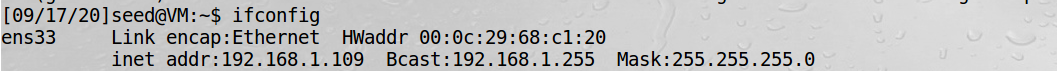
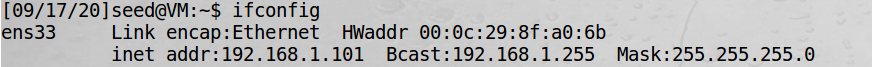
# Linux Firewall Exploration Lab

57117217戚吴祺

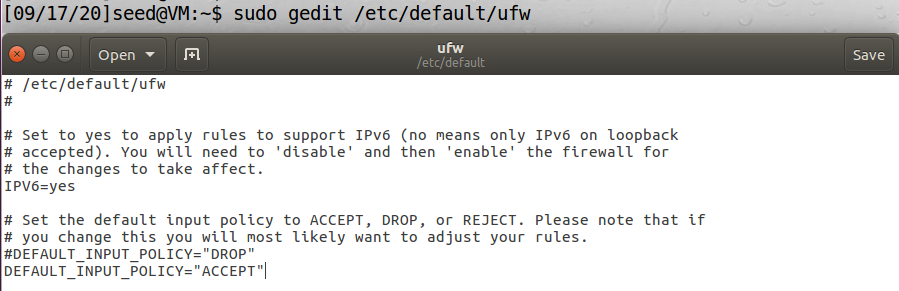
Machine A：

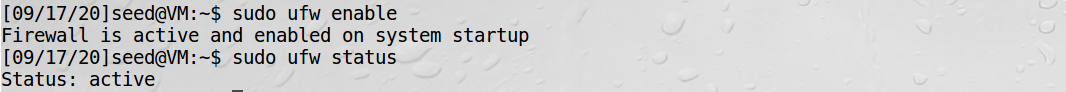


Machine B：

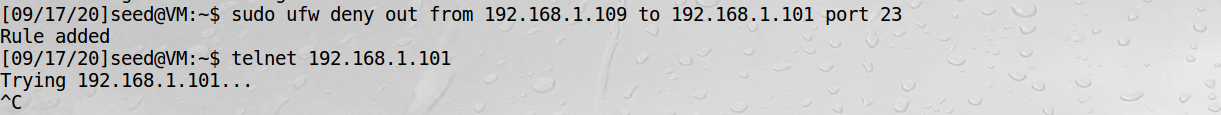


## Task 1: Using Firewall



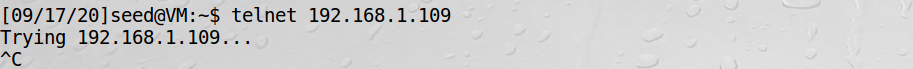


Prevent A from doing telnet to Machine B.

