**Lab6 Report**

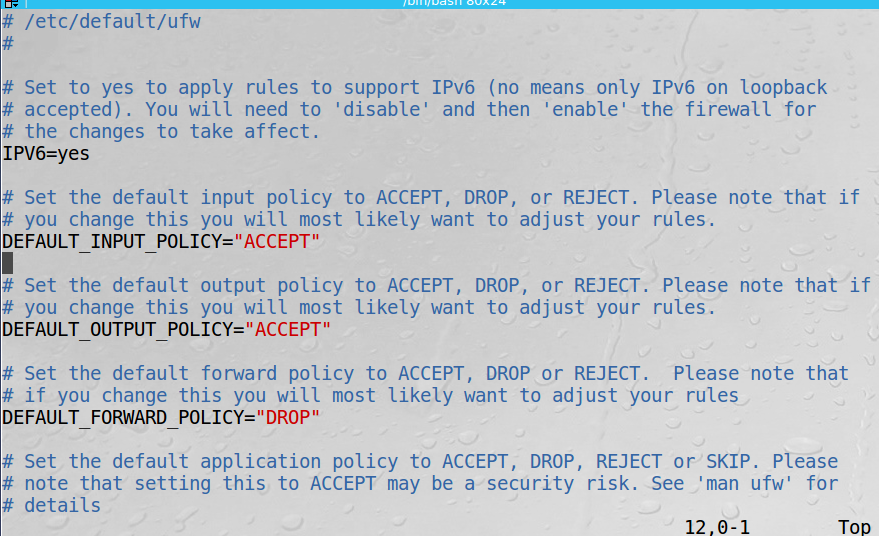
**Linux Firewall Exploration Lab**

57117107 赵笛言

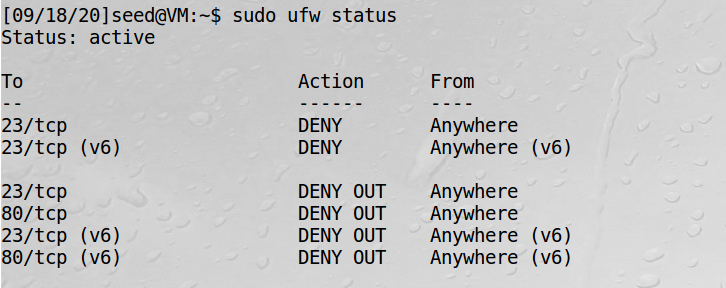
Set: A(192.168.118.153);B(192.168.118.151)

**Task1: Using Firewall**

首先将/etc/default/ufw文件中INPUT设置为默认“ACCEPT”

