Linux Firewall Exploration Lab

57117132费越

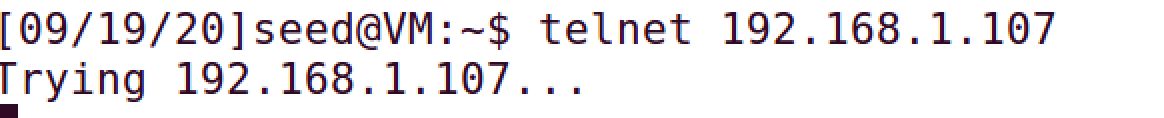
Task 1: Using Firewall

虚拟机A: 192.168.1.105

虚拟机B: 192.168.1.107

先启用ufw防火墙

阻断A到B的Telnet请求：sudo ufw deny out on ens33 proto tcp to 192.168.1.107 port 23



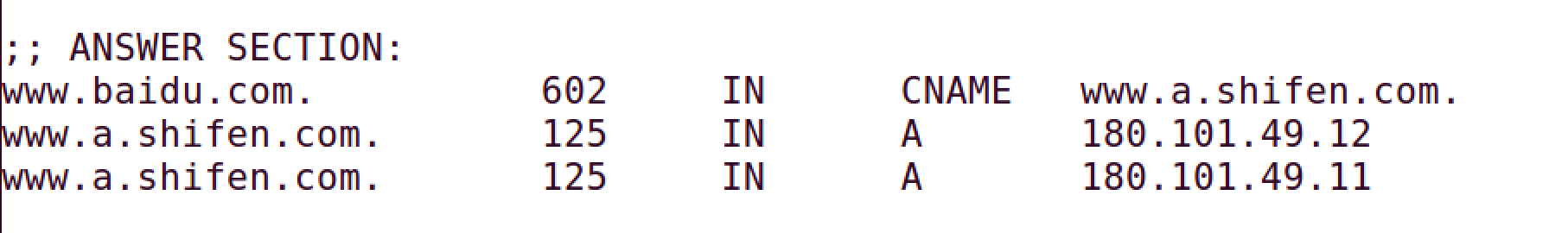
Telnet无法访问

同理，阻断B到A的Telnet请求：sudo ufw deny out on ens33 proto tcp to 192.168.1.105 port 23

结果相同

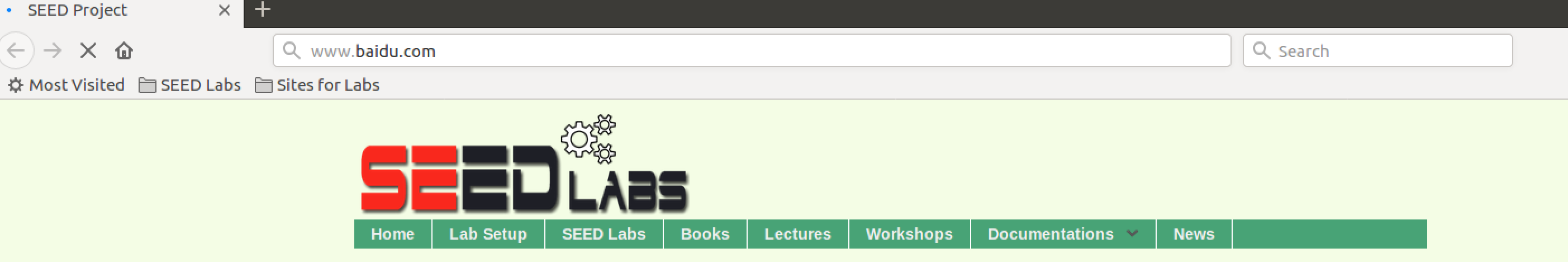
阻断到百度的访问

使用dig命令查看当前地址解析出的百度的IP地址：



使用命令：sudo ufw deny out on ens33 proto tcp to 180.101.49.0/24 port 443

