**Lab17-1: Linux Firewall Exploration Lab**

**实验环境：**

VM A：192.168.43.166；

VM B：192.168.43.139；

VM C：192.168.43.85。

**Task 1: Using Firewall**

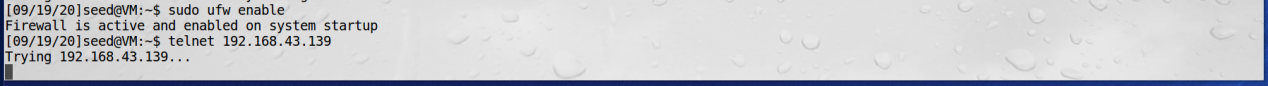
取消丢弃所有传入流量的设置，A与B可以进行远程连接：





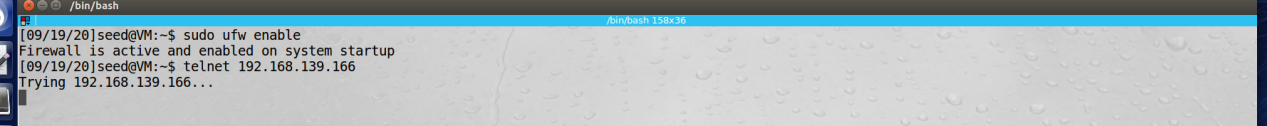


