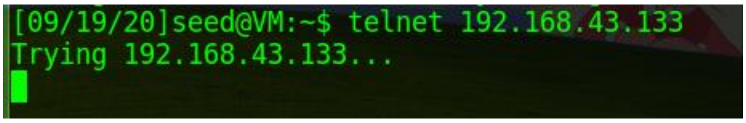
主机 A 192.168.43.132

主机 B 192.168.43.133

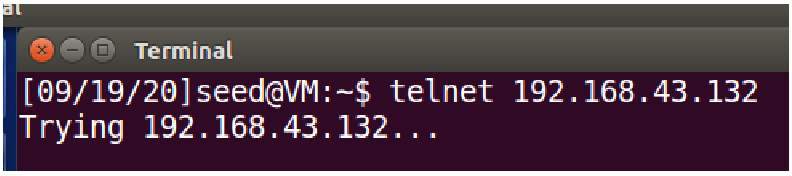
Task1

阻止 A 连 B



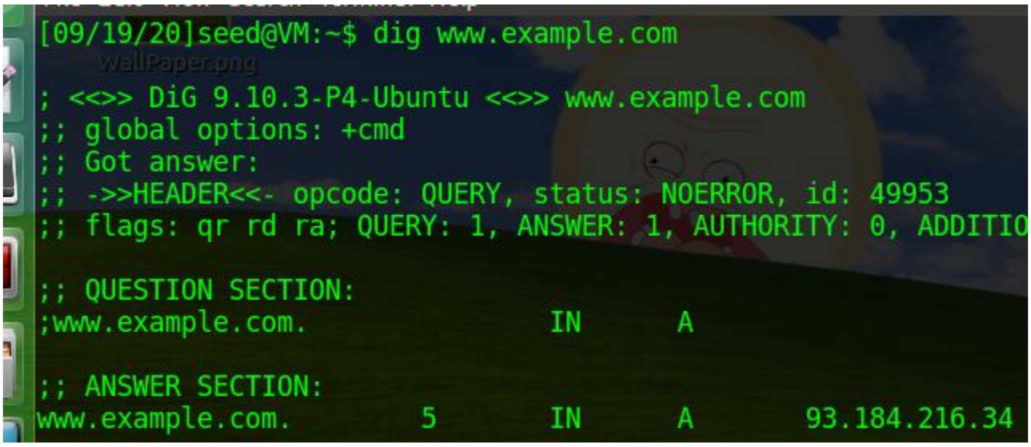
```
[09/19/20]seed@VM:~$ telnet 192.168.43.133
Trying 192.168.43.133...
```

阻止 B 连 A

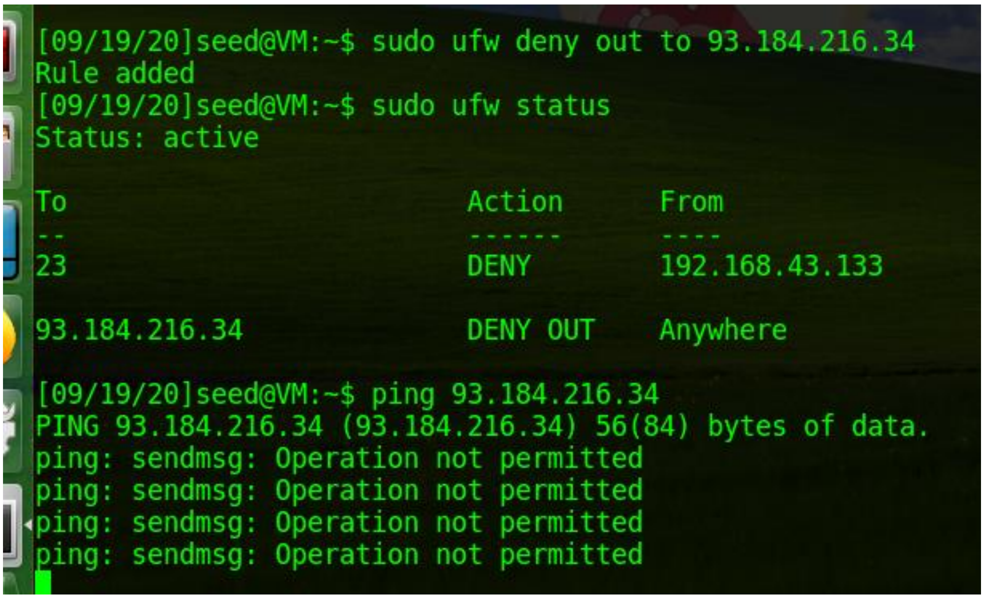


```
[09/19/20]seed@VM:~$ telnet 192.168.43.132
Trying 192.168.43.132...
```