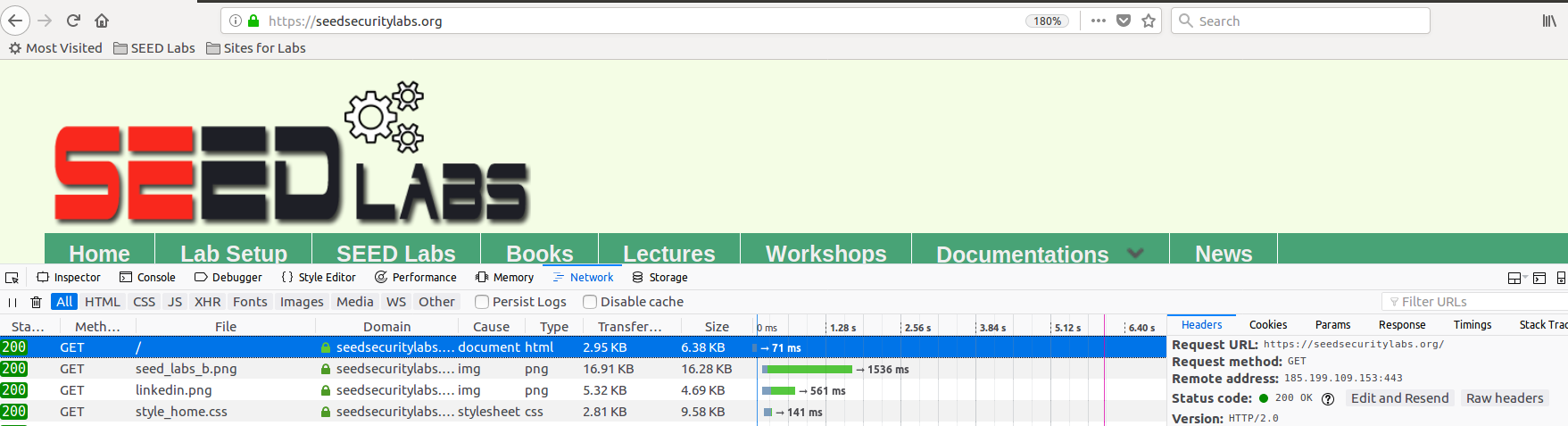


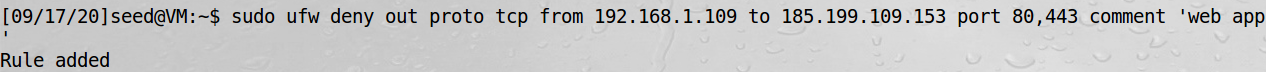
Prevent B from doing telnet to Machine A.





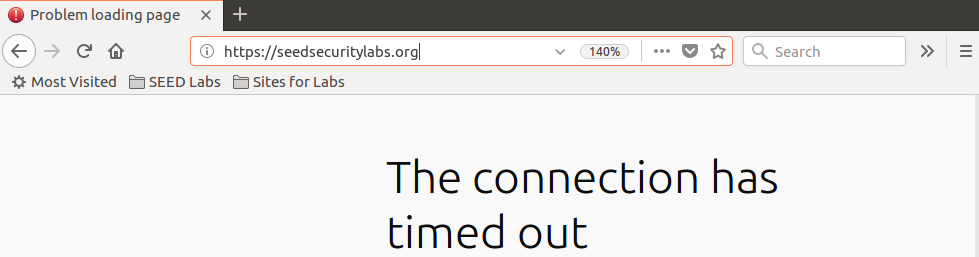
Prevent A from visiting an external web site.



