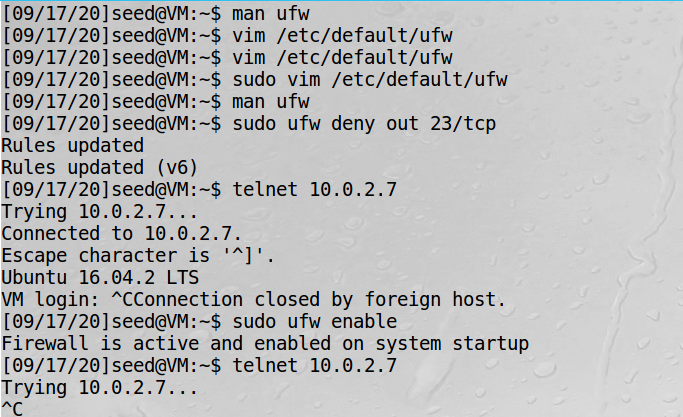
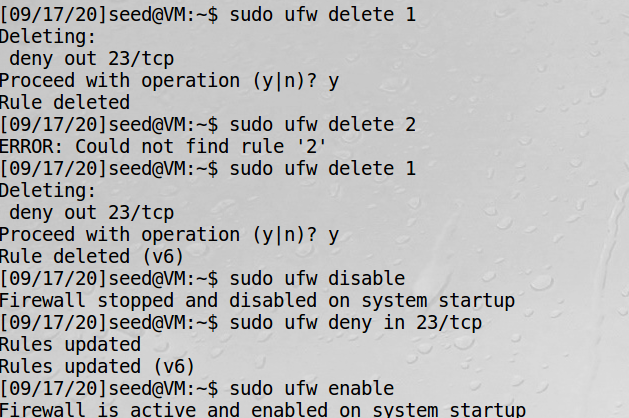
**Linux Firewall Exploration Lab**

**Task1**

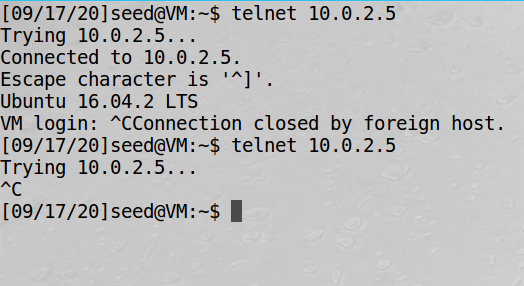
Prevent A from doing telnet to Machine B



