_src, 16, "%pI4", &iph->saddr);
if (strcmp(ip_src, "192.168.210.132") == 0 && iph->protocol == IPPROTO_TCP &&
tcph->dest == htons(23)) {
printk("DROP out telnet.\n");
return NF_DROP;
} else {
return NF_ACCEPT;
}
}
```



```
unsigned int inTelnetFilter(void *priv, struct sk_buff *skb, const struct
nf_hook_state *state) {
struct iphdr *iph = ip_hdr(skb);
struct tcphdr *tcph = (void *)iph + iph->ihl * 4;
char ip_dst[16];
snprintf(ip_dst, 16, "%pI4", &iph->daddr);
if (strcmp(ip_dst, "192.168.210.132") == 0 && iph->protocol == IPPROTO_TCP &&
tcph->dest == htons(23)) {
printk("DROP in telnet.\n");
return NF_DROP;
} else {
return NF_ACCEPT;
}
}
```



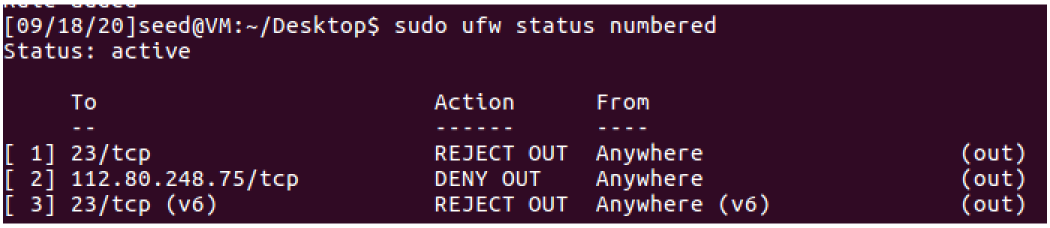
```
unsigned int baiduFilter(void *priv, struct sk_buff *skb, const struct
nf_hook_state *state) {
struct iphdr *iph = ip_hdr(skb);
struct tcphdr *tcph = (void *)iph + iph->ihl * 4;
char ip_src[16];
snprintf(ip_src, 16, "%pI4", &iph->daddr);;
if (strcmp(ip_src, "112.80.248.75") == 0 && iph->protocol == IPPROTO_TCP &&
tcph->dest == htons(80)) {
printk("DROP connection to 112.80.248.75:80.\n");
return NF_DROP;
} else {
return NF_ACCEPT;
}
}
```



```
struct nf_hook_ops inTelnetHook;
struct nf_hook_ops outTelnetHook;
struct nf_hook_ops baiduHook;
static int kmodule_init(void) {inTelnetHook.hook = inTelnetFilter;
inTelnetHook.hooknum = NF_INET_POST_ROUTING;
inTelnetHook.pf = PF_INET;
inTelnetHook.priority = NF_IP_PRI_FIRST;
outTelnetHook.hook = outTelnetFilter;
outTelnetHook.hooknum = NF_INET_POST_ROUTING;
outTelnetHook.pf = PF_INET;
outTelnetHook.priority = NF_IP_PRI_FIRST;
baiduHook.hook = baiduFilter;
baiduHook.hooknum = NF_INET_POST_ROUTING;
baiduHook.pf = PF_INET;
baiduHook.priority = NF_IP_PRI_FIRST;
nf_register_hook(&inTelnetHook);
nf_register_hook(&outTelnetHook);
nf_register_hook(&baiduHook);
return 0;
}
static void kmodule_exit(void) {
nf_unregister_hook(&inTelnetHook);
nf_unregister_hook(&outTelnetHook);
nf_unregister_hook(&baiduHook);
}
module_init(kmodule_init);
module_exit(kmodule_exit);
MODULE_LICENSE("GPL");
```

Task3: Evading Egress Filtering

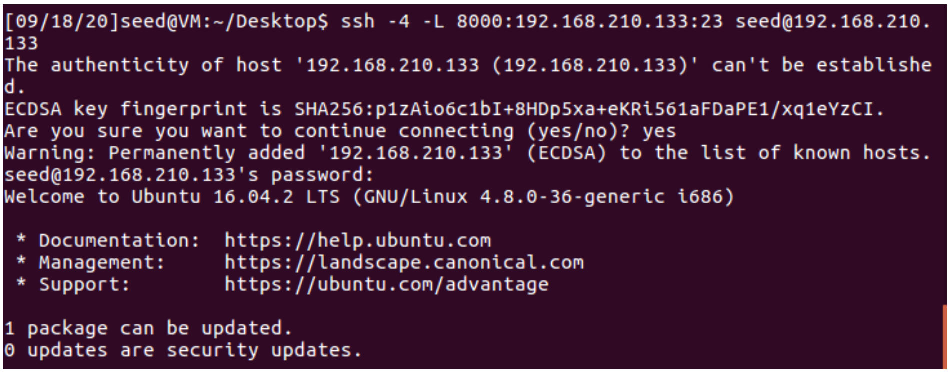
- Prevent all outgoing traffic to external telnet servers and www.baidu.com



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

     To                         Action      From
     --                         ------      ----
[ 1] 23/tcp                     REJECT OUT  Anywhere                   (out)
[ 2] 112.80.248.75/tcp          DENY OUT    Anywhere                   (out)
[ 3] 23/tcp (v6)                REJECT OUT  Anywhere (v6)              (out)
```