使用浏览器打开，输入百度网址，发现无响应

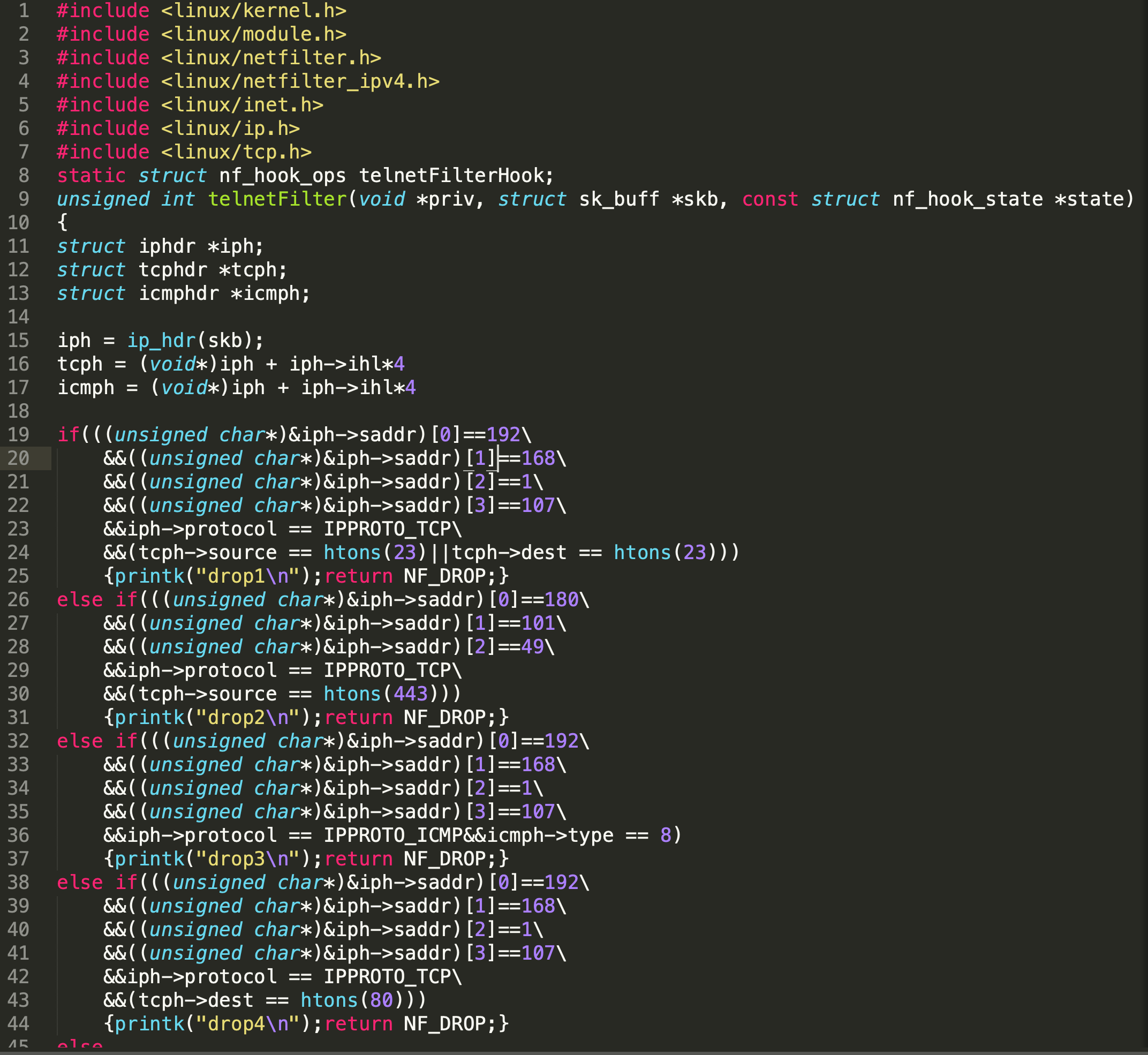


而其他网站可以正常访问。

Task 2: Implementing a Simple Firewall

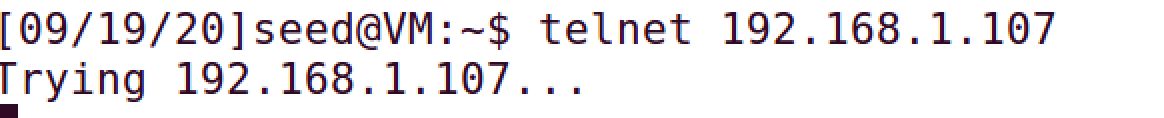
使用命令：sudo ufw disable关闭ufw

编写代码：（以下显示部分）



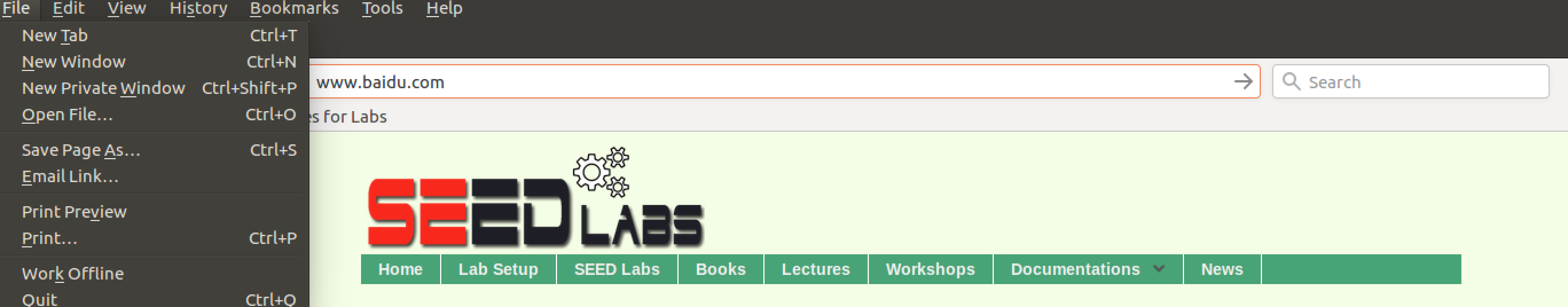
编写完后在当前目录下创建一个Makefile文件，然后输入make指令进行编译，编译完成后即得到可加载模块，使用insmod命令进行加载，使用rmmod卸载

规则1：禁止A向B发送Telnet请求。即丢弃目的地址为B的端口23的报文。



规则2：禁止B向A发送Telnet请求。原理相似，结果也相似

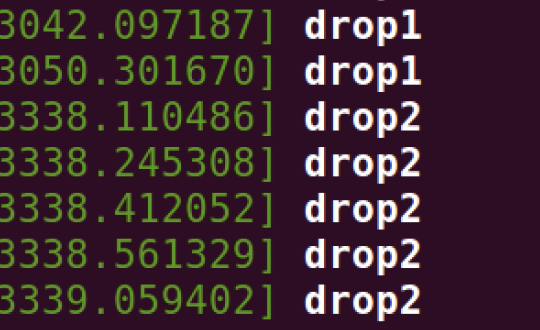
规则3：禁止访问百度网站。实现方法是丢弃端口443（百度使用HTTPS连接），网络号匹配百度服务器的报文。