Prevent B from doing telnet to Machine A

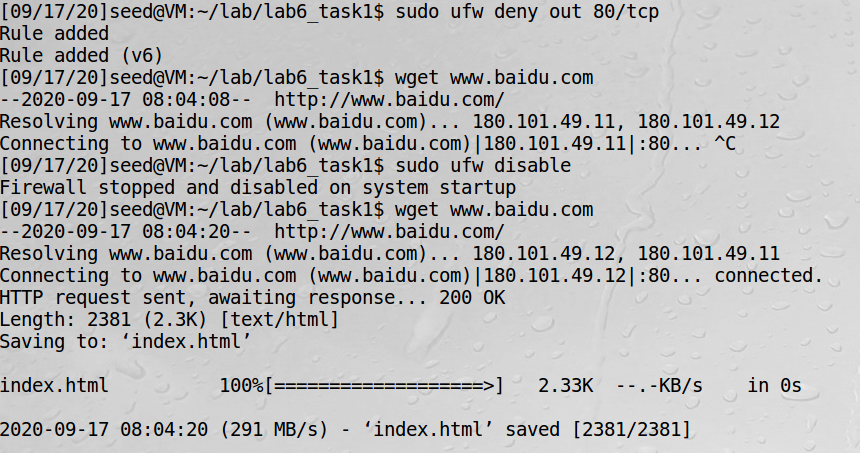


在A上设置相应的防火墙规则，禁止针对tcp23端口的流量进入



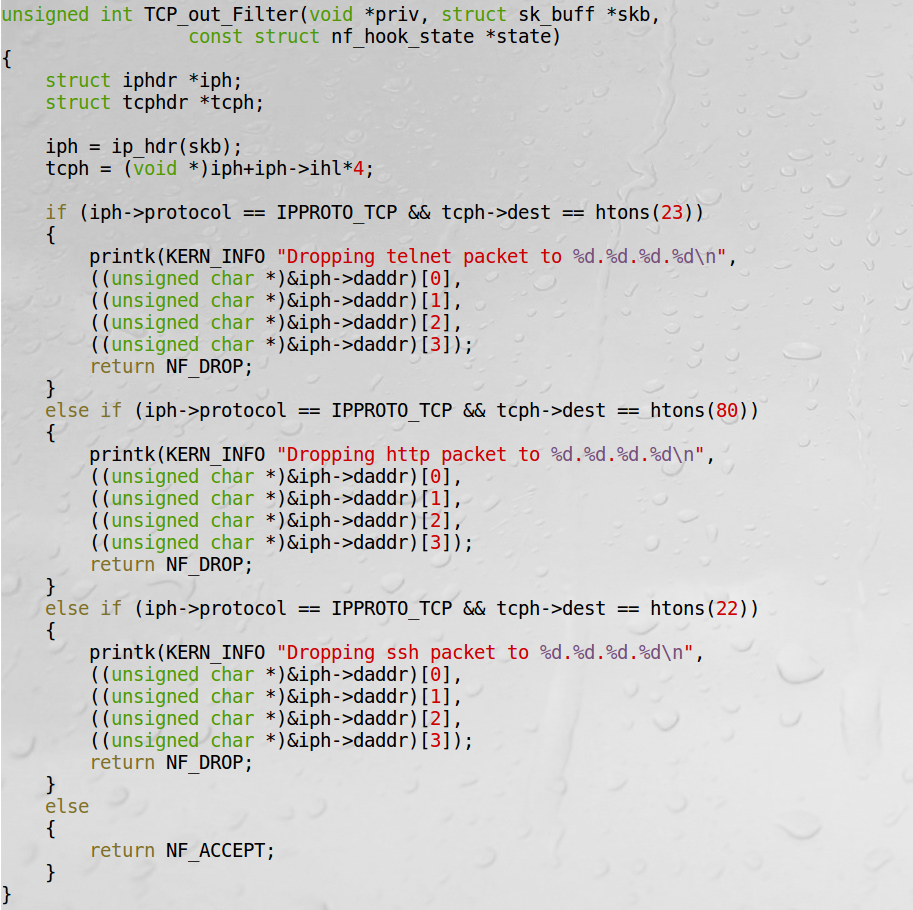
B在开启防火墙后无法通过telnet连接到A

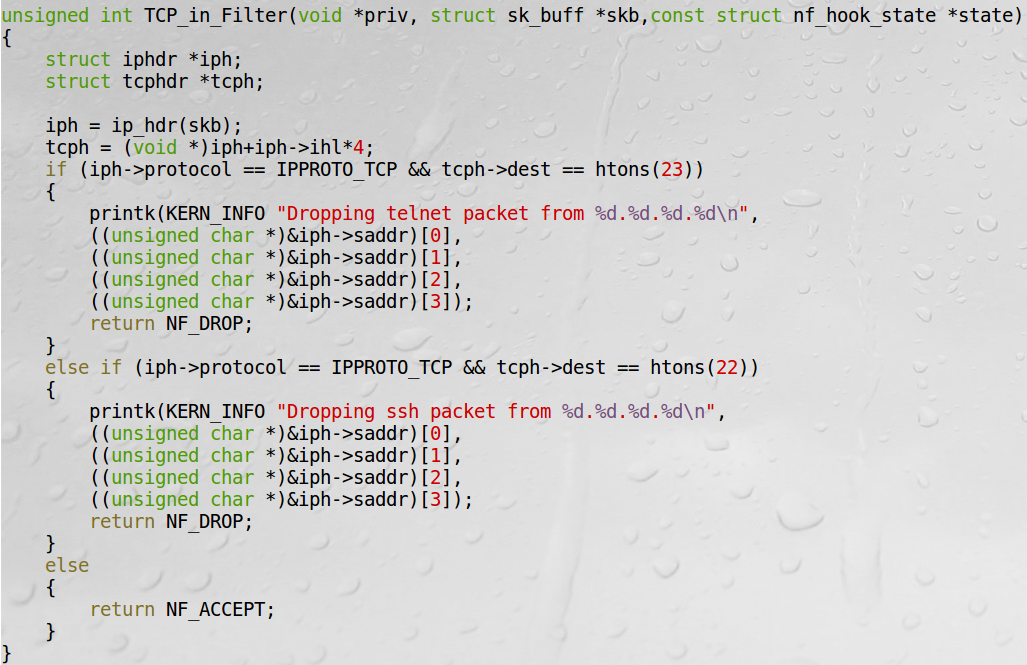
Prevent A from visiting an external web site

