**信息安全技术实验报告**

|  |  |  |
| --- | --- | --- |
| **实验名称** | **防火墙** | |
| **组长** | **姓名** | **学号** |
|  |  |
| **组员** |  |  |
|  |  |
| 叶梓聪 | 21307417 |
| **实验分工** | | |
| **姓名** | **任务** | |
|  | 完成了XXX | |
|  |  | |
| 叶梓聪 |  | |

表1-1 实验1中的节点名称、用户名及密码

|  |  |  |
| --- | --- | --- |
| **节点名称** | **用户名** | **密码** |
| 正常用户 | imool | imool |
| 代理服务器 | imool | imool |

表1-2 实验2中的节点名称、用户名及密码

|  |  |  |
| --- | --- | --- |
| **节点名称** | **用户名** | **密码** |
| 正常用户 | imool | imool |
| Web&FTP服务器 | imool | imool |
| 外网用户 | kali | kali |

【**交报告**】使用FTP方式提交，推荐使用Filezilla客户端

地址为ftp://ftp.network-security.asia；账号与密码为：student/5ecur1ty

文件以组号（组长学号）+实验名称命名

# 实验目的与实验内容

1. 理解并掌握包过滤防火墙的基本工作原理
2. 理解NetFilter的原理和使用方法
3. 掌握使用NetFilter API实现包过滤防火墙技术
4. 掌握使用iptables设置Netfilter防火墙技术
5. 了解防火墙绕过原理
6. 练习使用socks代理绕过防火墙技术

## 实验1：用Netfilter API实现包过滤防火墙

1. **测试网络连通性，以便验证防火墙效果**
2. **实现简单的包过滤防火墙**
3. 下载示例代码并仔细阅读
4. 防火墙代码编译并加载至内核
5. 防火墙效果测试
6. 卸载编写的内核模块
7. 编码实现一个基本防火墙

* 规则1：禁止正常用户主机访问代理服务器上的Web服务（http://192.168.1.140/），但允许其访问代理服务器上的其它服务。
* 规则2：禁止任何外部主机通过SSH连接正常用户主机，但允许正常用户主机通过SSH连接自己。

