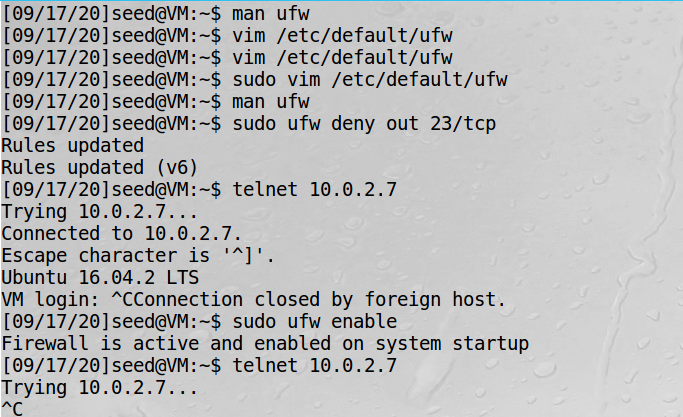
**Linux Firewall Exploration Lab**

**Task1**

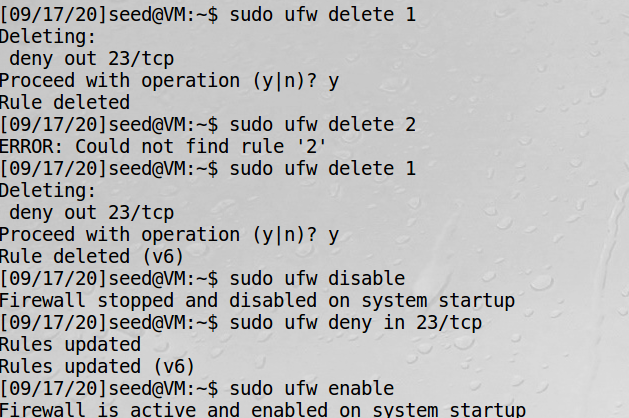
A的IP地址为10.0.2.5，B的IP地址为10.0.2.7。

Prevent A from doing telnet to Machine B

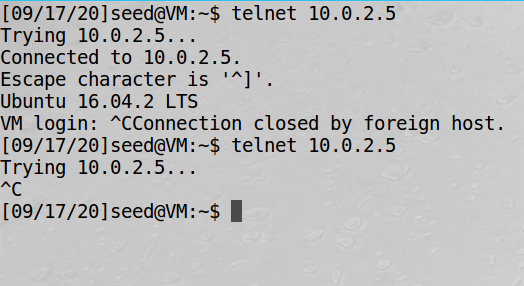