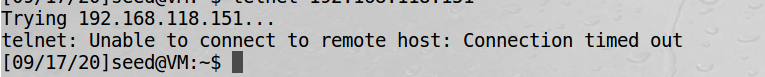


随后使用命令：ufw deny out 23/tcp；ufw deny in 23/tcp。



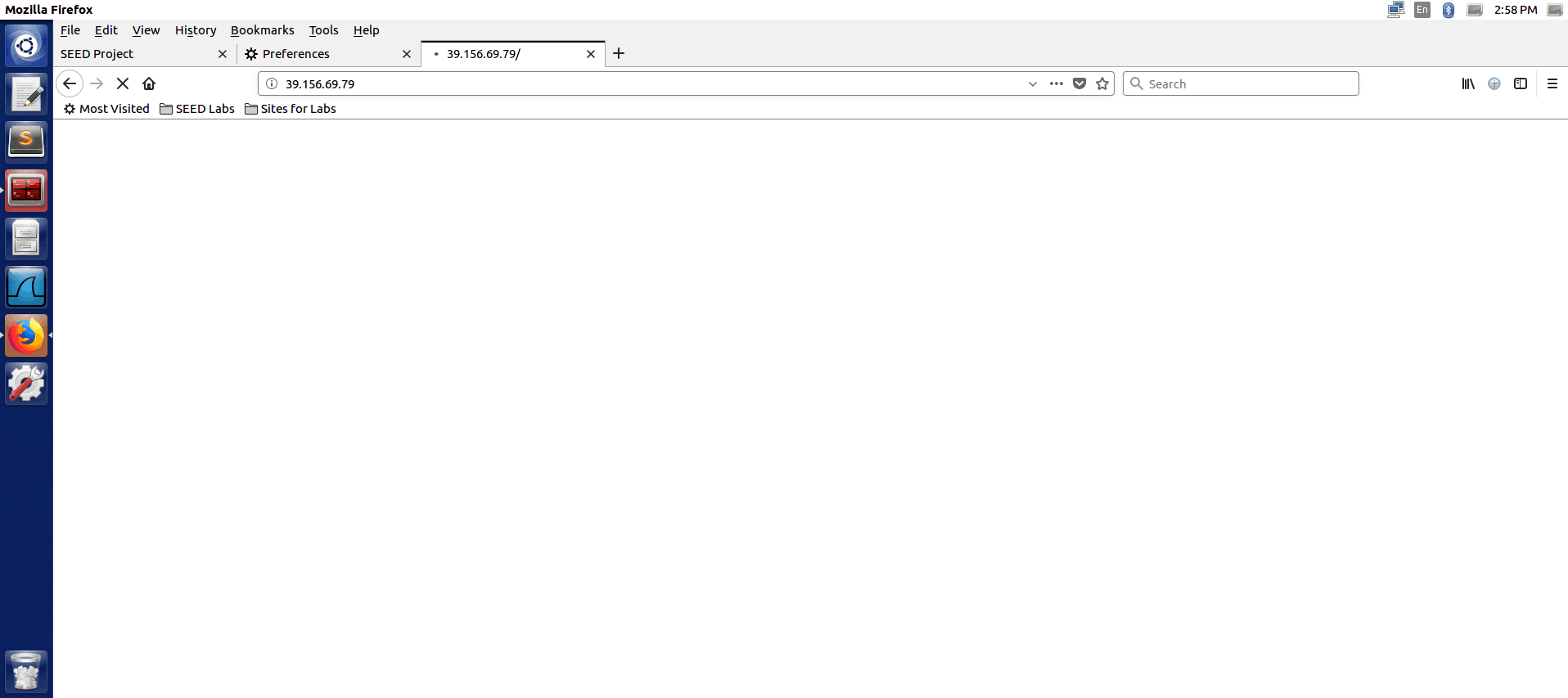
可以禁止A->B以及B<-A使用telnet服务。

结果如下，无法进行telnet连接：（A->B）



使用命令：ufw deny out 80/tcp。

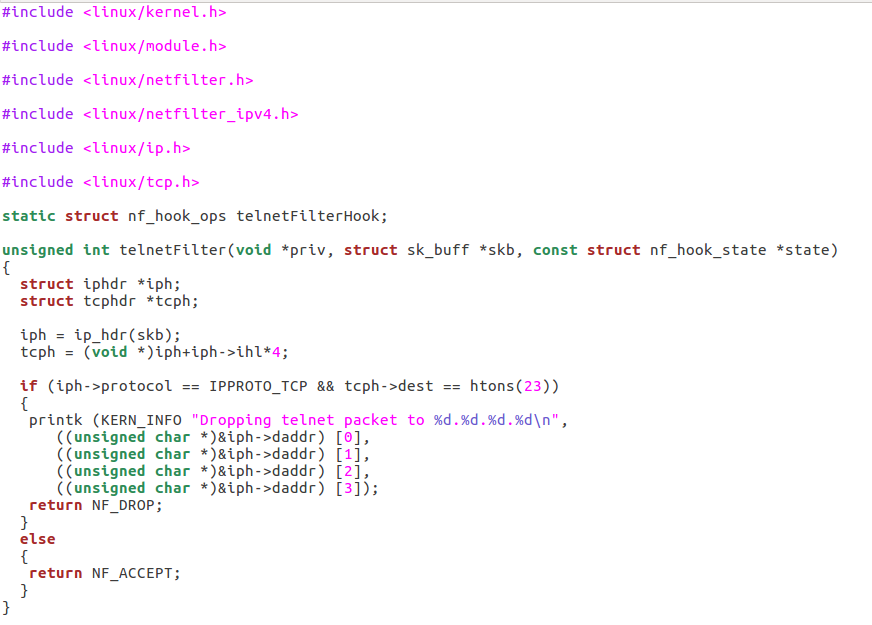
可以阻止网页访问：

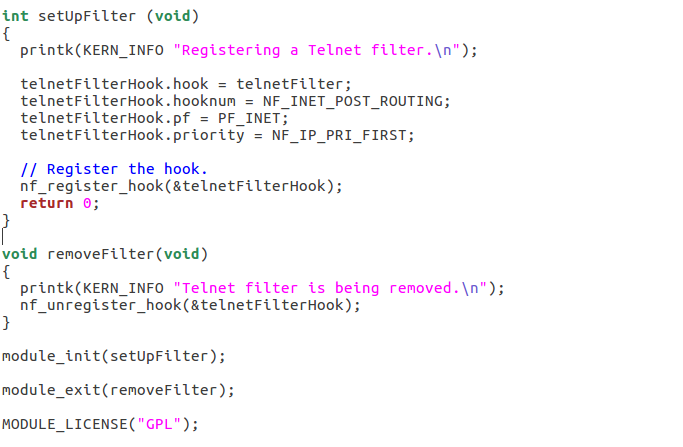


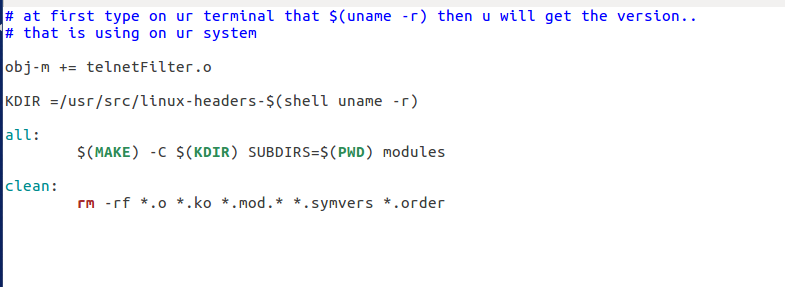
**Task2: Implementing a Simple Firewall**