规则4：禁止BpingA，丢弃B地址的ICMP报文。结果为报文全部丢失。

规则5：禁止B对A的HTTP请求。把原地址为B，目的端口为80的报文丢弃。结果Apache服务器无响应。

使用dmesg查看输出：



触发了hook，报文已被丢弃。

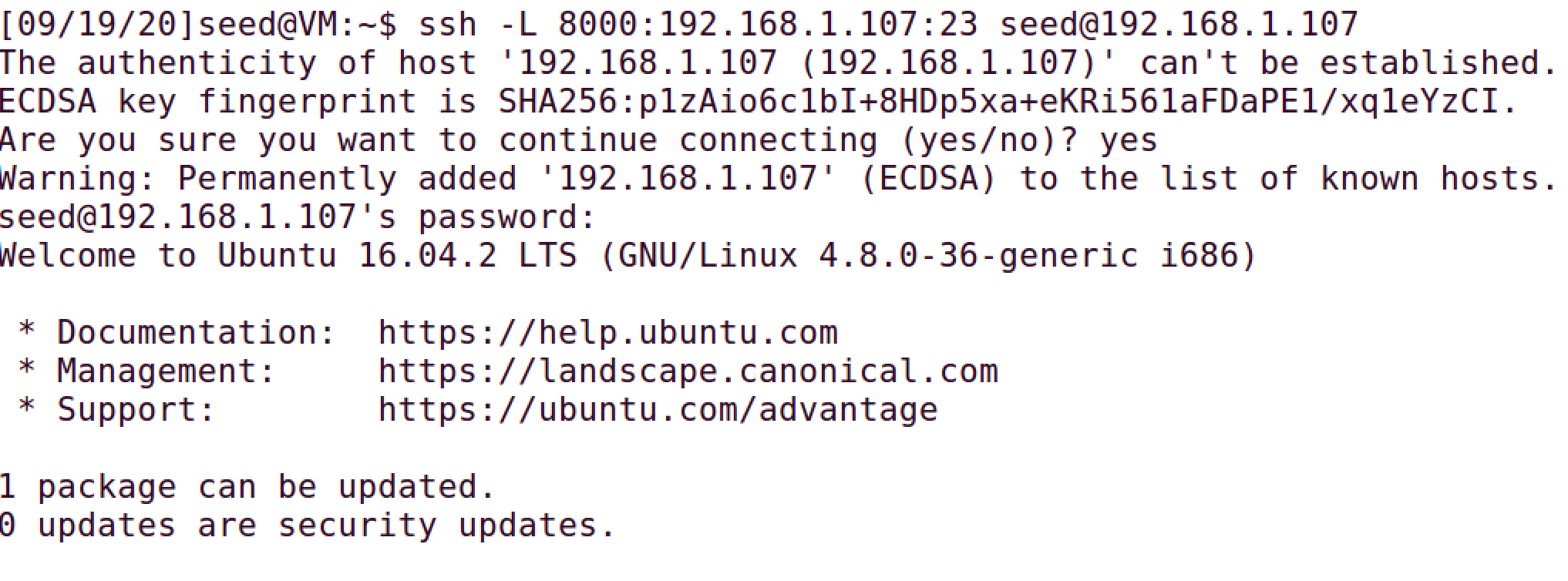
Task 3: Evading Egress Filtering

使用ufw关闭23端口，禁止Telnet

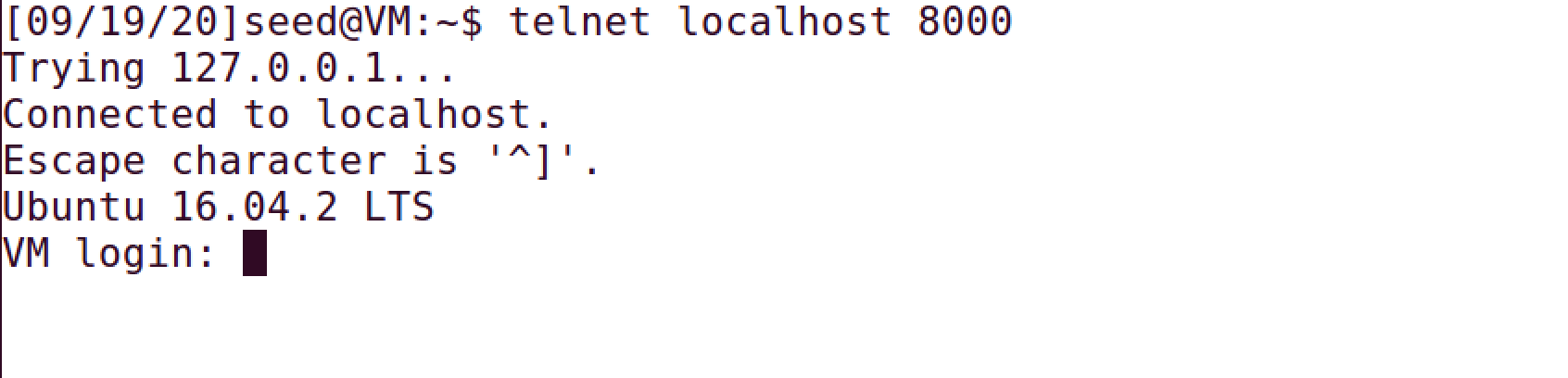
使用ufw禁止访问百度网址

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，在A和B之间建立SSH隧道，所有的telnet流量都将通过此隧道（加密），从而避免进行检查。