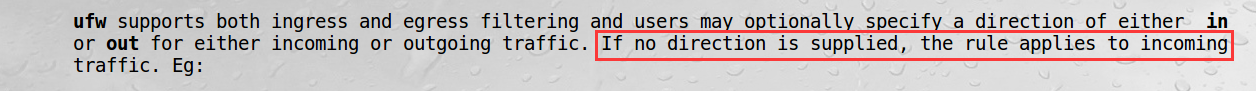


这条规则不知道为啥没起作用。干脆用了下面一条



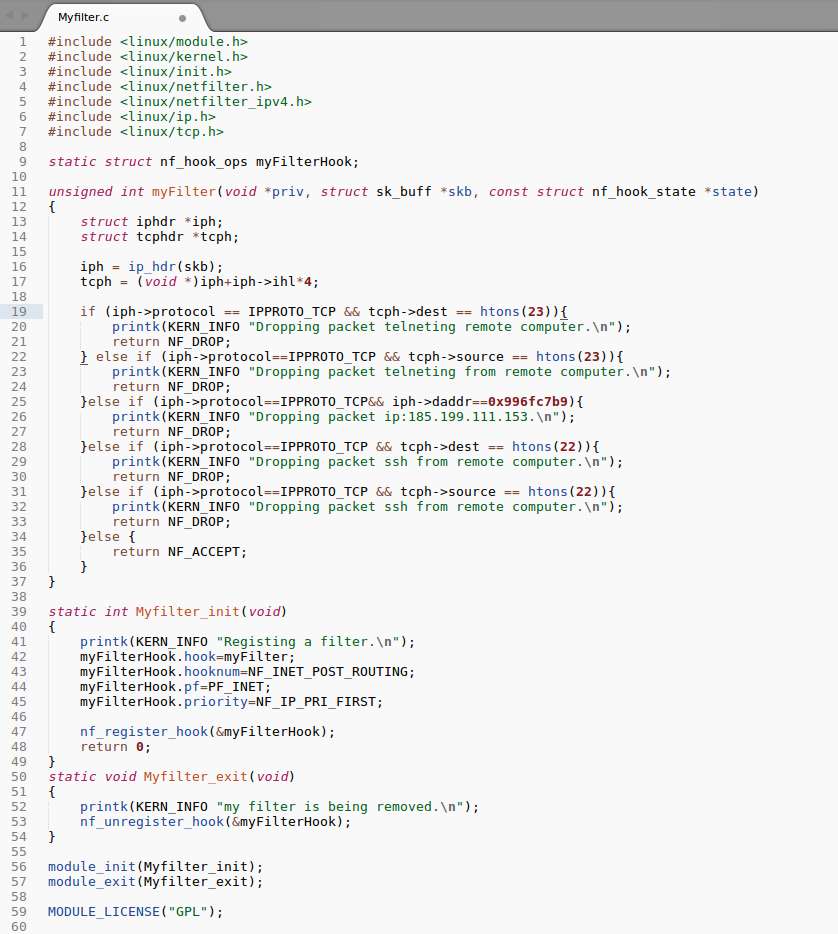


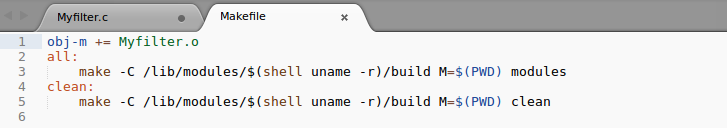
*注意:*

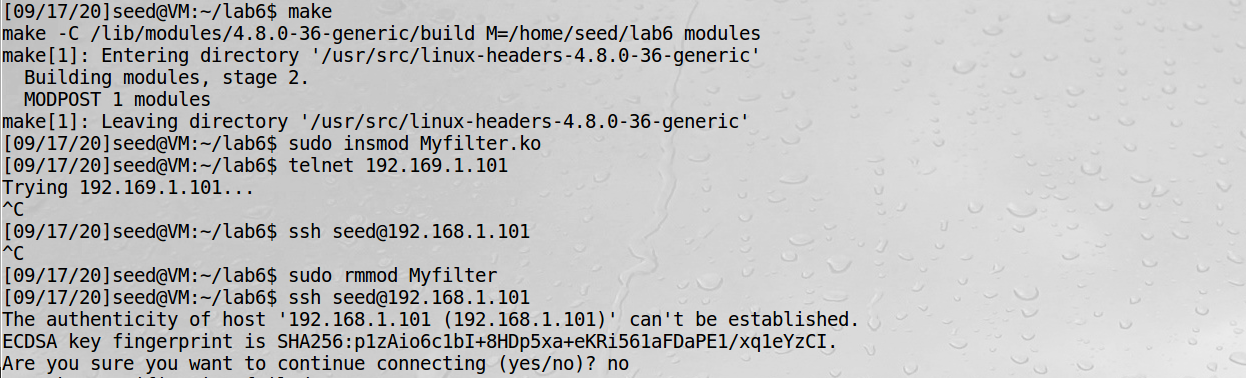
**

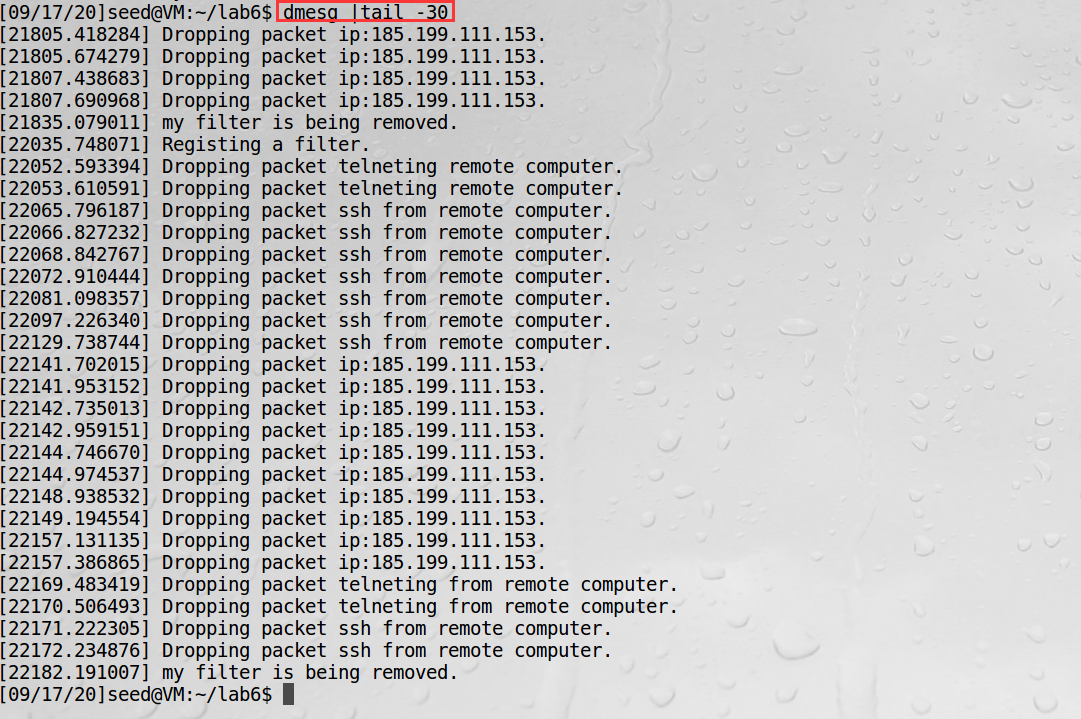