阻止连 example.com

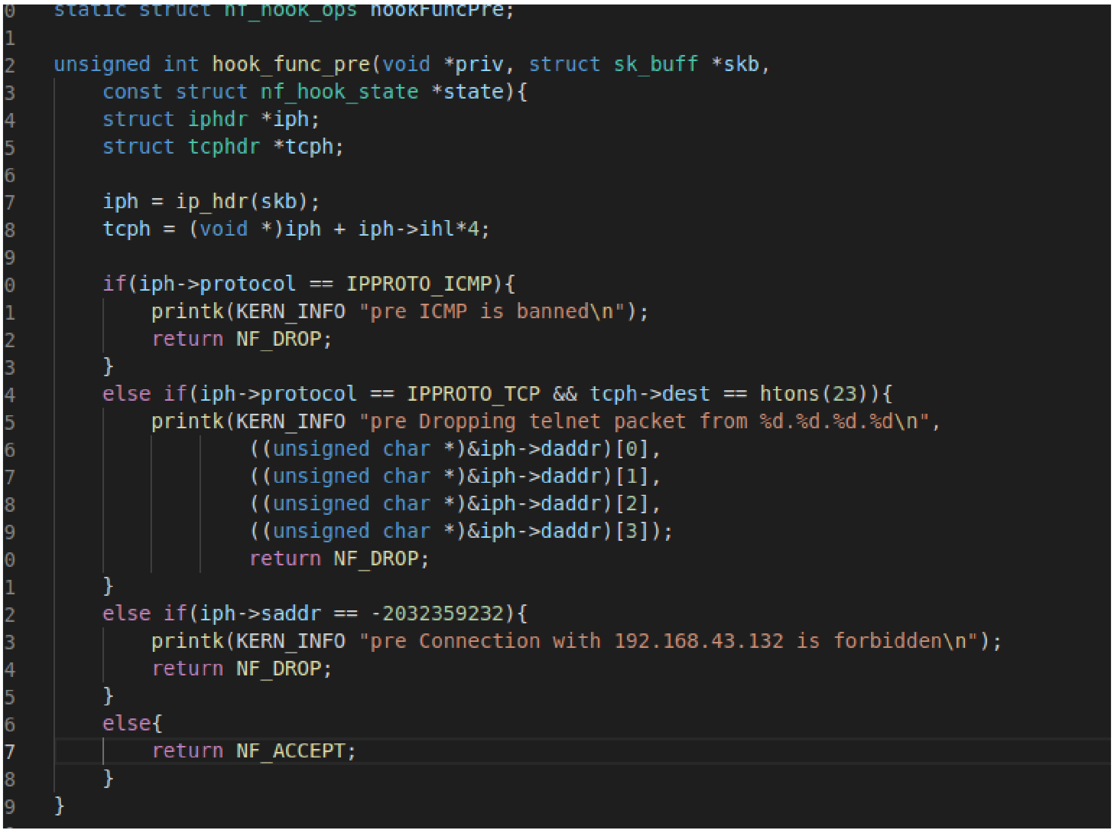


```
[09/19/20]seed@VM:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49953
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIO

;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        5       IN      A       93.184.216.34
```