另外开启一个terminal



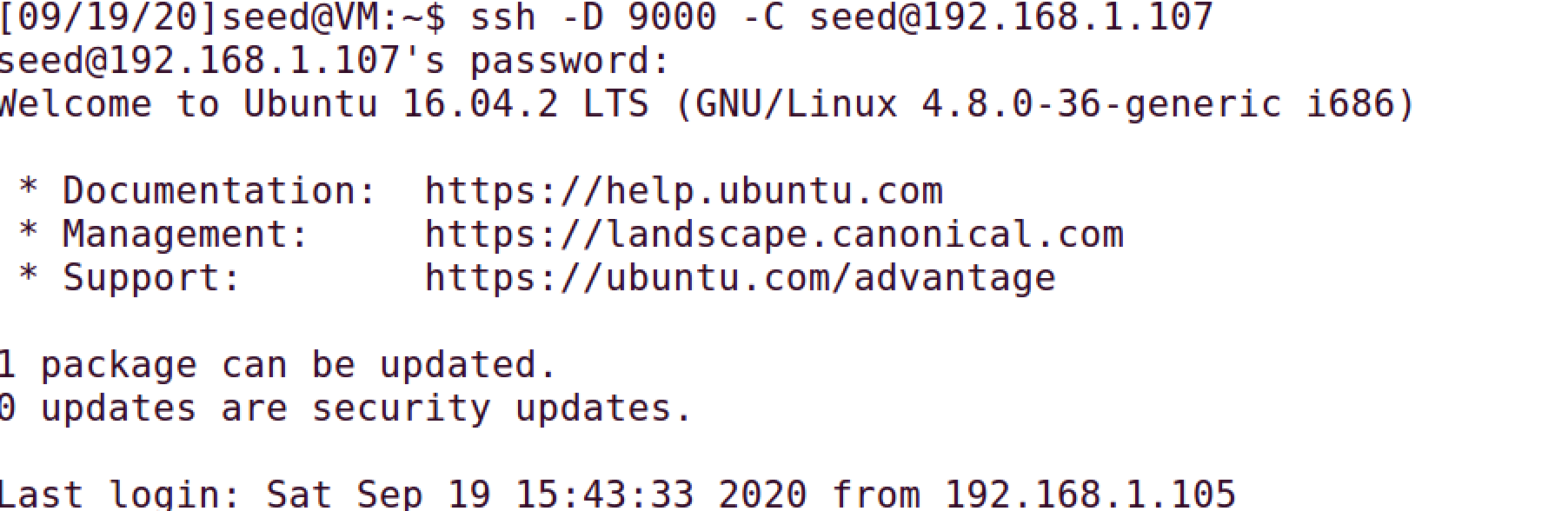
连接成功

使用wireshark查看报文，能够发现一个加密的ssh报文，Telnet连接通过此隧道来绕过防火墙