*不加 in 或者 out 默认为进入流量*

## Task 2: Implementing a Simple Firewall







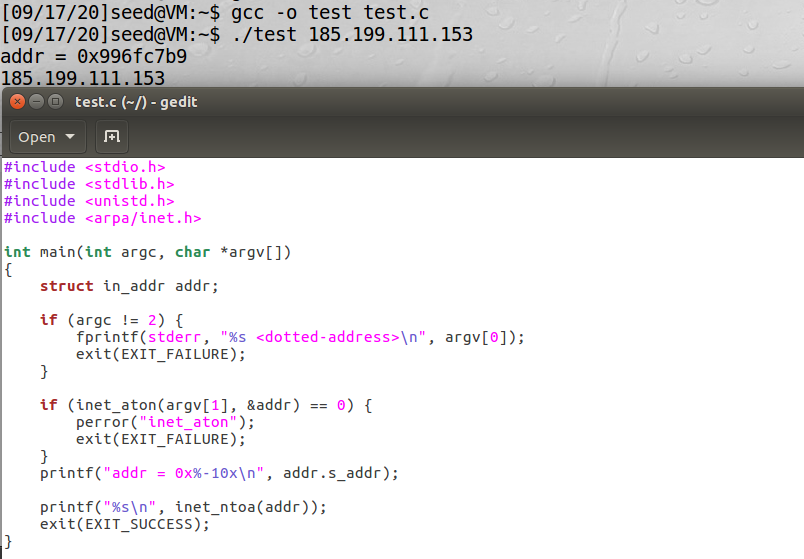


*注意：*

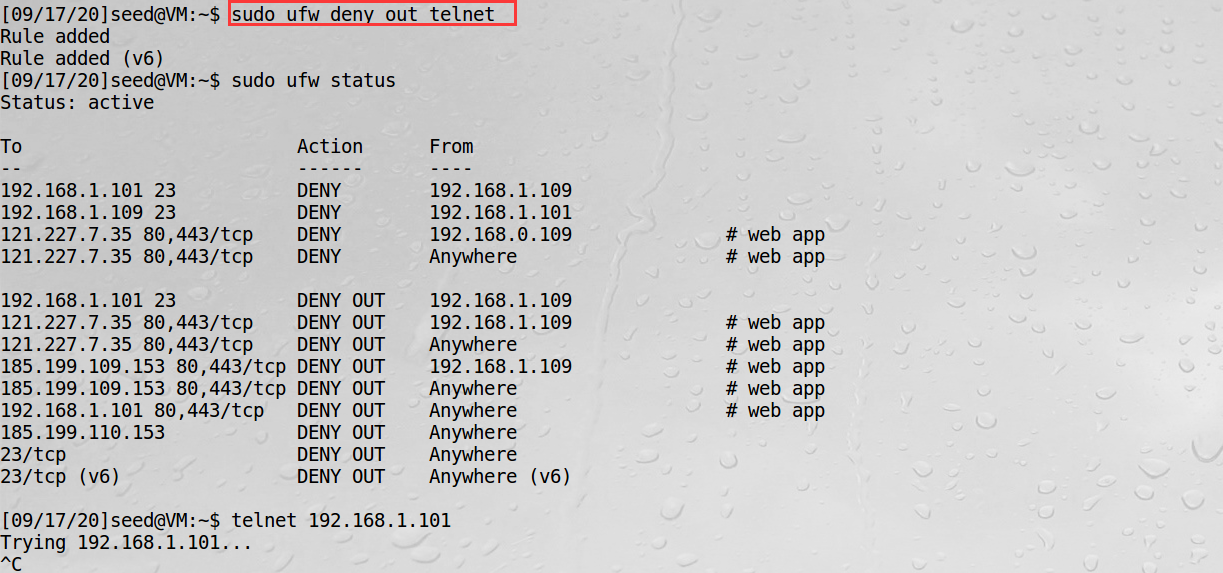
*封锁的网址* [*https://seedsecuritylabs.org/*](https://seedsecuritylabs.org/) *具有多个ip*