在A上打开防火墙并设置规则，A无法与B进行远程连接：

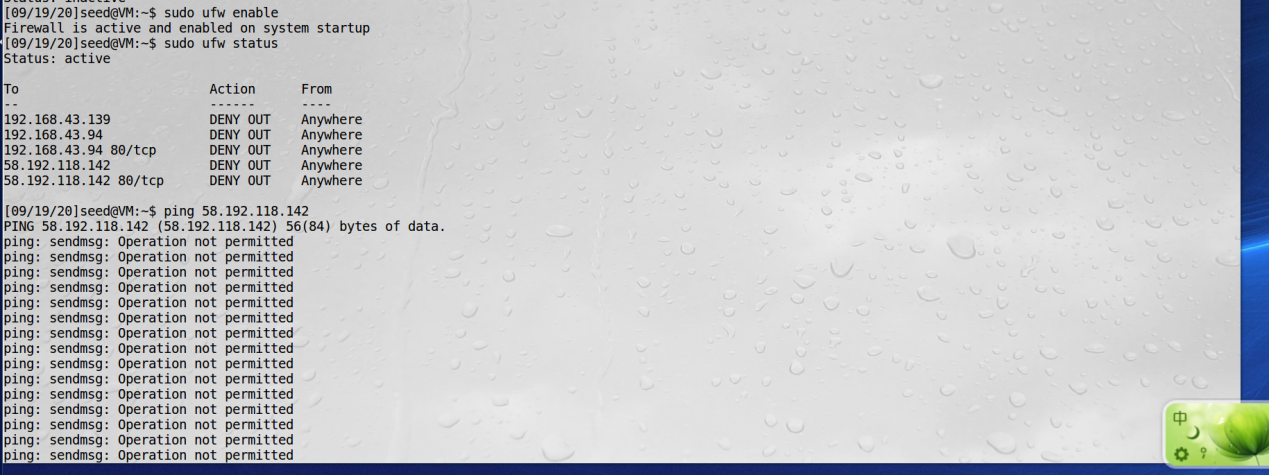


在A上关闭防火墙，在B上打开防火墙并设置规则，B无法与A进行远程连接：



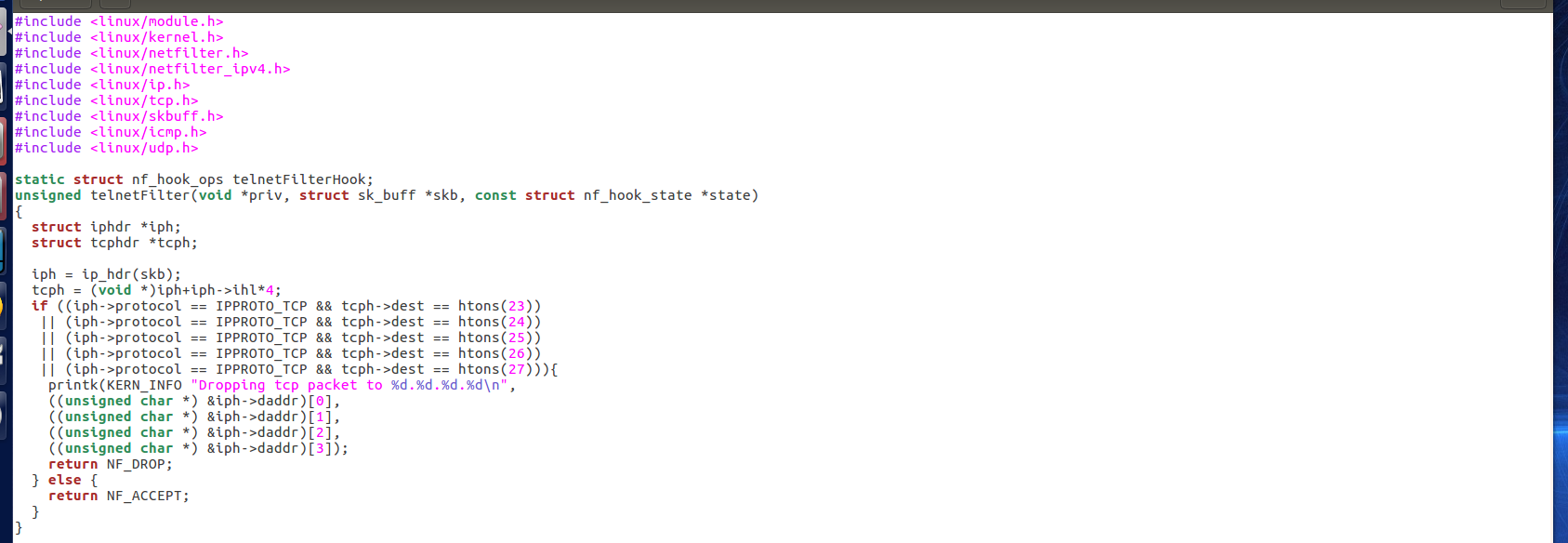


在A上打开防火墙并设置规则，A无法访问特定的外部ip：



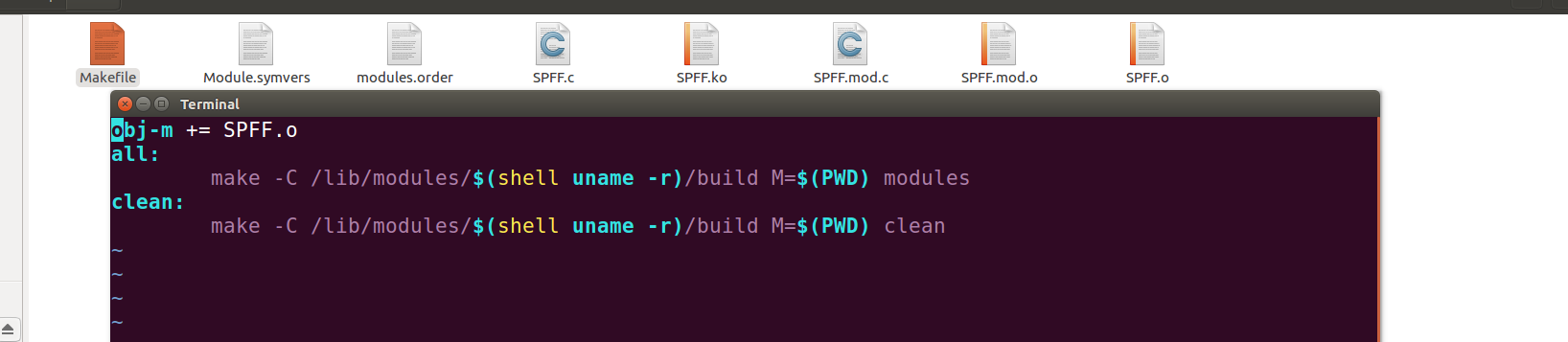
**Task 2: Implementing a Simple Firewall**