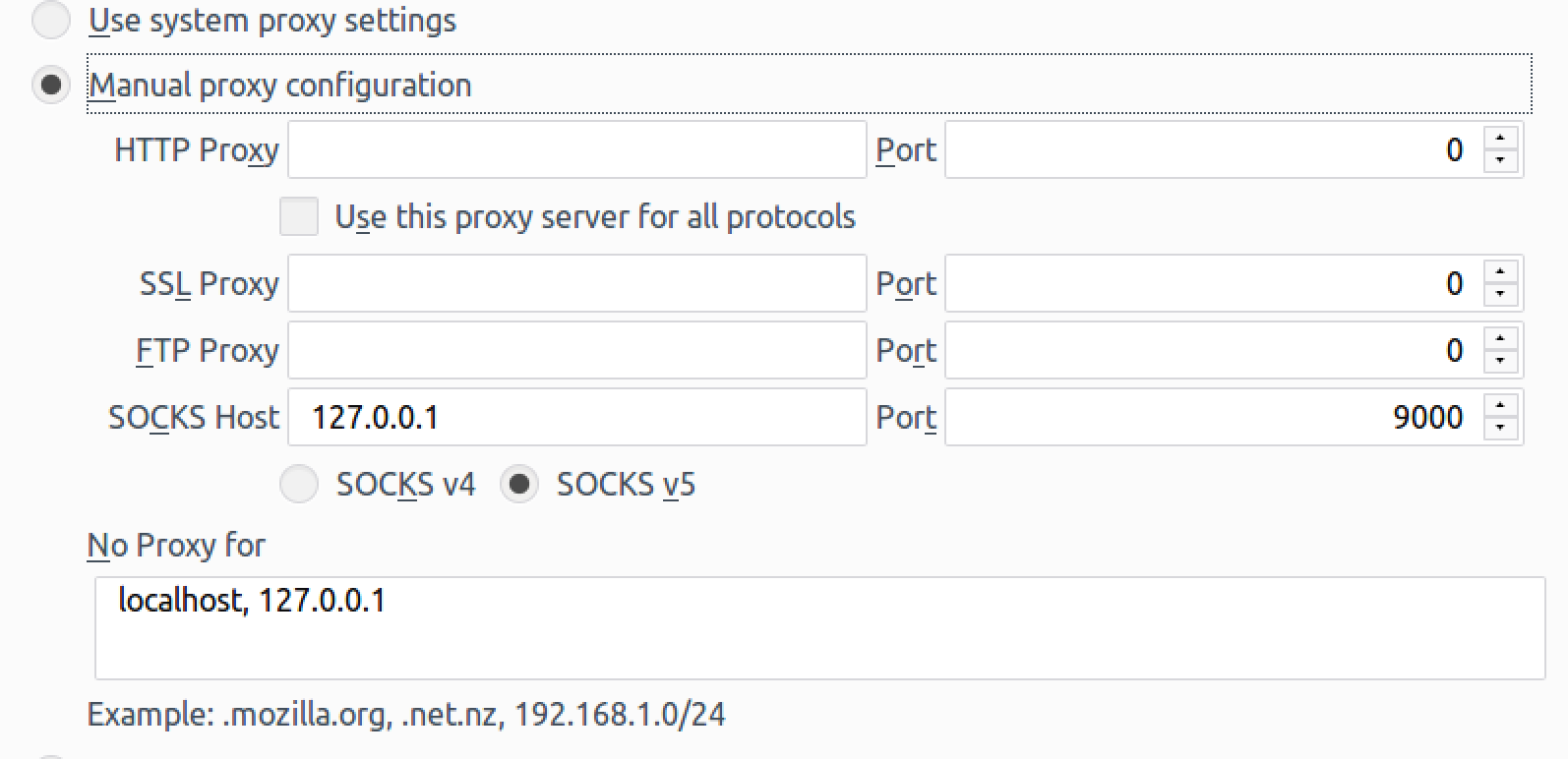
Task 3.b: Connect to Facebook using SSH Tunnel.