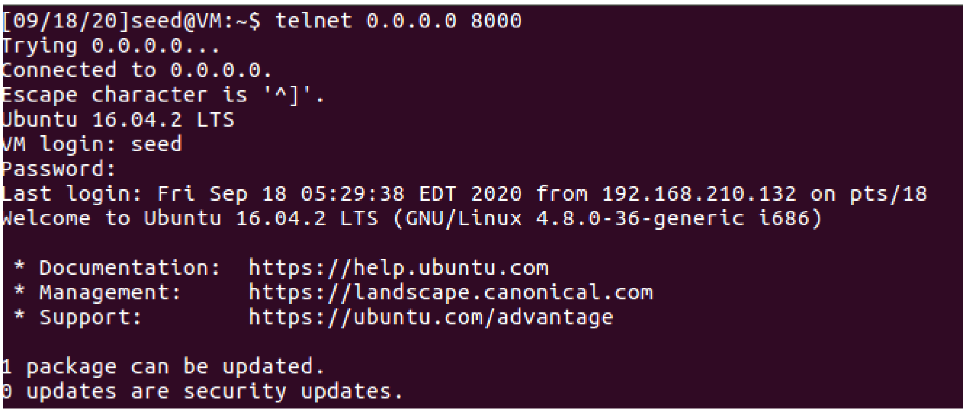
Task 3.a: Telnet to Machine B through the firewall

- Send `ssh` request to machine B on machine A



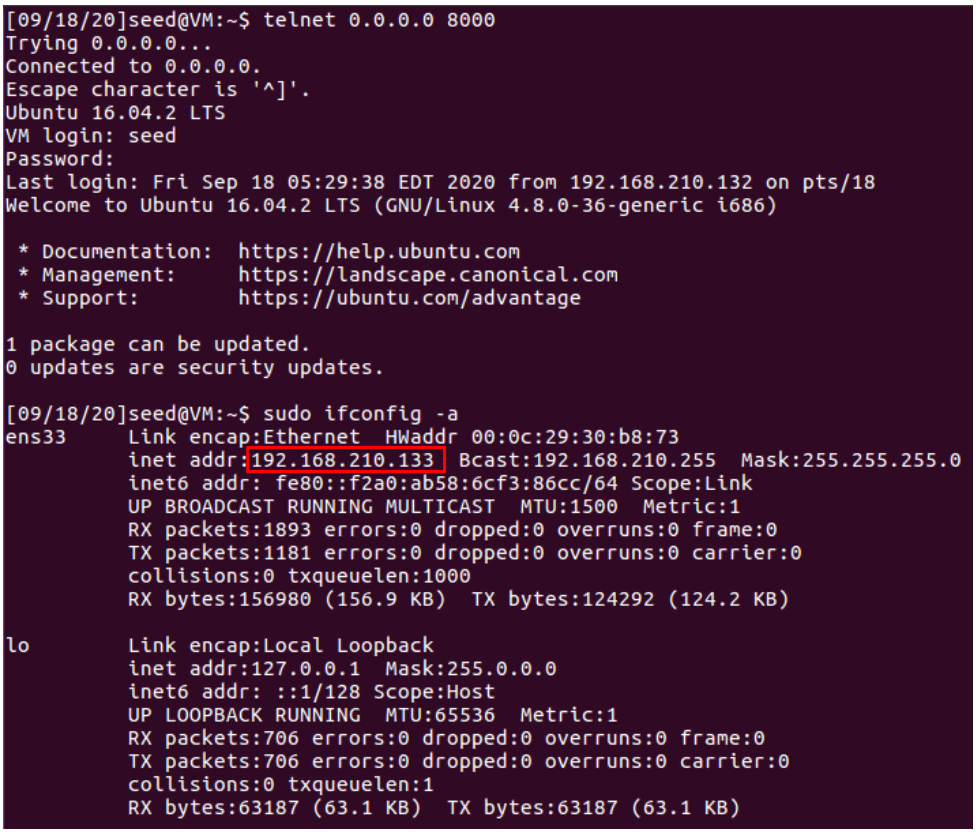
```
[09/18/20]seed@VM:~/Desktop$ ssh -4 -L 8000:192.168.210.133:23 seed@192.168.210.
133
The authenticity of host '192.168.210.133 (192.168.210.133)' can't be establishe
d.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.210.133' (ECDSA) to the list of known hosts.
seed@192.168.210.133'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.
```