设置相应的ufw规则，禁止针对tcp23端口的流量流出，设置成功后无法启动相应的telnet服务

Prevent B from doing telnet to Machine A

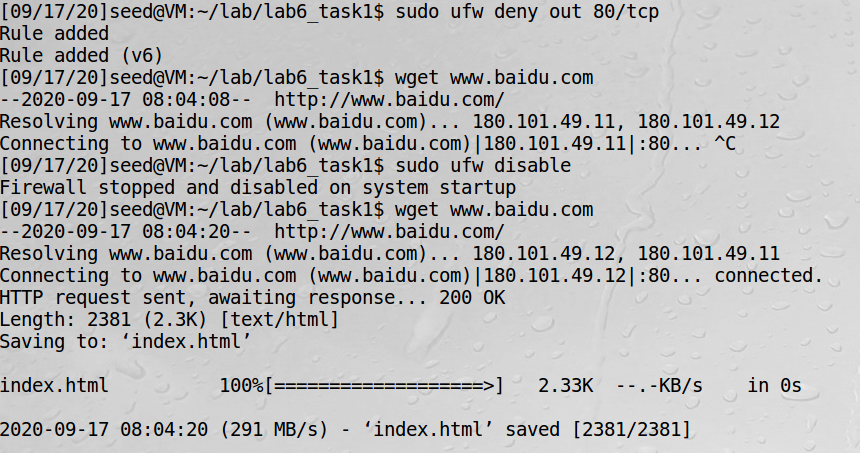


在A上设置相应的防火墙规则，禁止针对tcp23端口的流量进入



B在开启防火墙后无法通过telnet连接到A

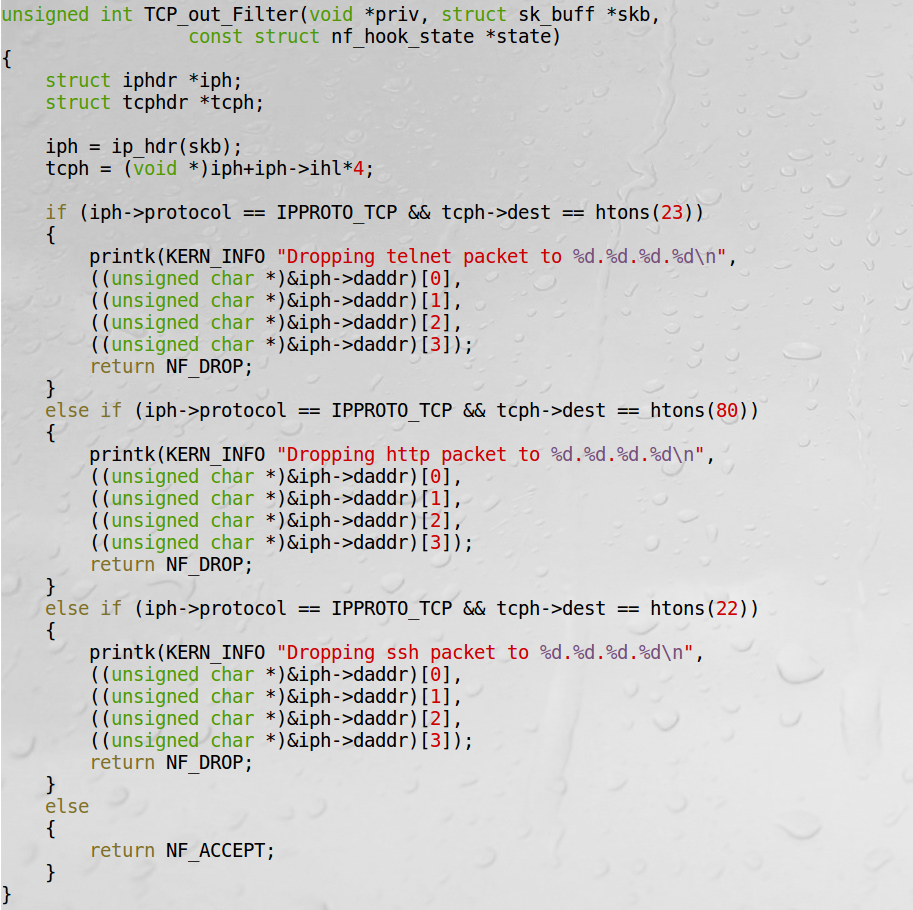
Prevent A from visiting an external web site