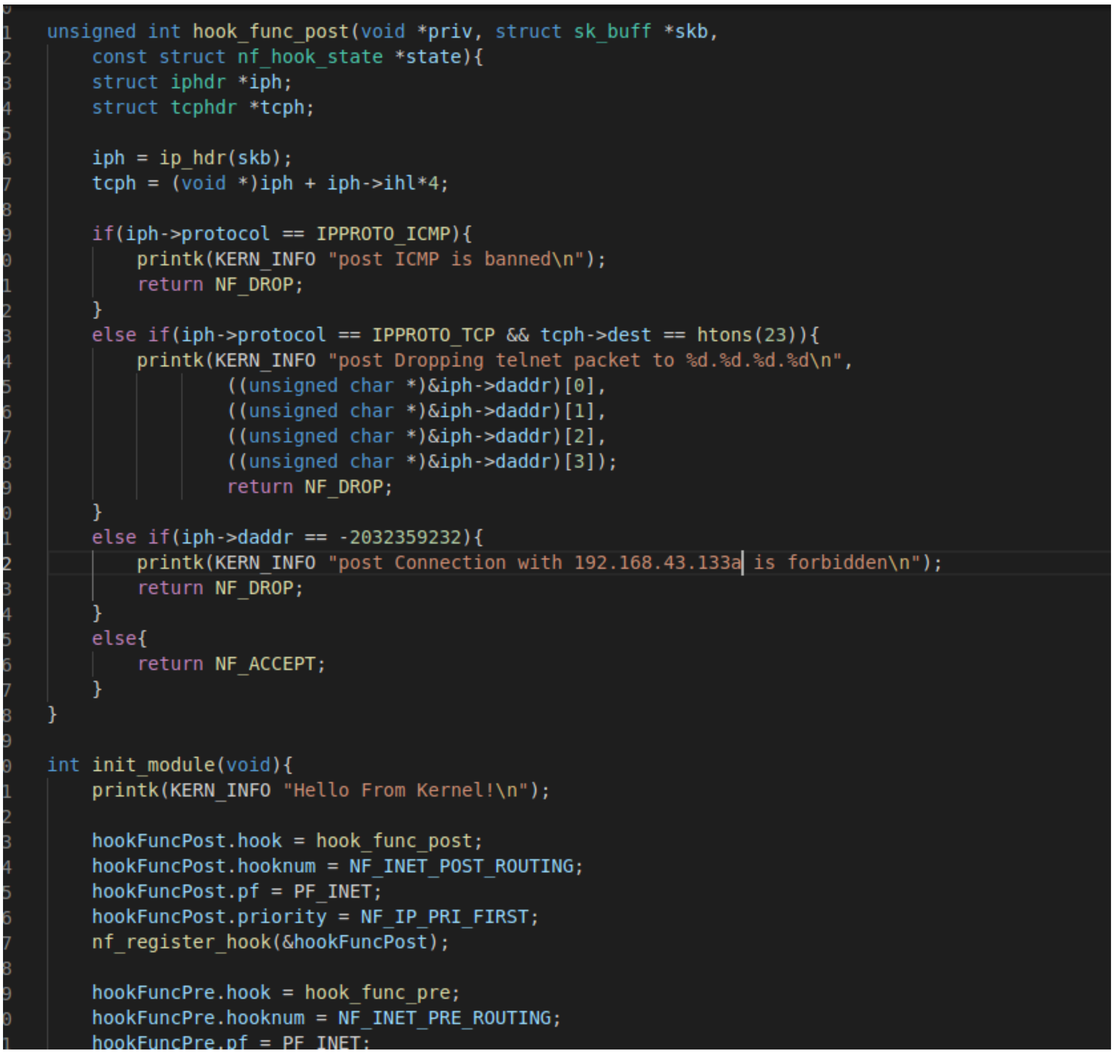


```
[09/19/20]seed@VM:~$ sudo ufw deny out to 93.184.216.34
Rule added
[09/19/20]seed@VM:~$ sudo ufw status
Status: active

To                          Action      From
--                          ------      ----
23                          DENY        192.168.43.133

93.184.216.34               DENY OUT    Anywhere

[09/19/20]seed@VM:~$ ping 93.184.216.34
PING 93.184.216.34 (93.184.216.34) 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
```