使用可加载内核模块（LKM）和Netfilter进行对数据包在内核中的筛选：

首先编写Netfilter.c:





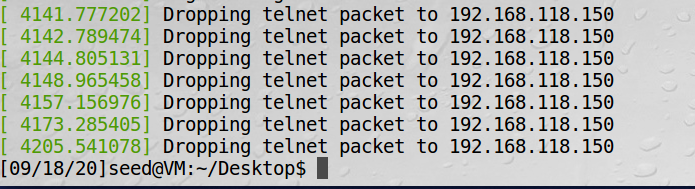
使用makefile将其加载在内核：  




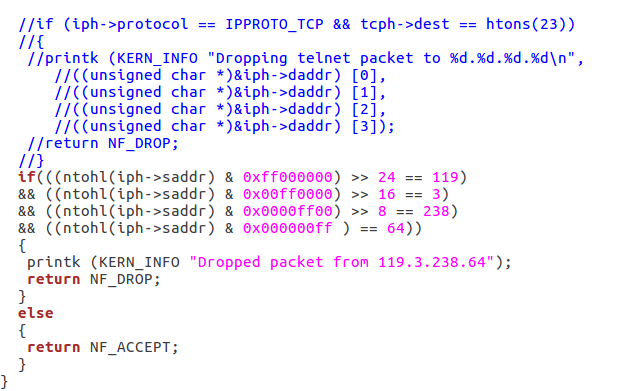
通过函数telnetFilter进行数据筛选。

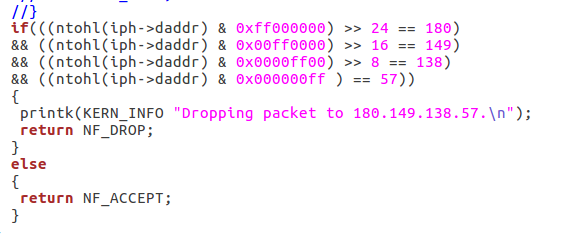
分别进行：

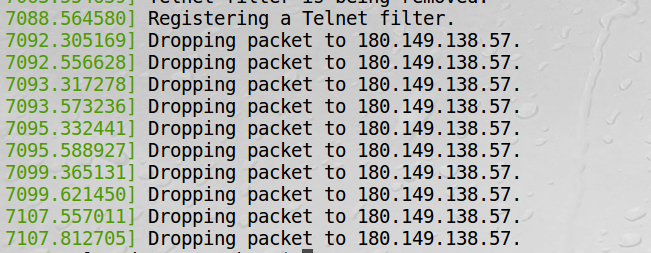
1. 禁止telnet连接。



1. 禁止访问weibo/Taobao/bilibili等网页（截图不完整）

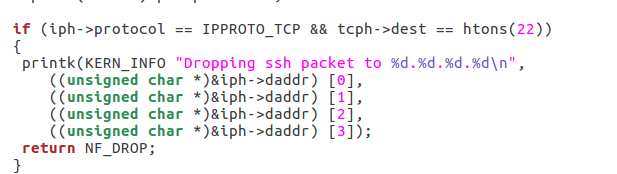


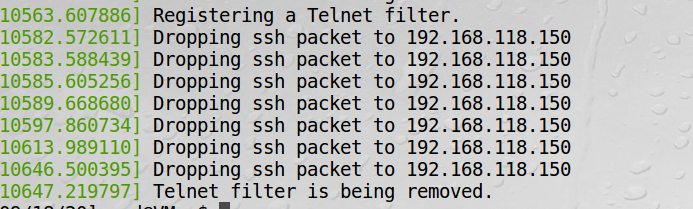




此处需要注意，这些常用高流量网络都不止一个ip地址，需要在防火墙中全部设置。还有比较神奇的是dig出来只有一个ip地址，禁止访问可以成功一小段时间，隔一段时间再次实验就又出现了可连接的新的ip。