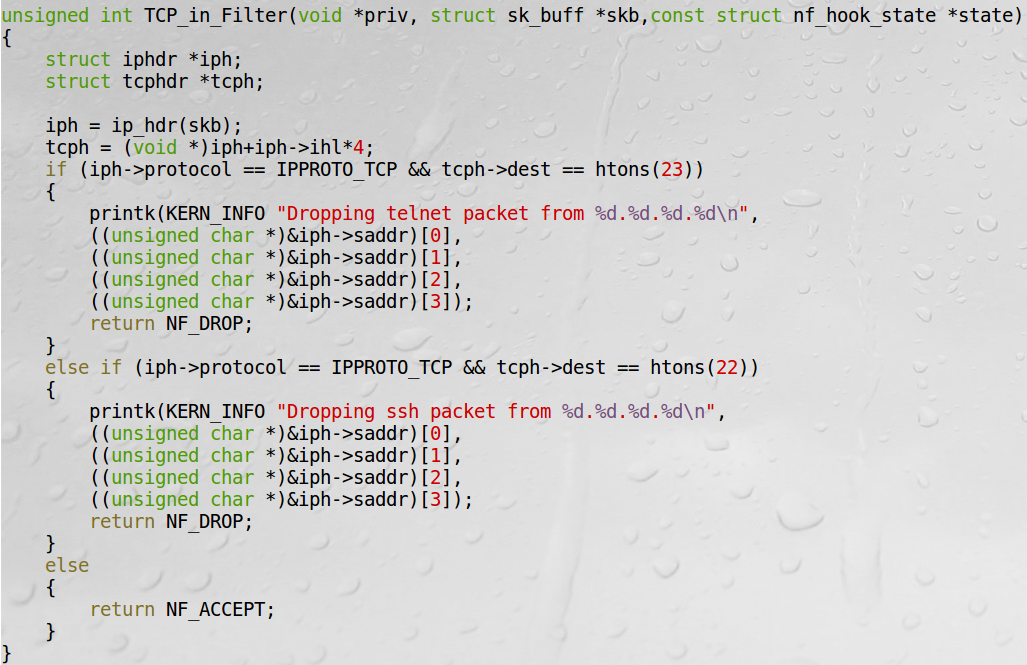


禁止流出指向80端口的流量即可

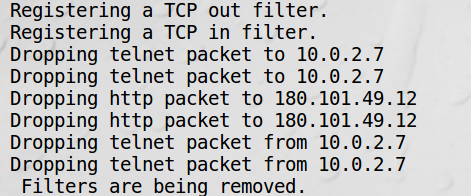
**Task2**

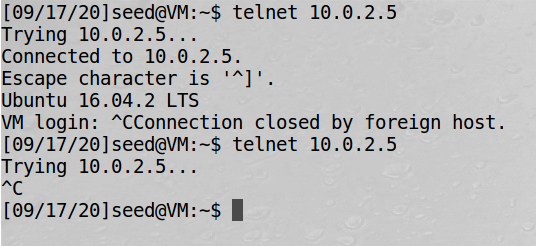
根据题目要求5条规则，所以写了两个过滤器（in or out）





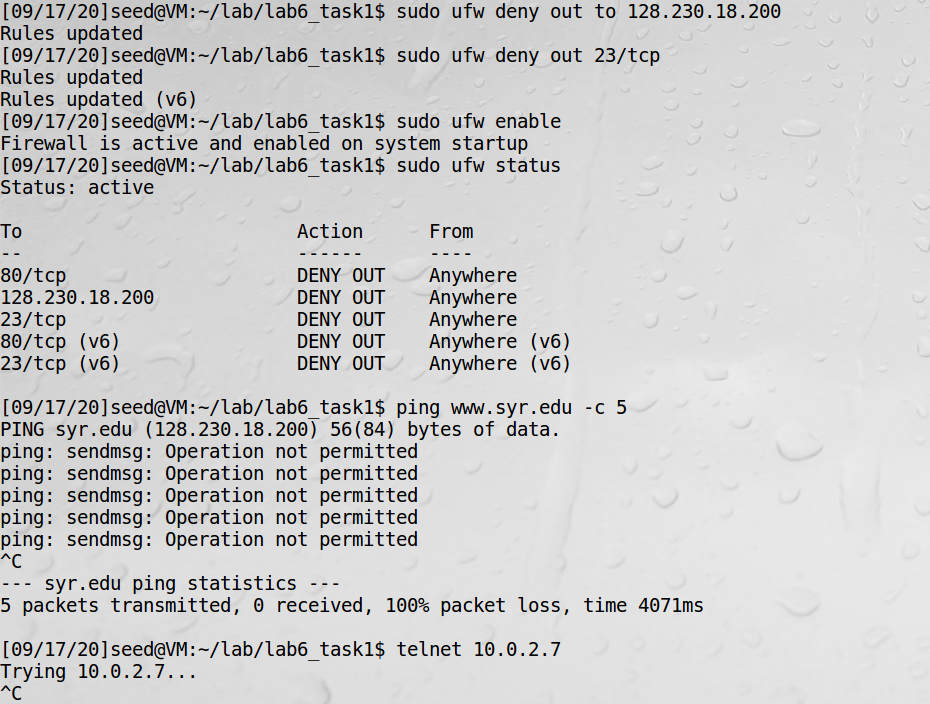
载入相关模块后，telnet访问B，wget访问baidu，B telnet访问A均失败，如下图所示