Task2

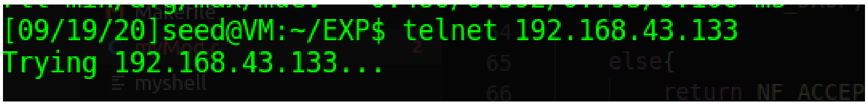


```c
static struct nf_hook_ops hookFuncPre;

unsigned int hook_func_pre(void *priv, struct sk_buff *skb,
    const struct nf_hook_state *state){
    struct iphdr *iph;
    struct tcphdr *tcph;

    iph = ip_hdr(skb);
    tcph = (void *)iph + iph->ihl*4;

    if(iph->protocol == IPPROTO_ICMP){
        printk(KERN_INFO "pre ICMP is banned\n");
        return NF_DROP;
    }
    else if(iph->protocol == IPPROTO_TCP && tcph->dest == htons(23)){
        printk(KERN_INFO "pre Dropping telnet packet from %d.%d.%d.%d\n",
                ((unsigned char *)&iph->daddr)[0],
                ((unsigned char *)&iph->daddr)[1],
                ((unsigned char *)&iph->daddr)[2],
                ((unsigned char *)&iph->daddr)[3]);
                return NF_DROP;
    }
    else if(iph->saddr == -2032359232){
        printk(KERN_INFO "pre Connection with 192.168.43.132 is forbidden\n");
        return NF_DROP;
    }
    else{
        return NF_ACCEPT;
    }
}
```

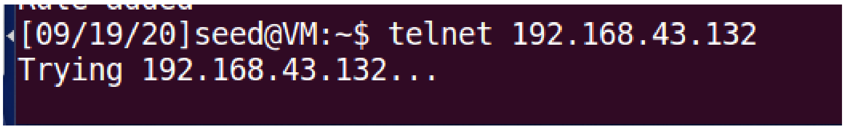


```c
unsigned int hook_func_post(void *priv, struct sk_buff *skb,
    const struct nf_hook_state *state){
    struct iphdr *iph;
    struct tcphdr *tcph;

    iph = ip_hdr(skb);
    tcph = (void *)iph + iph->ihl*4;

    if(iph->protocol == IPPROTO_ICMP){
        printk(KERN_INFO "post ICMP is banned\n");
        return NF_DROP;
    }
    else if(iph->protocol == IPPROTO_TCP && tcph->dest == htons(23)){
        printk(KERN_INFO "post Dropping telnet packet to %d.%d.%d.%d\n",
                ((unsigned char *)&iph->daddr)[0],
                ((unsigned char *)&iph->daddr)[1],
                ((unsigned char *)&iph->daddr)[2],
                ((unsigned char *)&iph->daddr)[3]);
                return NF_DROP;
    }
    else if(iph->daddr == -2032359232){
        printk(KERN_INFO "post Connection with 192.168.43.133a is forbidden\n");
        return NF_DROP;
    }
    else{
        return NF_ACCEPT;
    }
}

int init_module(void){
    printk(KERN_INFO "Hello From Kernel!\n");

    hookFuncPost.hook = hook_func_post;
    hookFuncPost.hooknum = NF_INET_POST_ROUTING;
    hookFuncPost.pf = PF_INET;
    hookFuncPost.priority = NF_IP_PRI_FIRST;
    nf_register_hook(&hookFuncPost);

    hookFuncPre.hook = hook_func_pre;
    hookFuncPre.hooknum = NF_INET_PRE_ROUTING;
    hookFuncPre.pf = PF_INET;
```

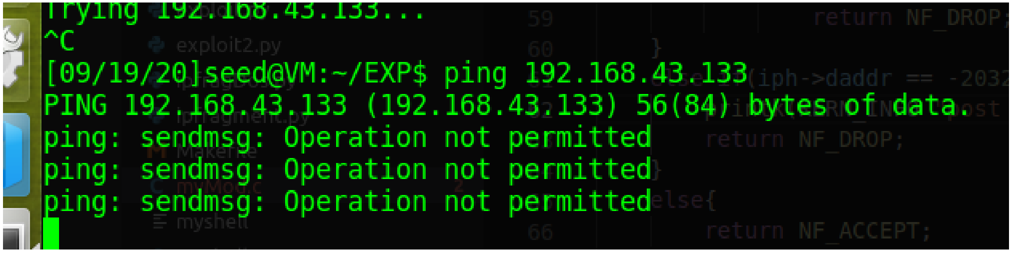
如上图：禁止了本机被 telnet 链接，本机发出 telnet 链接，禁止本机被 ICMP 访问，禁止本机与 192.168.43.133 链接



```
[09/19/20]seed@VM:~/EXP$ telnet 192.168.43.133
Trying 192.168.43.133...
```