1. 禁止进行ssh连接。

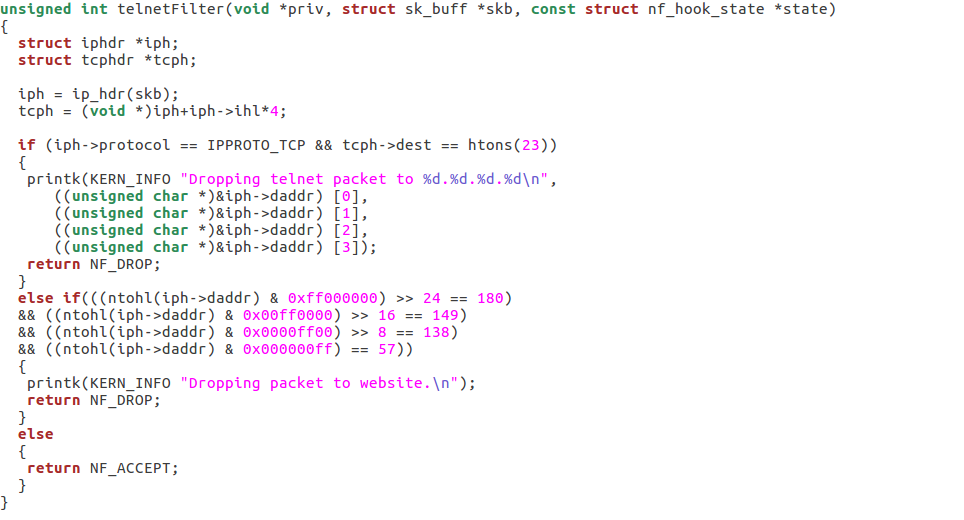




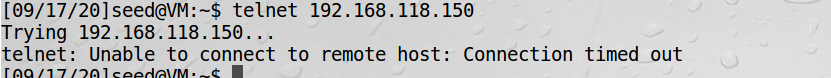


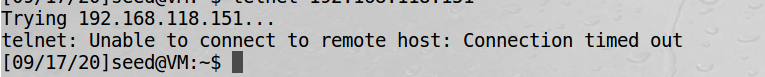
**Task3: Evading Egress Filtering**

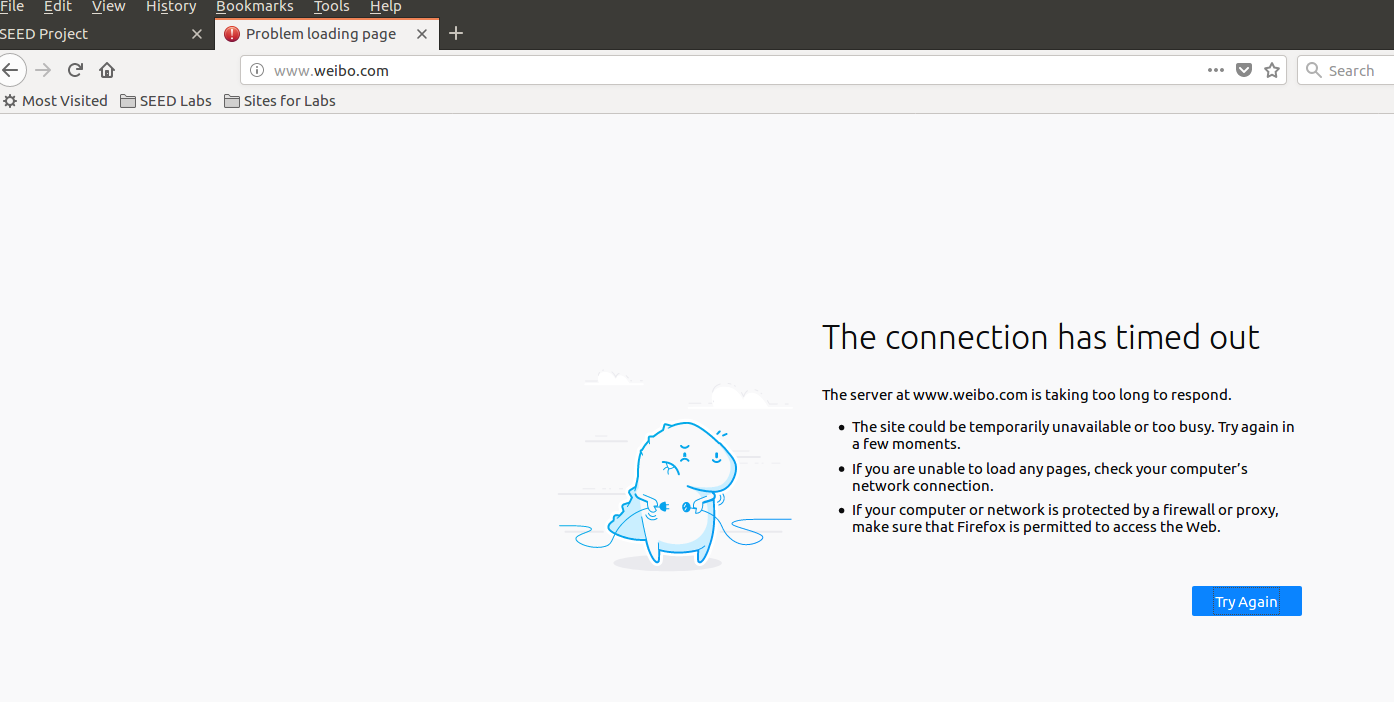
此处使用ufw更简洁，但由于当时我的主机对ufw反应迟钝无法正常进行实验，因此我使用了task2中的内核程序来进行禁用设置。