*185.199.111.153/185.199.110.153/185.199.109.153/185.199.108.153*

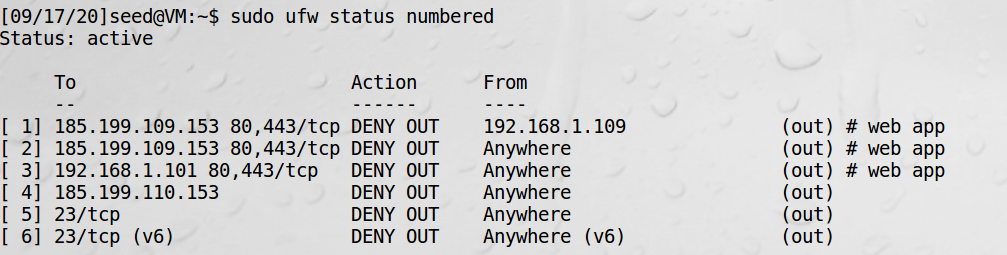
*Ip地址 用到了 inet\_addr函数*



## Task 3: Evading Egress Filtering

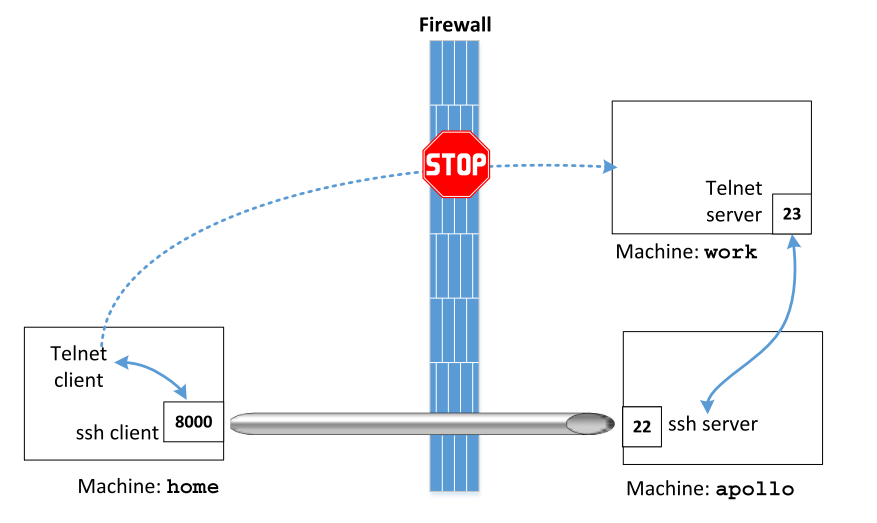