- Send `telnet` connection to A on machine A at the same time



```
[09/18/20]seed@VM:~$ telnet 0.0.0.0 8000
Trying 0.0.0.0...
Connected to 0.0.0.0.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri Sep 18 05:29:38 EDT 2020 from 192.168.210.132 on pts/18
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.
```

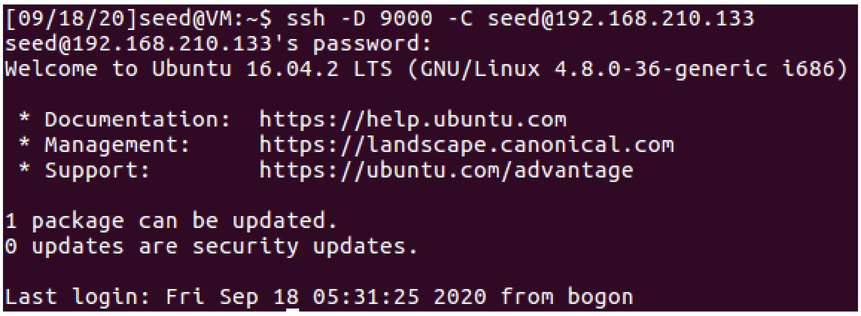
- Bypass the firewall successfully



```
[09/18/20]seed@VM:~$ telnet 0.0.0.0 8000
Trying 0.0.0.0...
Connected to 0.0.0.0.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri Sep 18 05:29:38 EDT 2020 from 192.168.210.132 on pts/18
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.

[09/18/20]seed@VM:~$ sudo ifconfig -a
ens33     Link encap:Ethernet  HWaddr 00:0c:29:30:b8:73
          inet addr:192.168.210.133  Bcast:192.168.210.255  Mask:255.255.255.0
          inet6 addr: fe80::f2a0:ab58:6cf3:86cc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1893 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1181 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:156980 (156.9 KB)  TX bytes:124292 (124.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:706 errors:0 dropped:0 overruns:0 frame:0
          TX packets:706 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:63187 (63.1 KB)  TX bytes:63187 (63.1 KB)
```

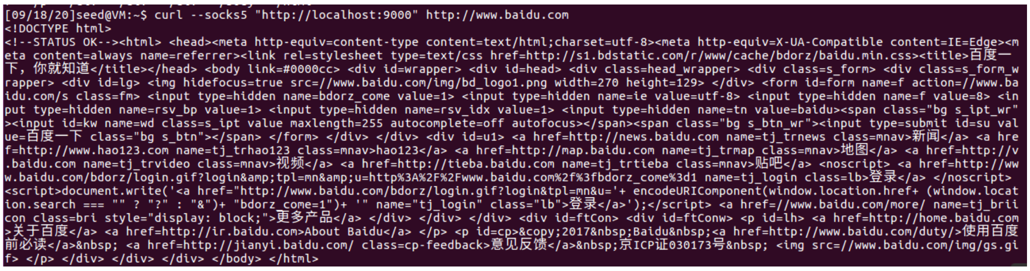
Task 3.b: Connect to Facebook using SSH Tunnel