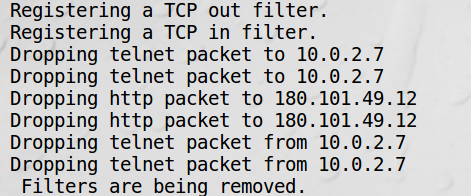


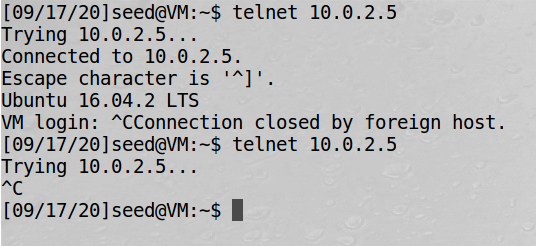
禁止流出指向80端口的流量即可

**Task2**



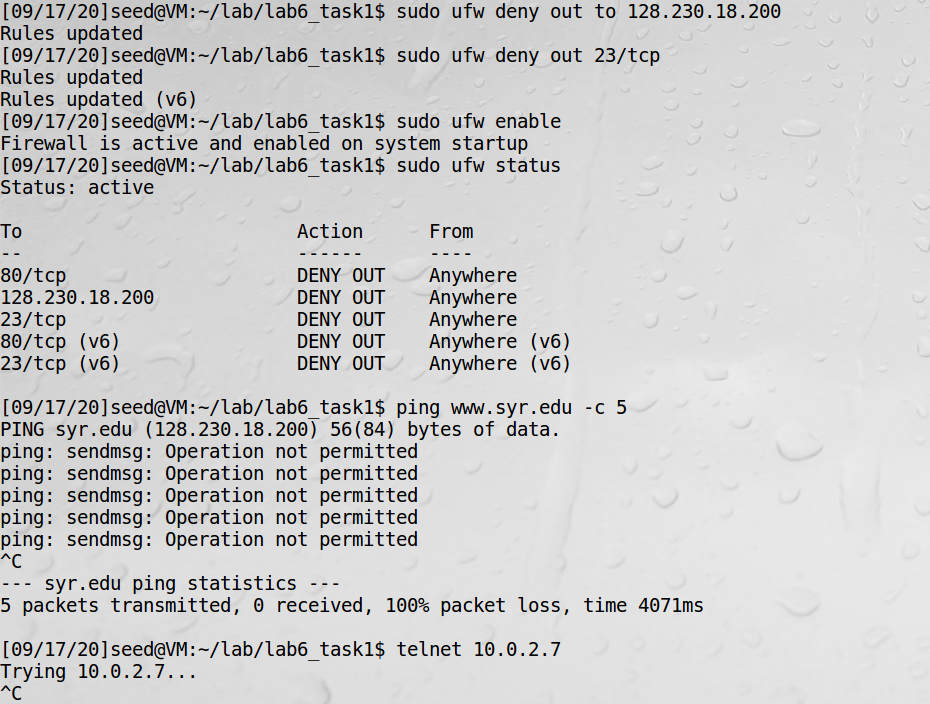






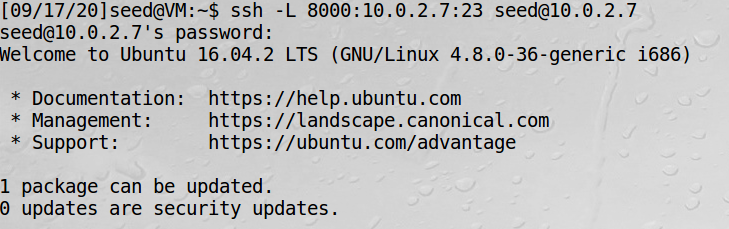


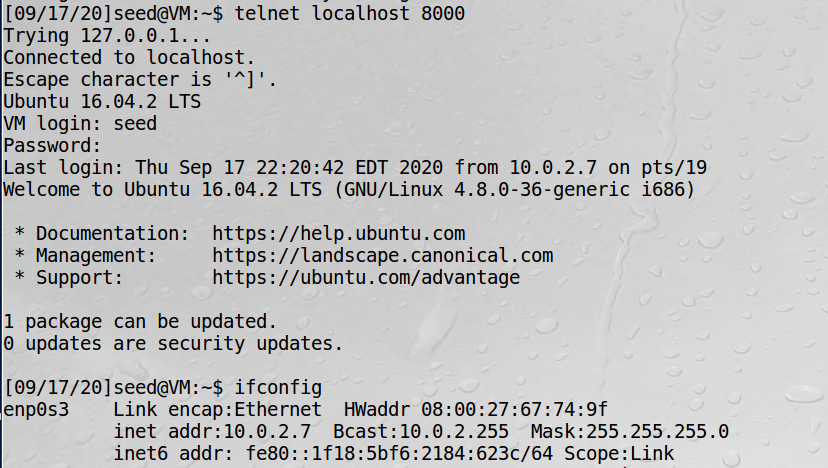