禁用telnet以及禁止网络访问。（这里出现了我刚刚提到的问题，我dig weibo.com时只有一个IP地址（180.149.138.57），修改程序测试时又成功实现了网页的禁止访问，结果等到做3.b的时候，又有新的ip地址可用来连接到微博，于是后面将实验的目标网址改成了seu.edu.cn，而此处沿用对weibo.com进行的测试写报告)

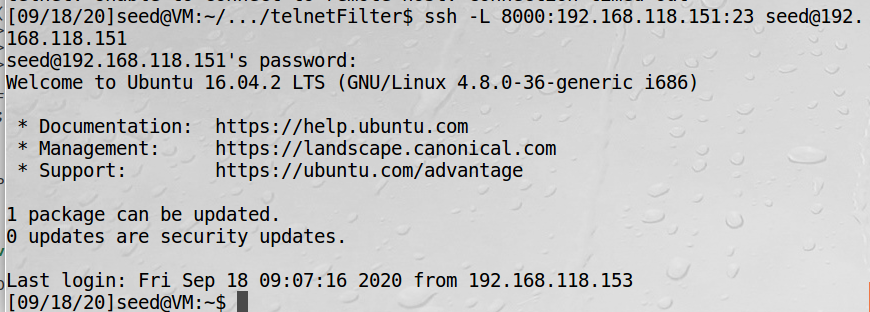




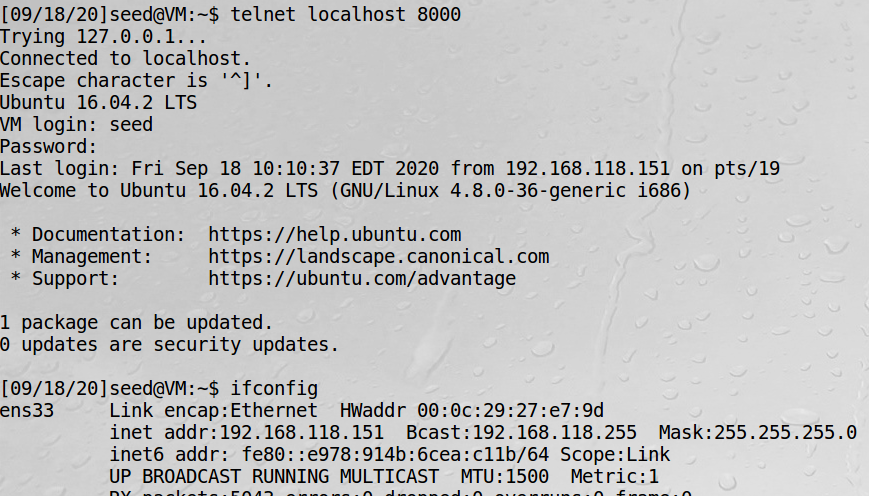


**Task 3.a: Telnet to Machine B through the Firewall**

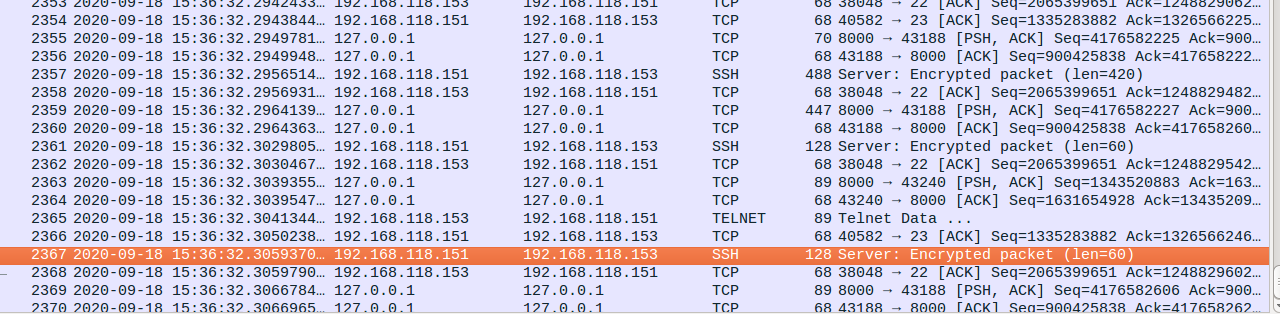
通过防火墙Telnet到计算机B要绕过防火墙，我们可以在A和B之间建立SSH隧道，因此所有的telnet流量都将通过此隧道（加密），从而避免进行检查。