在有防火墙的情况下，无法访问百度

建立ssh端口动态转发：



对浏览器进行设置：



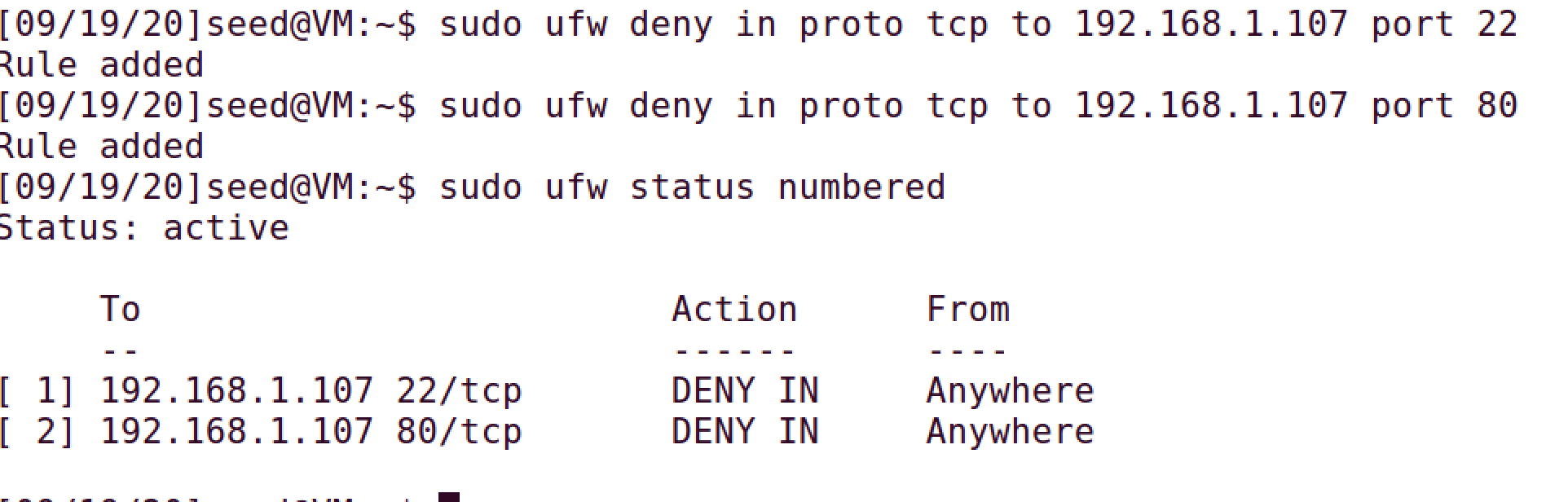
访问百度：



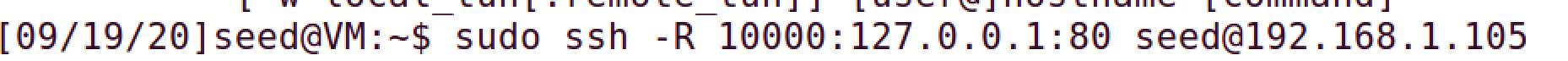
成功通过隧道技术突破防火墙，通过wireshark可以观察到虚拟机A和B之间的ssh加密通信以及B对百度的访问