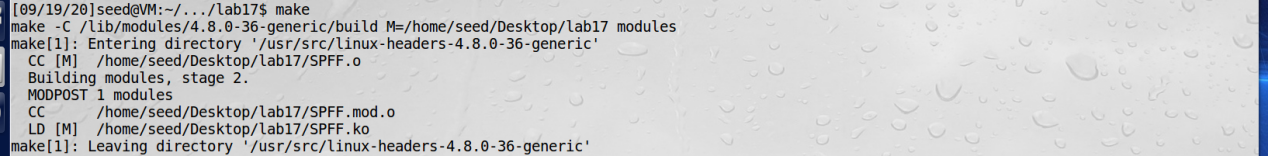
编写过滤代码：



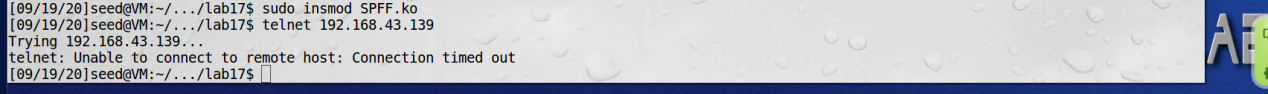


编写Makefile文件并运行：

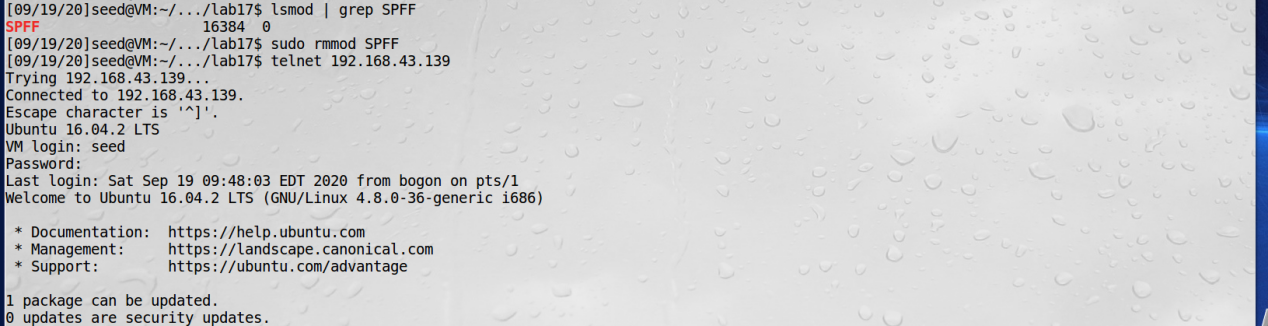




将模块载入内核后，A与B无法远程连接：



将模块移出内核后，A与B又可以远程连接了：