连接成功：

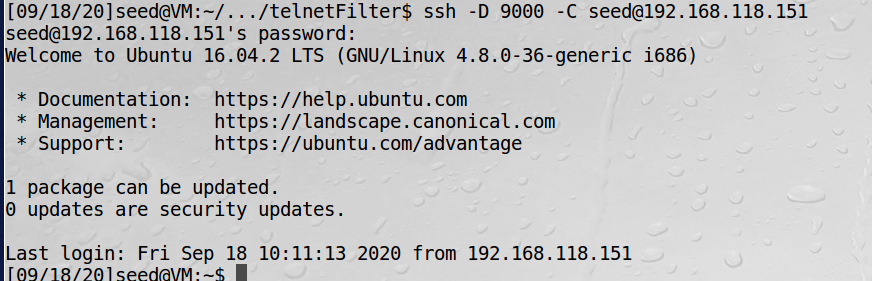


Wireshark流量如下：由隧道传送数据，不会被防火墙阻拦，数据部分实现加密处理。

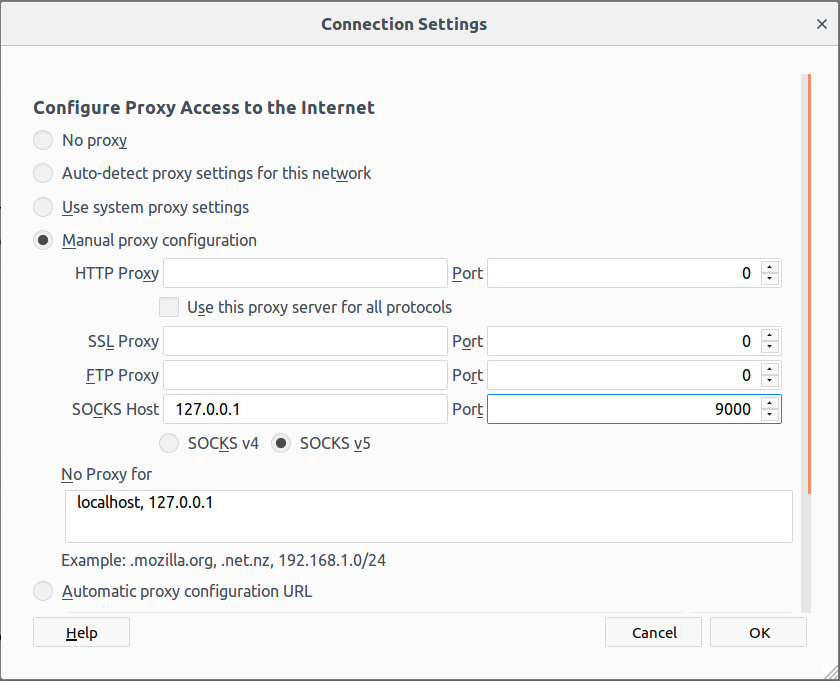


**Task 3.b: Connect to Facebook