Task 4: Evading Ingress Filtering

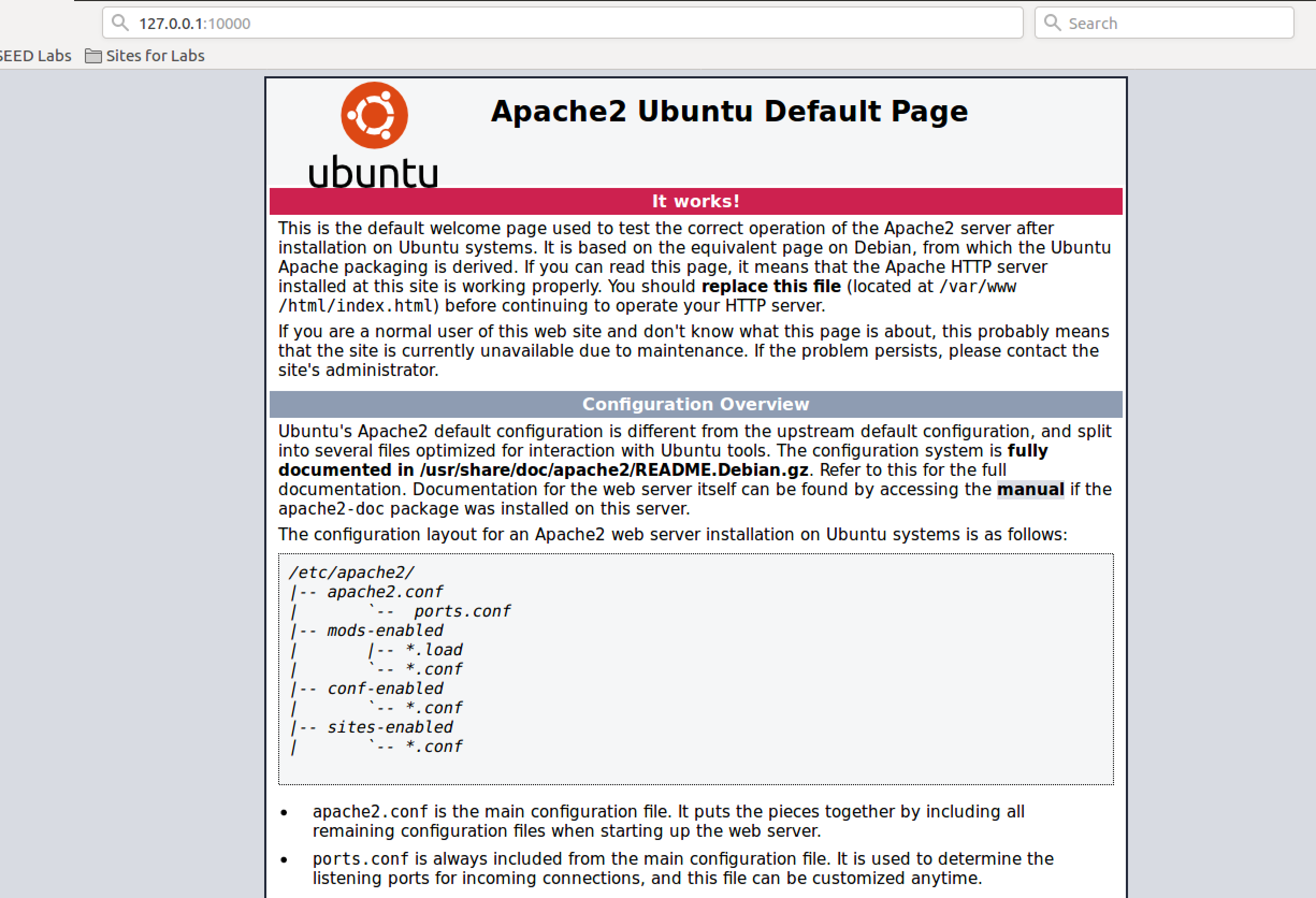
使用ufw禁止外面连接本机（B）的22和80端口



在B中使用命令



在A中输入127.0.0.1:10000



建立反向隧道进行访问。