**Task 3: Evading Egress Filtering**

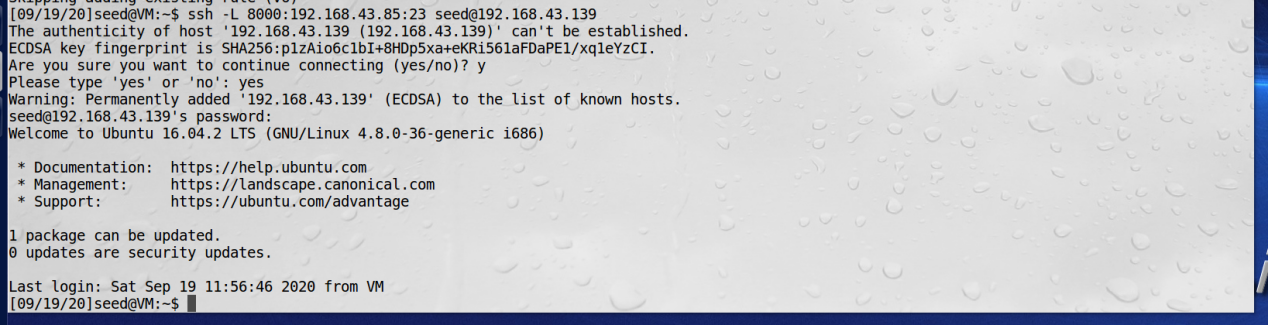
设置防火墙：





**3.1 Loadable Kernel Module**

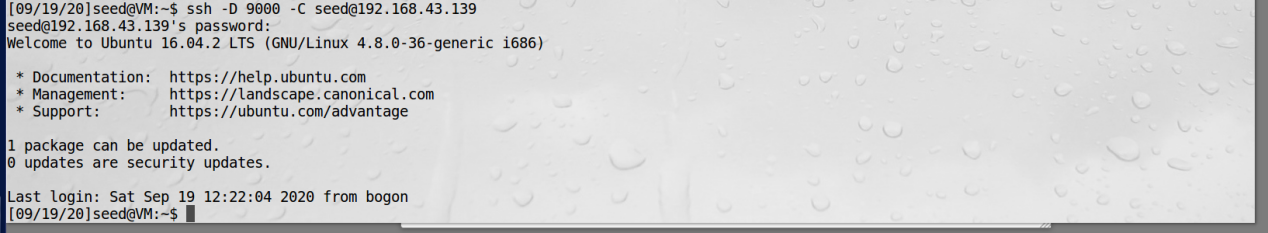
通过对C进行SSH连接，A可以成功绕过防火墙与B进行远程连接：

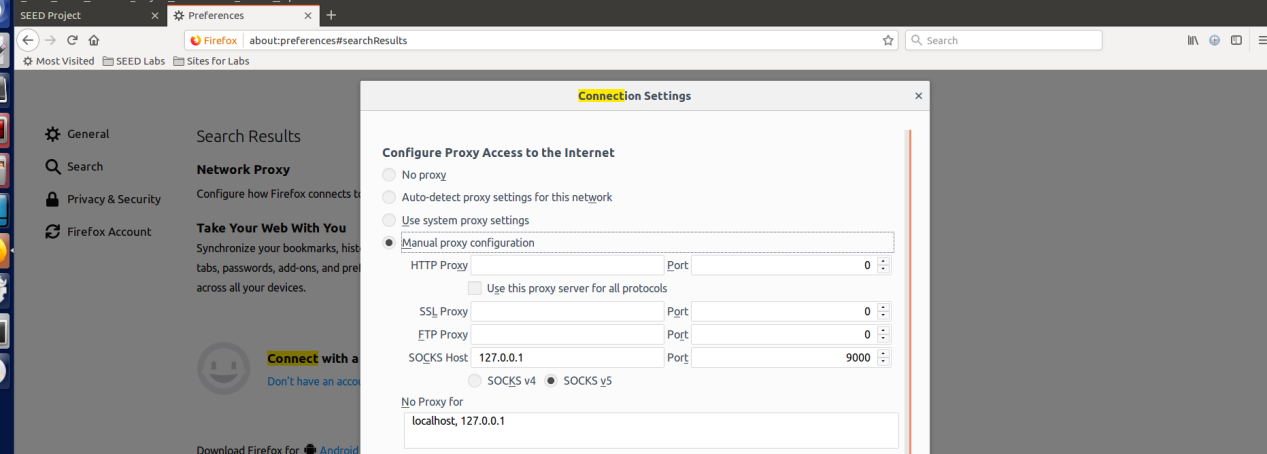