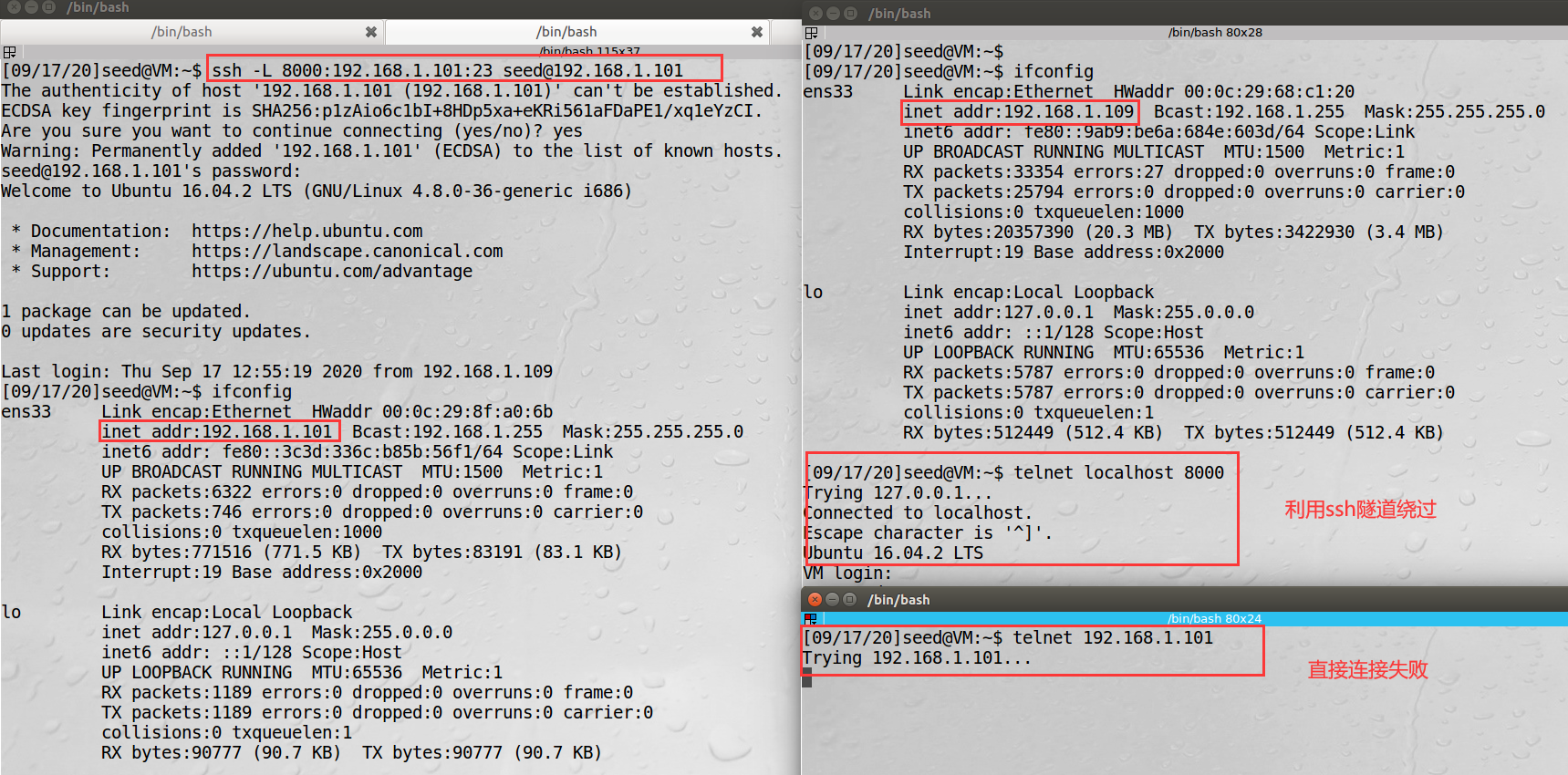
After deleting some rules:



Block <https://seedsecuritylabs.org/>

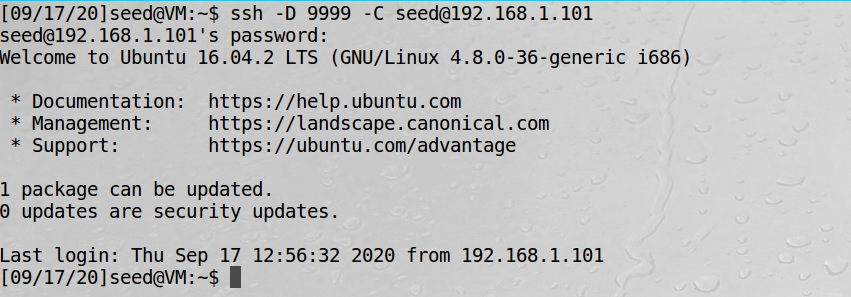
#### Task 3.a: Telnet to Machine B through the firewall