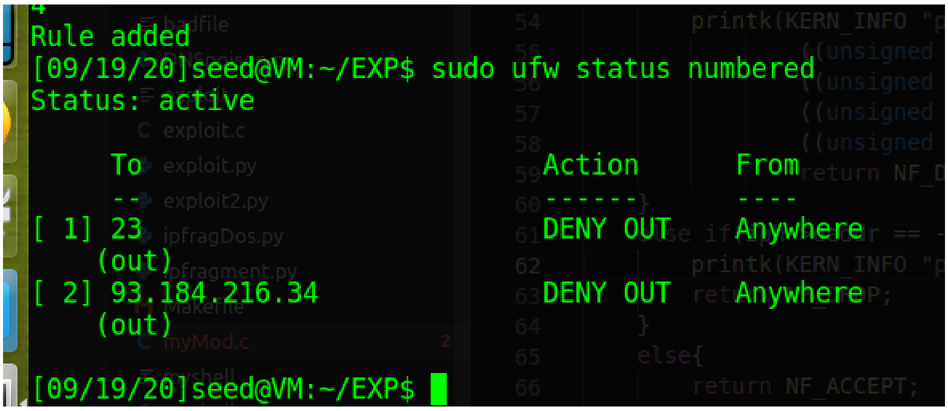


```
[09/19/20]seed@VM:~$ telnet 192.168.43.132
Trying 192.168.43.132...
```



```
Trying 192.168.43.133...
^C
[09/19/20]seed@VM:~/EXP$ ping 192.168.43.133
PING 192.168.43.133 (192.168.43.133) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

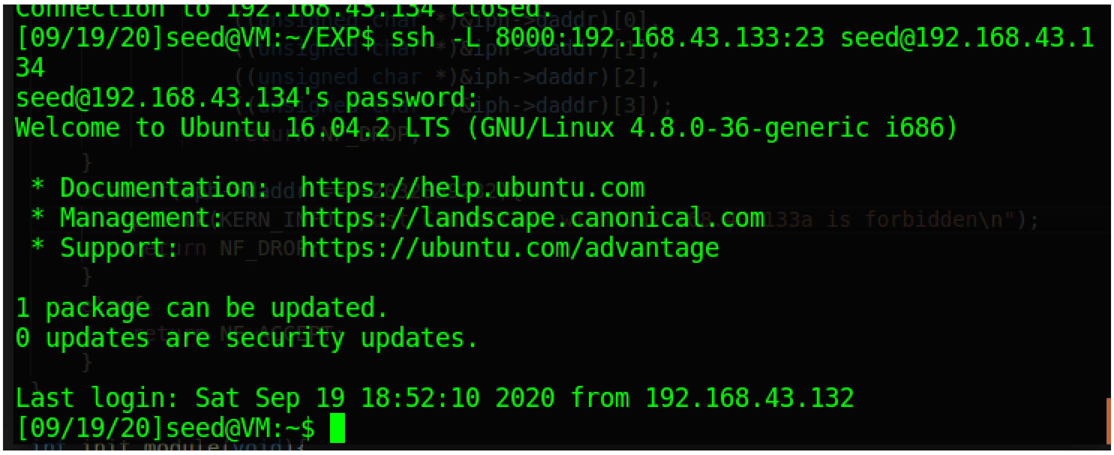
Task3



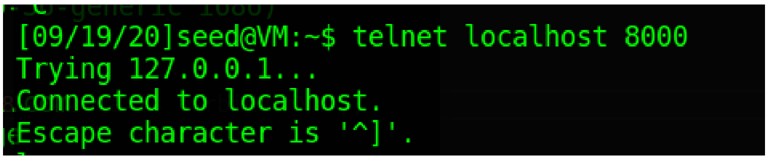
```
Rule added
[09/19/20]seed@VM:~/EXP$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY OUT    Anywhere
    (out)
[ 2] 93.184.216.34              DENY OUT    Anywhere
    (out)