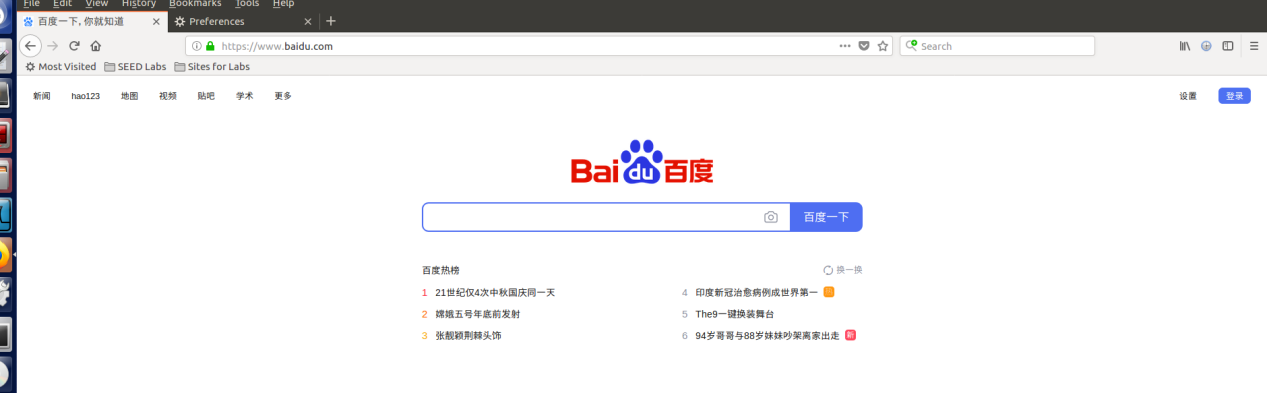


**3.2 A Simple Program that Uses Netfilt**er

使用SSH隧道，并设置浏览器代理，A可以通过B访问防火墙禁止访问的网页：

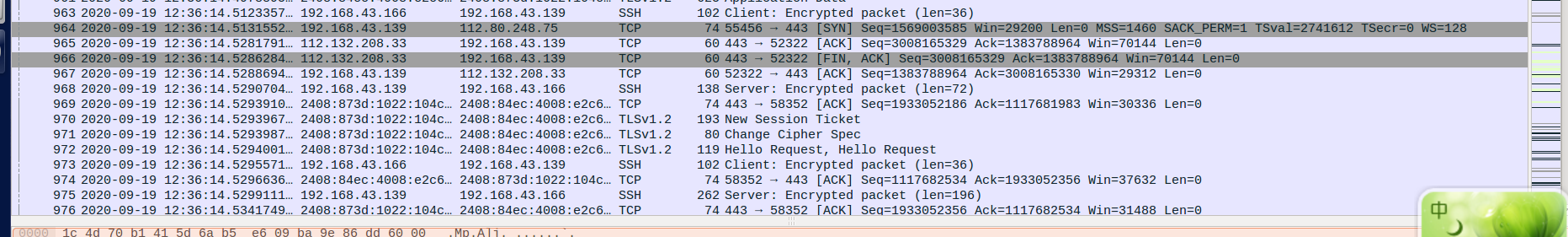




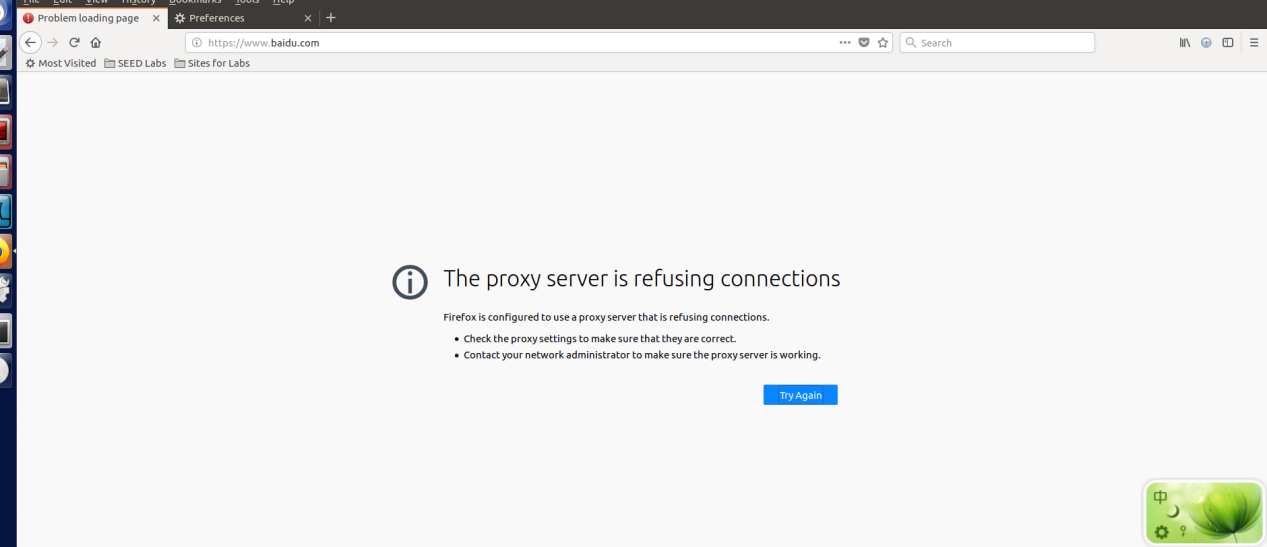


可以看出A是通过B来访问该网页的：