using SSH Tunnel**

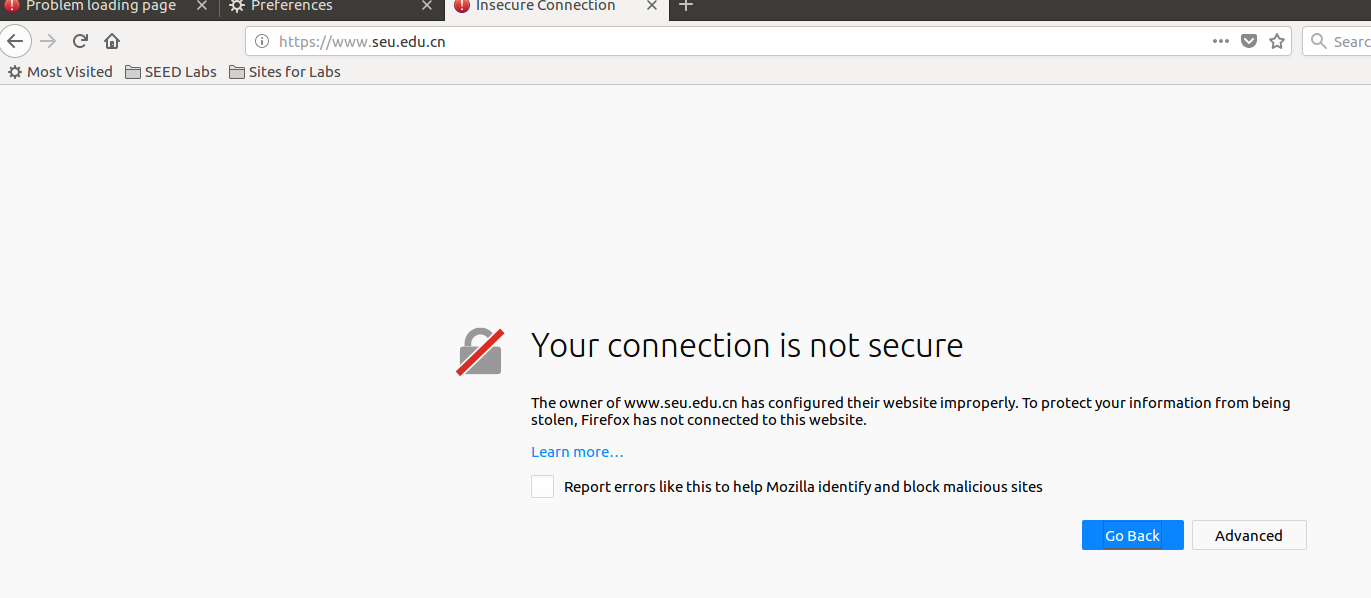
建立端口动态转发：



并在浏览器中设置代理：

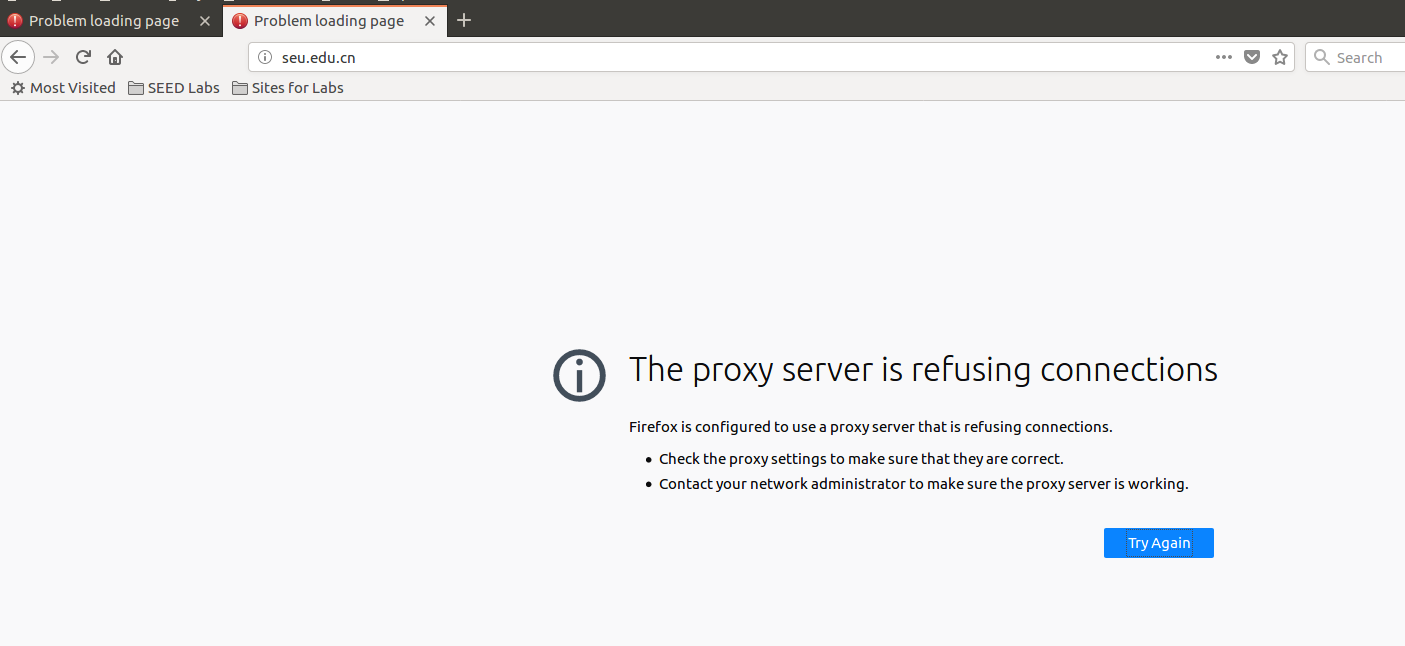


随后可以访问seu.edu.cn (从weibo.com更换至此)