[09/19/20]seed@VM:~/EXP$ 
```

阻止对 93.184.216.34 的访问

Task3a



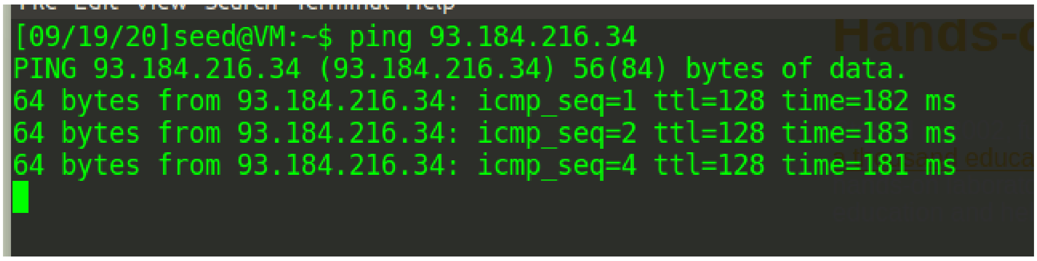
```
Connection to 192.168.43.134 closed.
[09/19/20]seed@VM:~/EXP$ ssh -L 8000:192.168.43.133:23 seed@192.168.43.1
34
seed@192.168.43.134's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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: Sat Sep 19 18:52:10 2020 from 192.168.43.132
[09/19/20]seed@VM:~$ 
```