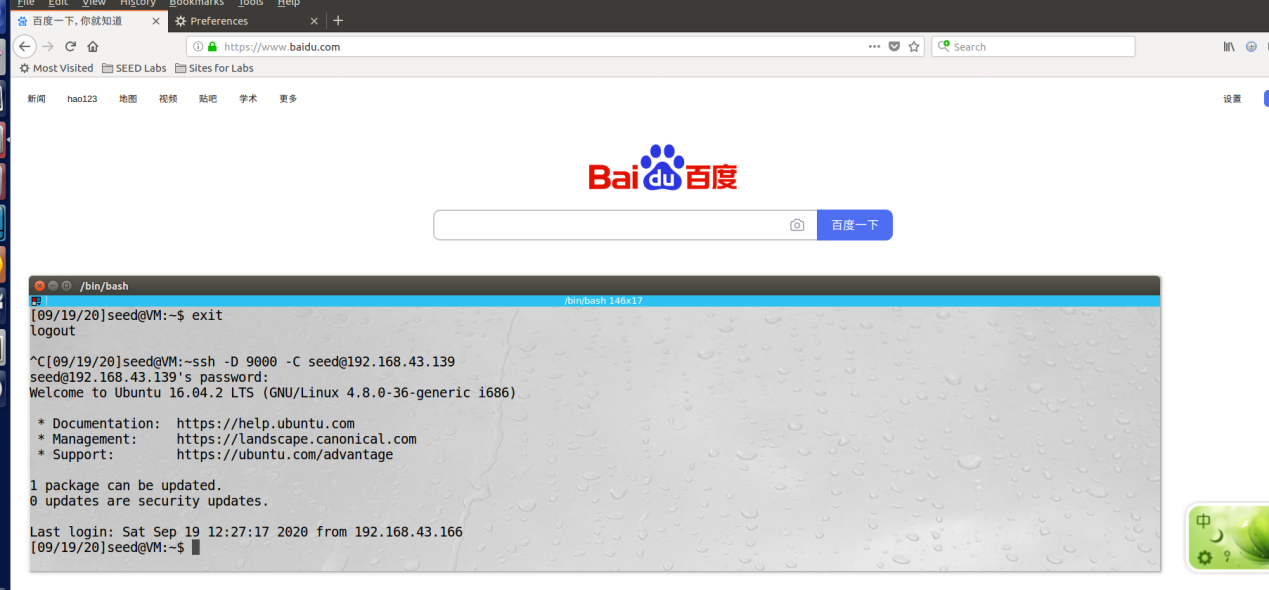




断开SSH连接后无法访问：



重新连接后又可以访问了：

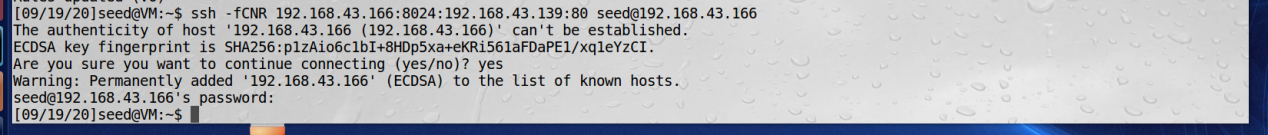


**Task 4: Evading Ingress Filtering**

设置规则，阻止B访问端口80（Web服务器）和22（SSH服务器）：



在A上设置反向SSH隧道：



可以成功访问在A上受保护的Web服务器：