说明：从B主机访问该页面就是这个界面，此处正常。

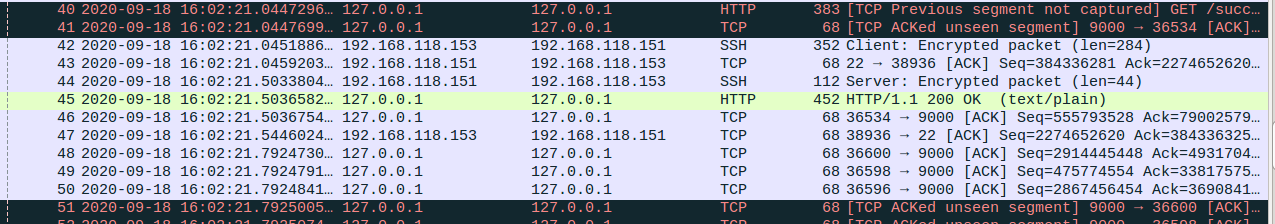
而断开连接，网页无法访问：



重新连接则恢复正常。

以下观察wireshark：

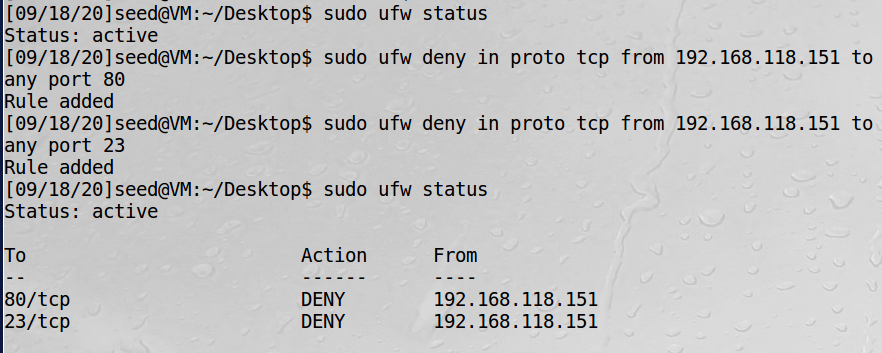
与目标网页相关的数据包都与主机B（.151）相连接，证明其利用端口转发和代理端口实现绕过防火墙。

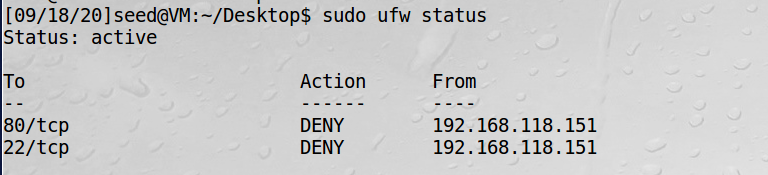


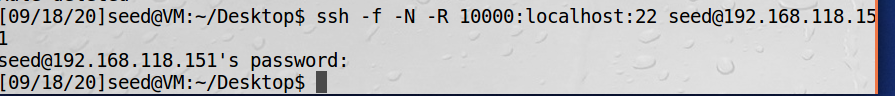
**Task4: Evading Ingress Filtering**

建立反向隧道。

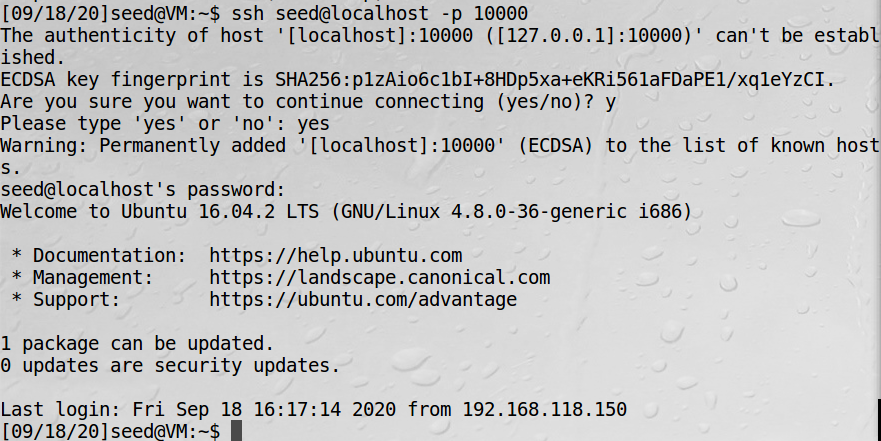
首先禁止B访问A的22、80端口：



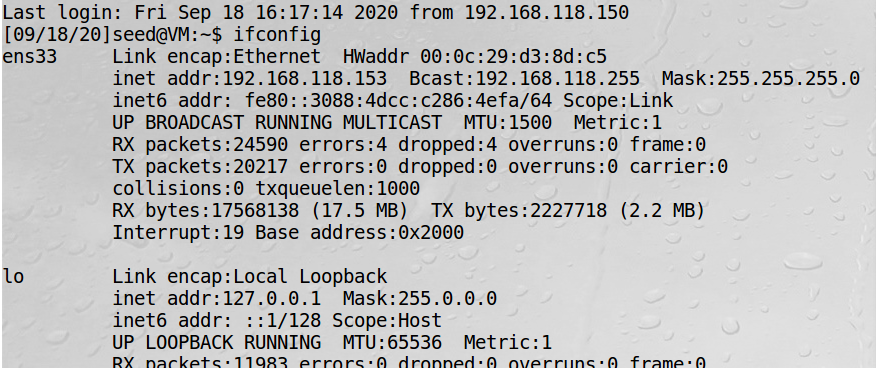


随后将主机B的端口转发到本地22：  


最后在主机B输入如下命令：



建立反向隧道：



总结：

在做实验的中途，ufw的突然无法使用让人十分头疼，iptables和直接运用c语言编写内核模块虽然都可以代替但都麻烦了不少，后期又莫名其妙可以使用ufw了，但由于可能忽略掉的iptables命令清空-F，以及telnetFilter的内核模块的移除，导致我整个实验做得很混乱低效。而且网页的ip地址可能有多个，想当然的相信dig命令会影响后续实验的进行。