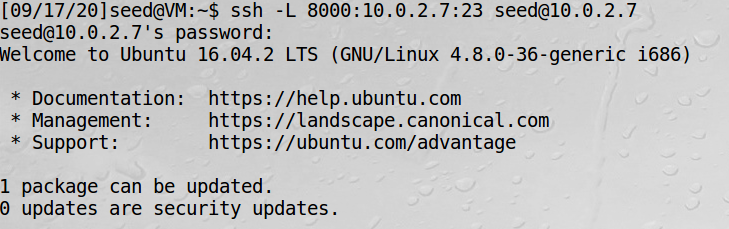


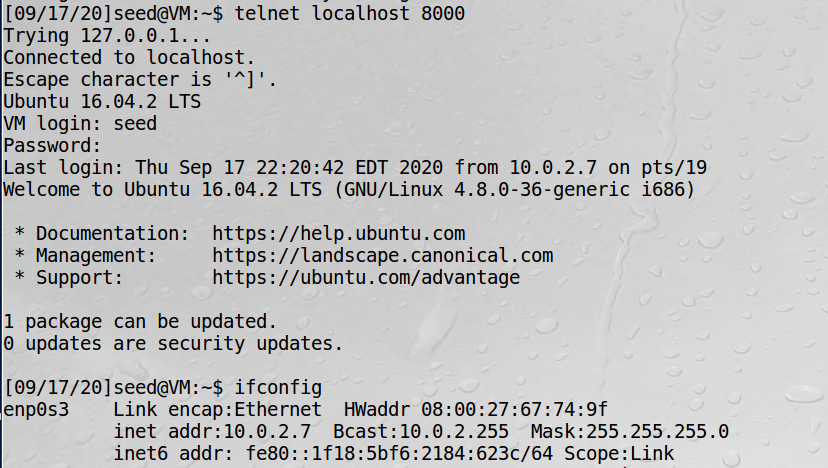
**Task3**



通过设置规则，禁止了虚拟机A访问雪城大学官网与其他主机的telnet的服务

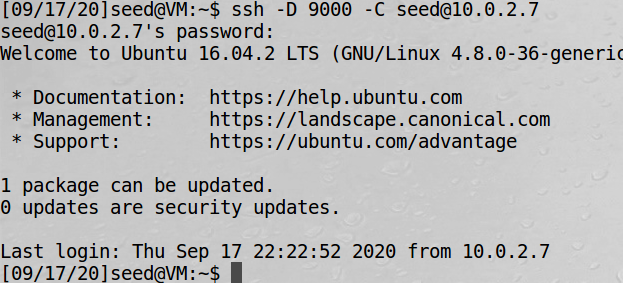
**Task3.a**

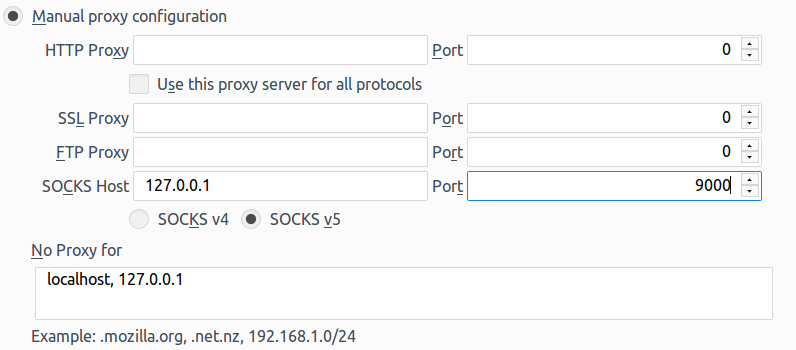




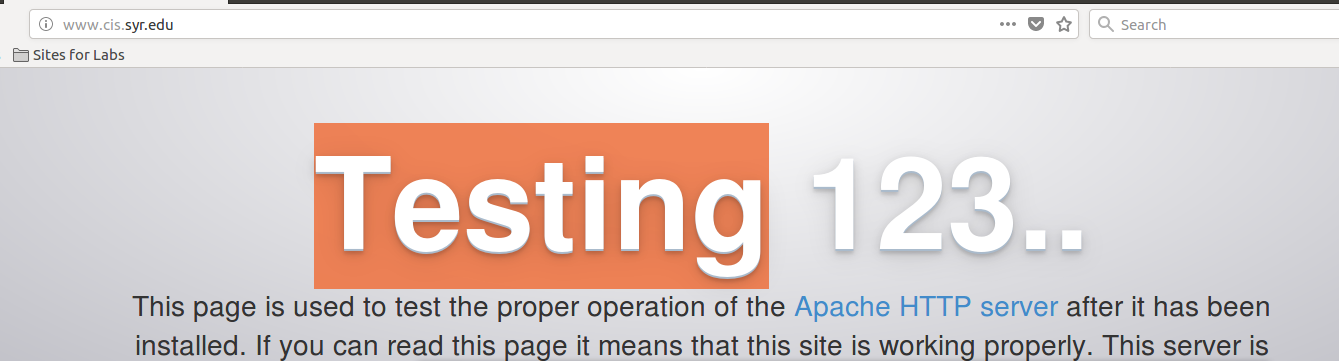
通过ssh隧道实现了访问machineB的23端口并登陆成功

**Task3.b**

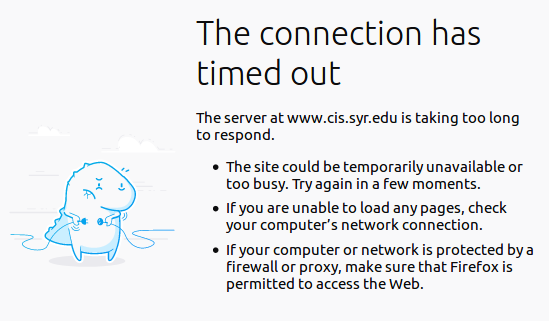




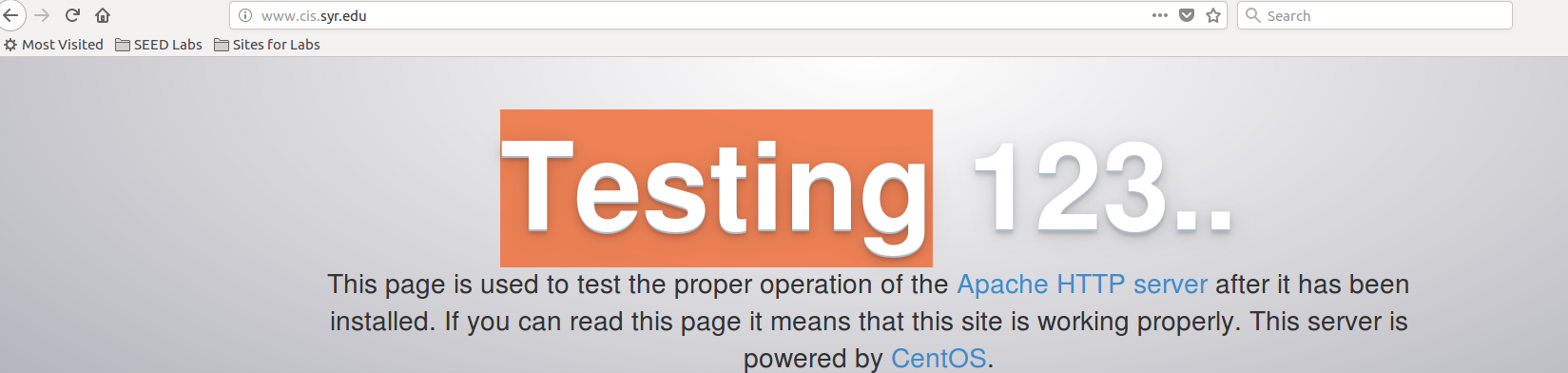