**Task3**



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

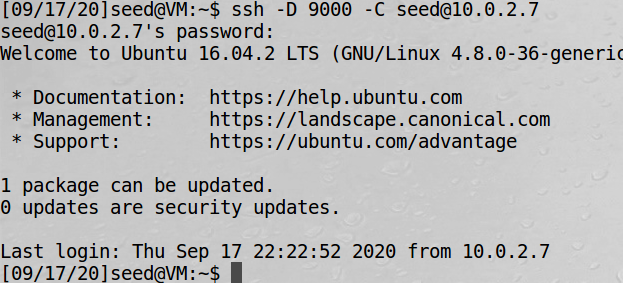
**Task3.a**

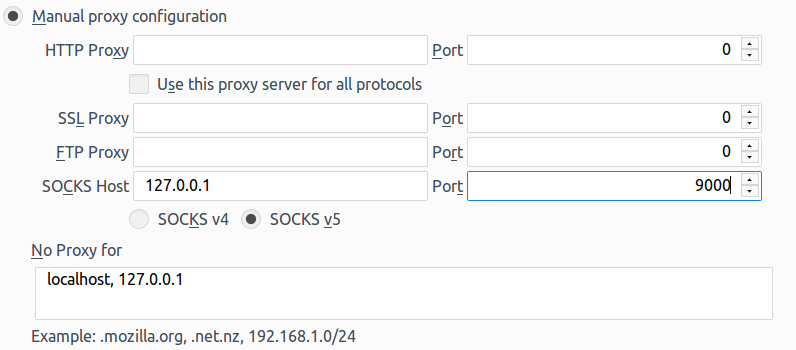


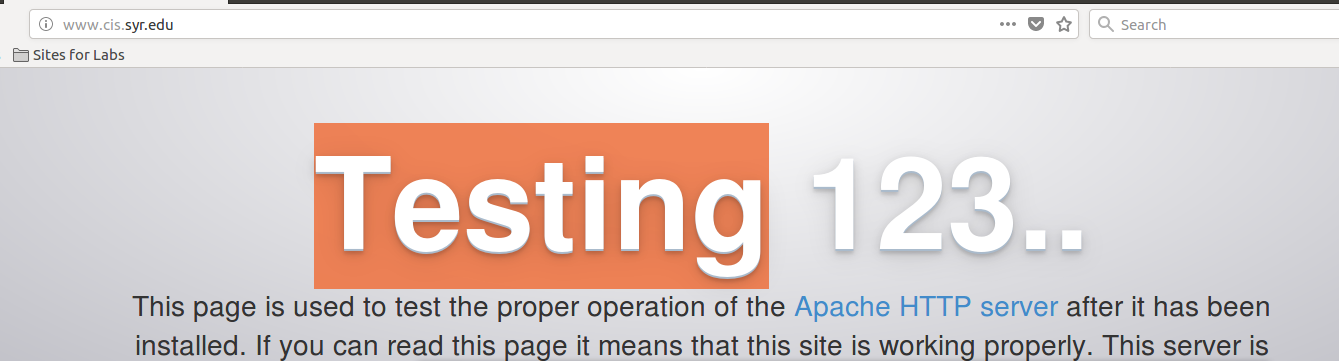


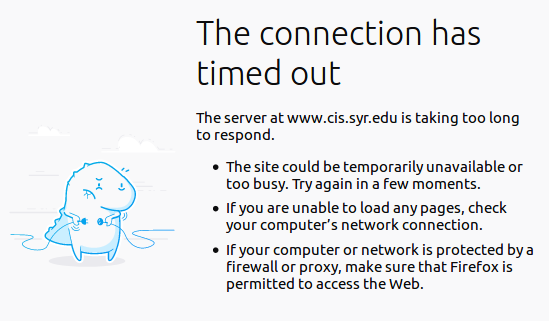
通过ssh隧道实现了访问machineB的23端口并登陆成功