#### Task 3.b: Connect to website using SSH Tunnel.

Block <https://seedsecuritylabs.org/>



1. Run Firefox and go visit the Facebook page. Can you see the Facebook page? Please describe your observation.

YES



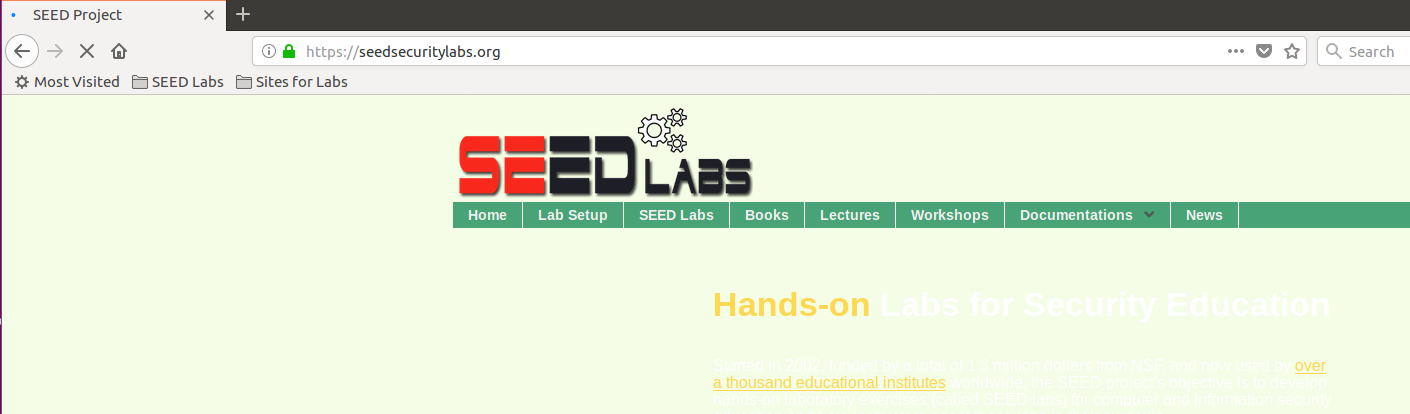
1. After you get the facebook page, break the SSH tunnel, clear the Firefox cache, and try the connection again. Please describe your observation.