```
[09/19/20]seed@VM:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
```

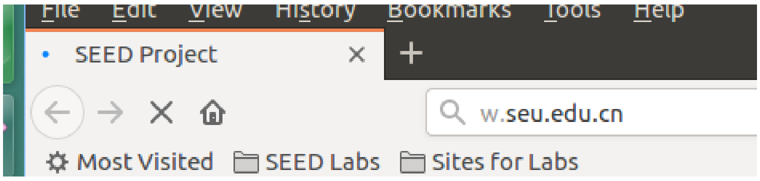
用这个指令，可以通过 8000 端口建立的 ssh 隧道绕过对 133 的 telnet

Task3b



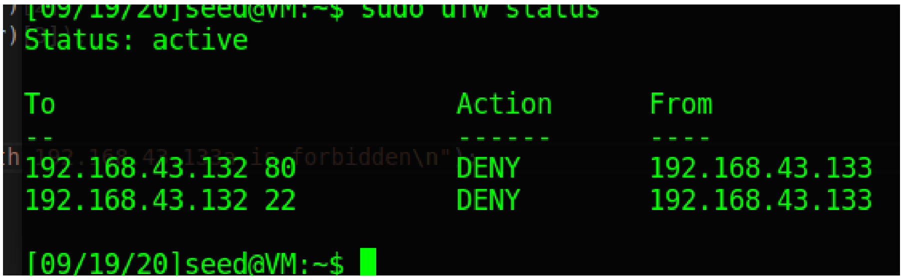
```
[09/19/20]seed@VM:~$ ping 93.184.216.34
PING 93.184.216.34 (93.184.216.34) 56(84) bytes of data.
64 bytes from 93.184.216.34: icmp_seq=1 ttl=128 time=182 ms
64 bytes from 93.184.216.34: icmp_seq=2 ttl=128 time=183 ms
64 bytes from 93.184.216.34: icmp_seq=4 ttl=128 time=181 ms
```

建立隧道后可以



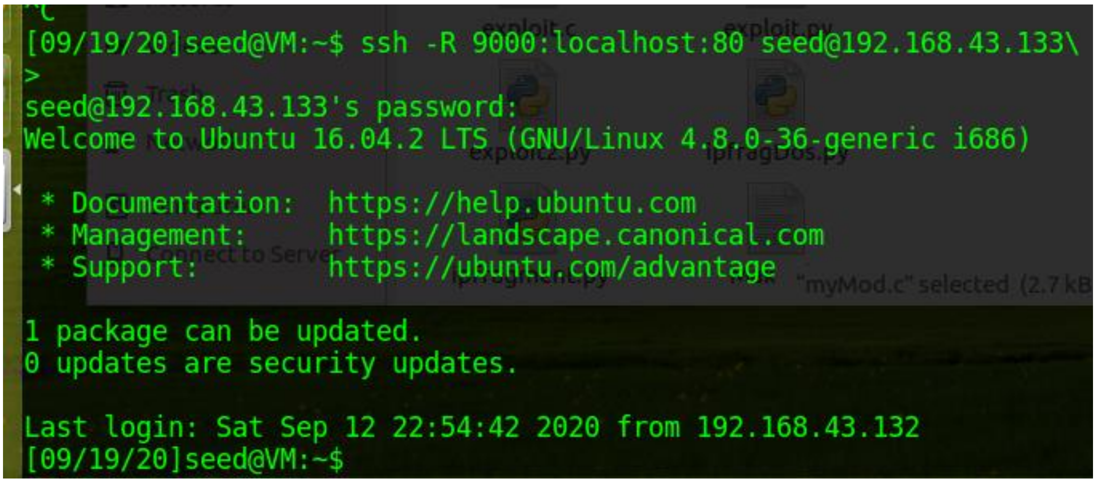
解除隧道之后无法访问

Task4

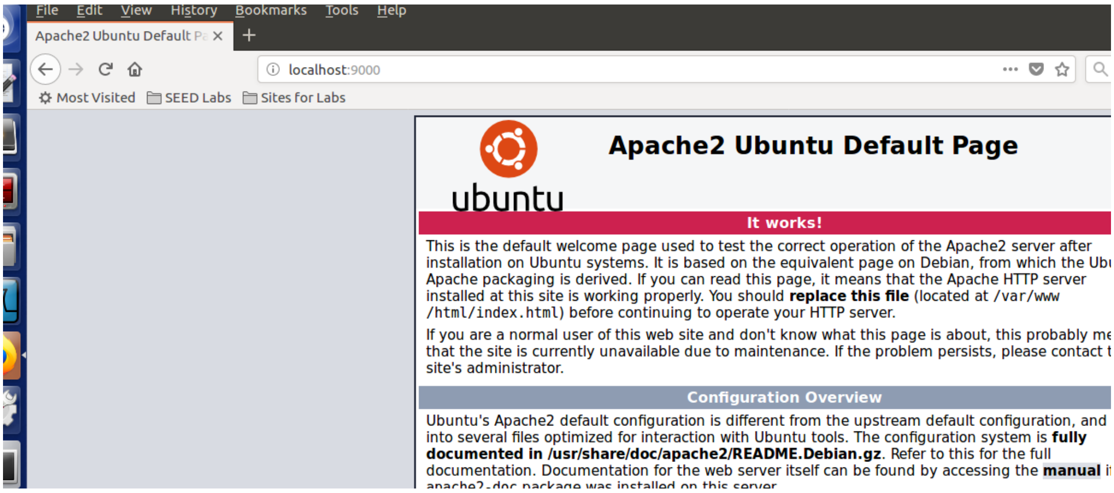


```
[09/19/20]seed@VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
192.168.43.132 80          DENY        192.168.43.133
192.168.43.132 22          DENY        192.168.43.133

[09/19/20]seed@VM:~$ 
```

阻止了 133 对本机 80 跟 22 端口的访问



```
^C
[09/19/20]seed@VM:~$ ssh -R 9000:localhost:80 seed@192.168.43.133\
>
seed@192.168.43.133'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: Sat Sep 12 22:54:42 2020 from 192.168.43.132
[09/19/20]seed@VM:~$
```



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www /html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably me that the site is currently unavailable due to maintenance. If the problem persists, please contact t site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** i apache2-doc package was installed on this server.

在主机二访问 localhost：9000 到 Apache 页面说明反向链接成功。