**Task3.b**

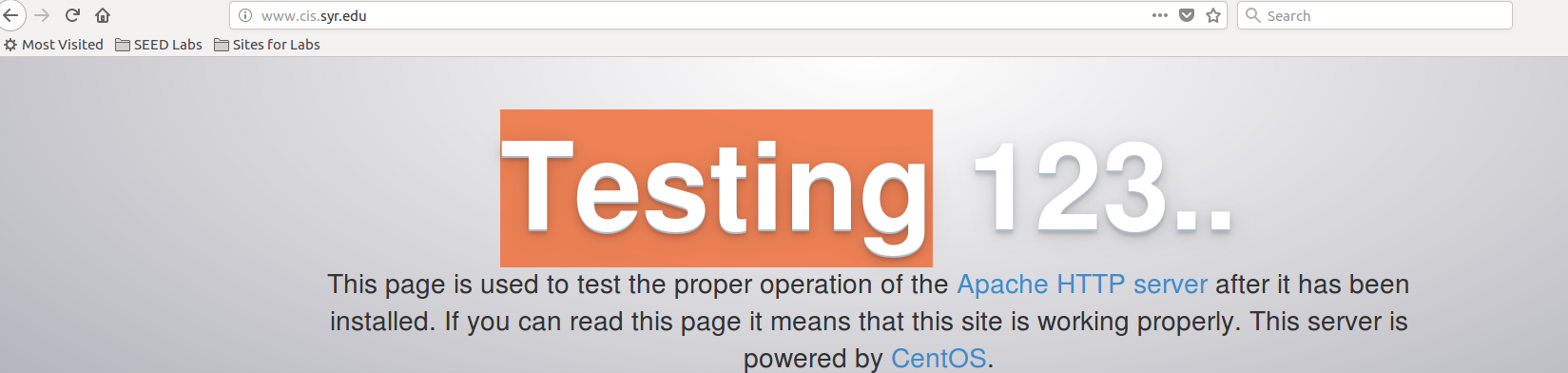




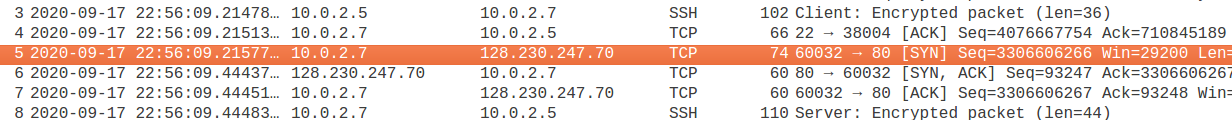




关闭ssh与代理设置后会显示访问失败，连接超时。

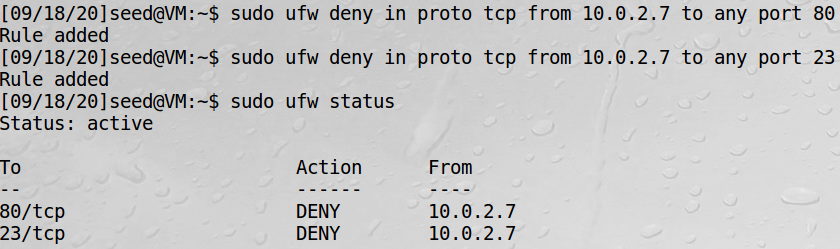


重新设置后会再次显示该界面



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**





A