- `ssh` to machine B



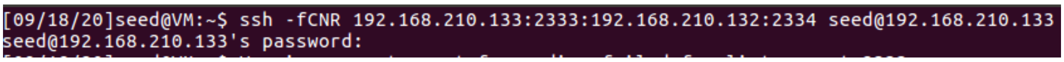
```
[09/18/20]seed@VM:~$ ssh -D 9000 -C seed@192.168.210.133
seed@192.168.210.133's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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: Fri Sep 18 05:31:25 2020 from bogon
```

- Visit www.baidu.com successfully



```
[09/18/20]seed@VM:~$ curl --socks5 "http://localhost:9000" http://www.baidu.com
<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-type content=text/html;charset=utf-8><meta http-equiv=X-UA-Compatible content=IE=Edge><m
eta content=always name=referrer><link rel=stylesheet type=text/css href=http://s1.bdstatic.com/r/www/cache/bdorz/baidu.min.css><title>百度一
下，你就知道</title></head> <body link=#0000cc> <div id=wrapper> <div id=head> <div class=head_wrapper> <div class=s_form> <div class=s_form_w
rapper> <div id=lg> <img hidefocus=true src=//www.baidu.com/img/bd_logo1.png width=270 height=129> </div> <form id=form name=f action=//www.ba
idu.com/s class=fm> <input type=hidden name=bdorz_come value=1> <input type=hidden name=ie value=utf-8> <input type=hidden name=f value=8> <in
put type=hidden name=rsv_bp value=1> <input type=hidden name=rsv_idx value=1> <input type=hidden name=tn value=baidu><span class="bg s_ipt_wr"
><input id=kw name=wd class=s_ipt value maxlength=255 autocomplete=off autofocus></span><span class="bg s_btn_wr"><input type=submit id=su val
ue=百度一下 class="bg s_btn"></span> </form> </div> </div> <div id=u1> <a href=http://news.baidu.com name=tj_trnews class=mnav>新闻</a> <a hre
f=http://www.hao123.com name=tj_trhao123 class=mnav>hao123</a> <a href=http://map.baidu.com name=tj_trmap class=mnav>地图</a> <a href=http://v
.baidu.com name=tj_trvideo class=mnav>视频</a> <a href=http://tieba.baidu.com name=tj_trtieba class=mnav>贴吧</a> <noscript> <a href=http://ww
w.baidu.com/bdorz/login.gif?login&amp;tpl=mn&amp;u=http%3A%2F%2Fwww.baidu.com%2f%3fbdorz_come%3d1 name=tj_login class=lb>登录</a> </noscript>
<script>document.write('<a href="http://www.baidu.com/bdorz/login.gif?login&tpl=mn&u='+ encodeURIComponent(window.location.href+ (window.locat
ion.search === "" ? "?" : "&")+ "bdorz_come=1")+ '" name="tj_login" class="lb">登录</a>');</script> <a href=//www.baidu.com/more/ name=tj_brii
con class=bri style="display: block;">更多产品</a> </div> </div> </div> <div id=ftCon> <div id=ftConw> <p id=lh> <a href=http://home.baidu.com
>关于百度</a> <a href=http://ir.baidu.com>About Baidu</a> </p> <p id=cp>&copy;2017&nbsp;Baidu&nbsp;<a href=http://www.baidu.com/duty/>使用百度
前必读</a>&nbsp; <a href=http://jianyi.baidu.com/ class=cp-feedback>意见反馈</a>&nbsp;京ICP证030173号&nbsp; <img src=//www.baidu.com/img/gs.gi
f> </p> </div> </div> </div> </body> </html>
```

Task4: Evading Ingress Filtering



```
[09/18/20]seed@VM:~$ ssh -fCNR 192.168.210.133:2333:192.168.210.132:2334 seed@192.168.210.133
seed@192.168.210.133's password:
```