启动ssh，设置代理，访问结果如下图



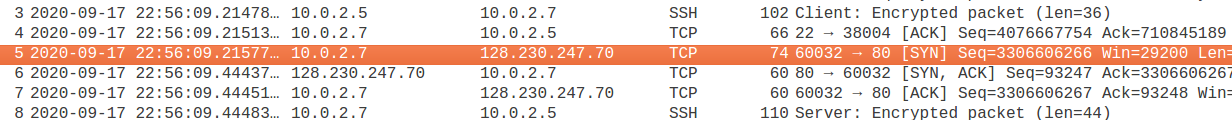
虽然显示test，但是因为B访问这一网站也显示test，所以说明已经访问成功



关闭ssh与代理设置后会显示访问失败，连接超时。

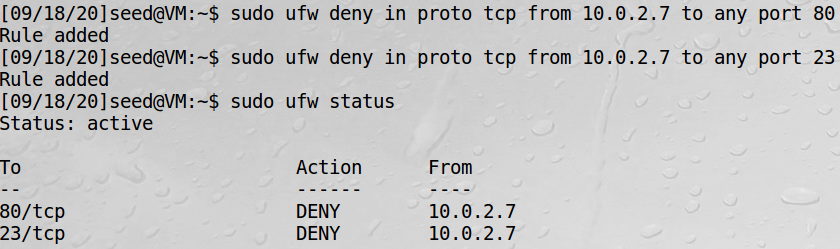


重新设置后会再次显示该界面



Wireshark截图显示A先将访问内容通过ssh发给B，B在进行相关访问，然后将访问结果返回给A

**Task4**



首先进行主机A的配置，禁止B主机访问23端口和80端口

设置主机C的相关文件/etc/ssh/sshd\_config，添加GatewayPorts yes



设置逆向的ssh隧道，使得主机B可以通过访问主机C的6666端口来访问主机A



主机B访问主机A成功