Ssh断了 ， 代理就断了

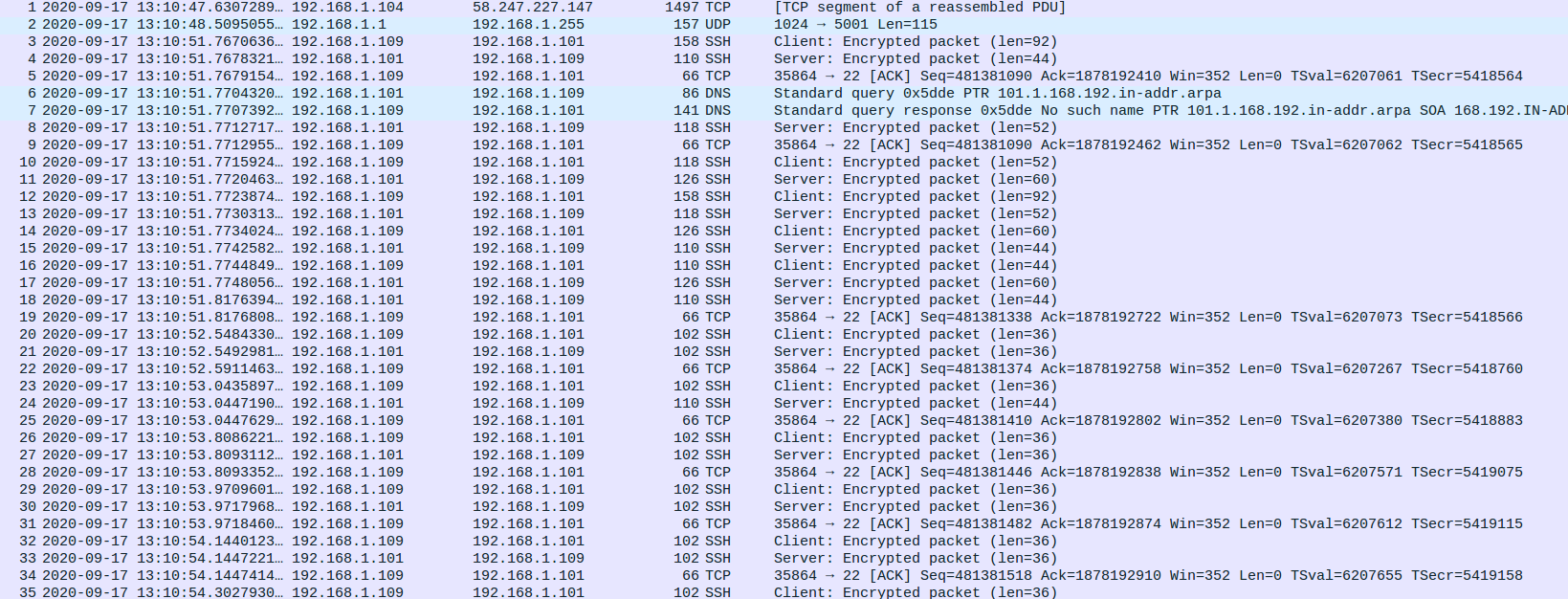


1. Establish the SSH tunnel again and connect to Facebook. Describe your observation.

重新连接成功



1. Please explain what you have observed, especially on why the SSH tunnel can help bypass the egress filtering. You should use Wireshark to see what exactly is happening on the wire. Please describe your observations and explain them using the packets that you have captured.



流量被代理转发了

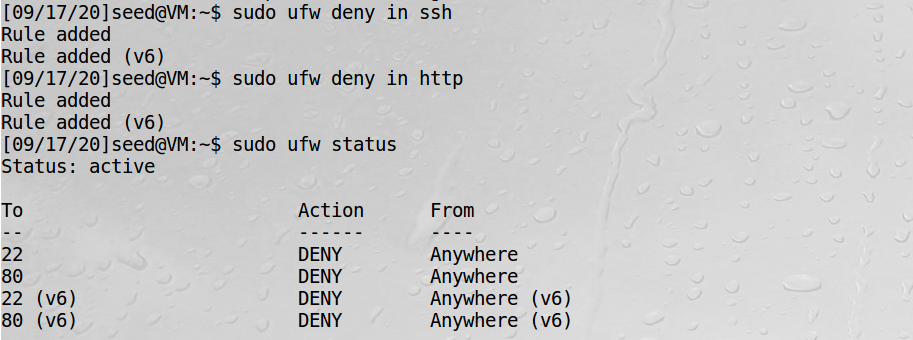
-L port:host:hostport

将本地机(客户机)的某个端口转发到远端指定机器的指定端口. 工作原理是这样的, 本地机器上分配了一个 socket 侦听 port 端口, 一旦这个端口上有了连接, 该连接就经过安全通道转发出去, 同时远程主机和 host 的 hostport 端口建立连接.

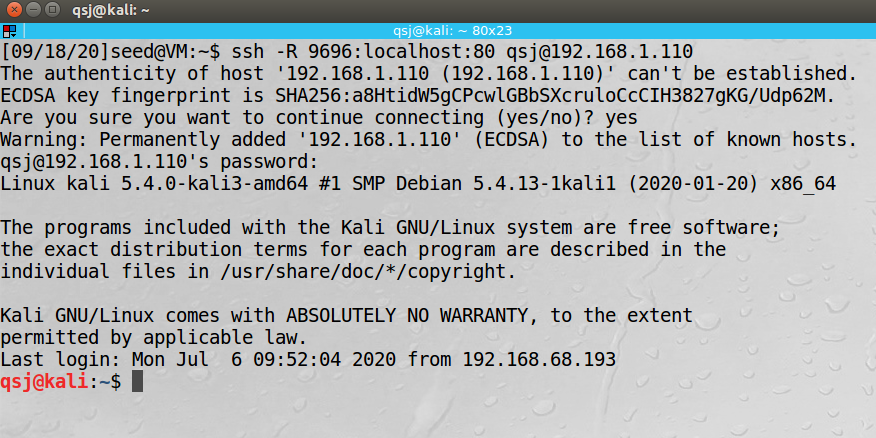
-D port

指定一个本地机器 “动态的’’ 应用程序端口转发. 工作原理是这样的, 本地机器上分配了一个 socket 侦听 port 端口, 一旦这个端口上有了连接, 该连接就经过安全通道转发出去

## Task 4: Evading Ingress Filtering



此处新增一台机器：kali 192.168.1.110，因为109主机的防火墙策略，110访问不了109的22和80端口，以下使用反向代理，访问109上受保护的网站。



Kali浏览器访问本地9696端口，即访问109的80端口