1. **测试并验证包过滤防火墙效果**
2. **包过滤防火墙绕过**
3. **思考：如何用Netfilter实现状态检测防火墙**

## 实验2：用iptables命令设置包过滤防火墙

1. **测试网络连通性，以便验证防火墙效果**
2. **使用iptables设置防火墙**

* 规则1：外网主机可以访问Web&FTP服务器上提供的WEB服务和FTP服务
* 规则2：允许内网主机主动连接外网主机，但禁止外网内网主机连接内网主机

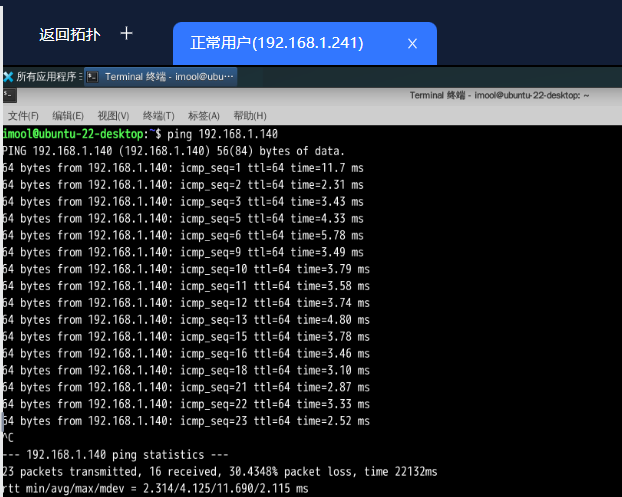
1. **测试并验证防火墙效果**
2. **重要配置命令和验证结果请截图**

# 实验步骤与实验结果记录

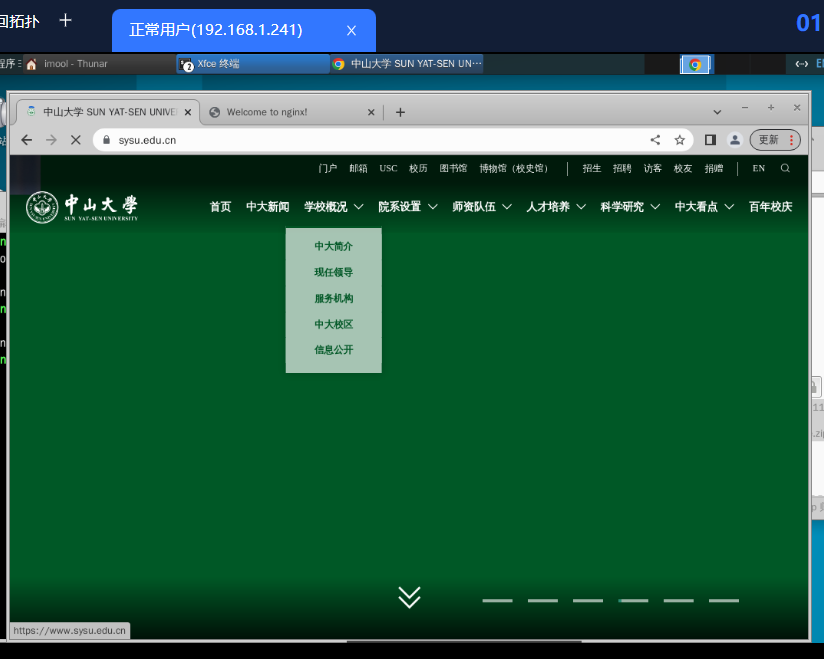
## 实验1：用Netfilter API实现包过滤防火墙

**1.测试网络连通性，以便验证防火墙效果**

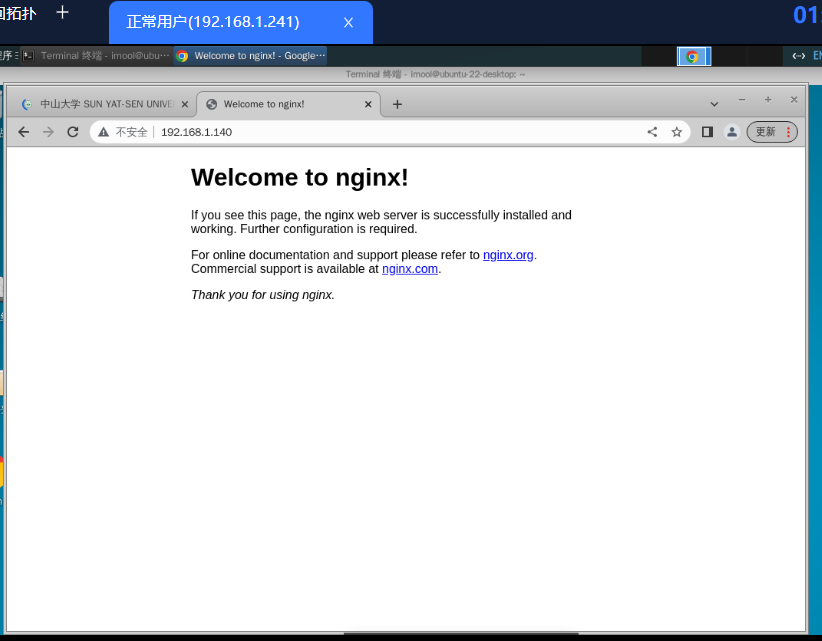
**（1）ping代理服务器**

****

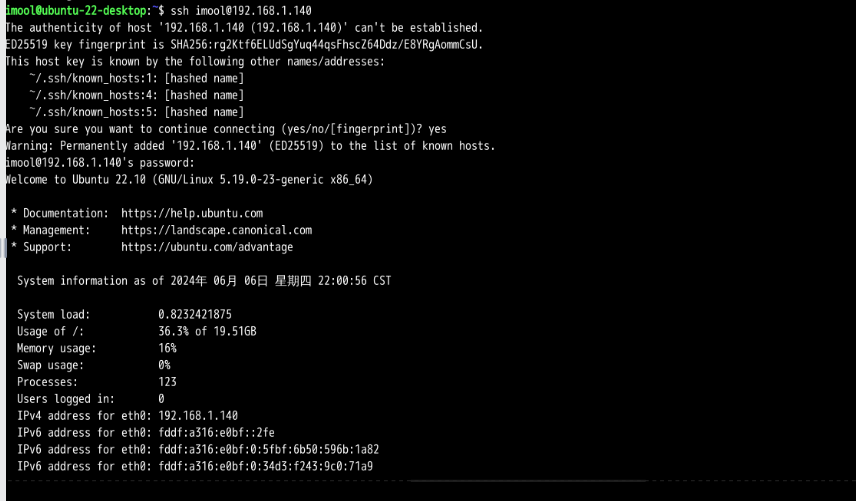
**（2）浏览器访问sysu.edu.cn**

****

**（3）浏览器访问代理服务器**

****

**（4）ssh命令连接代理服务器**

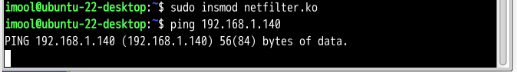
****

**2.实现简单的包过滤防火墙**

（1）下载示例代码并仔细阅读

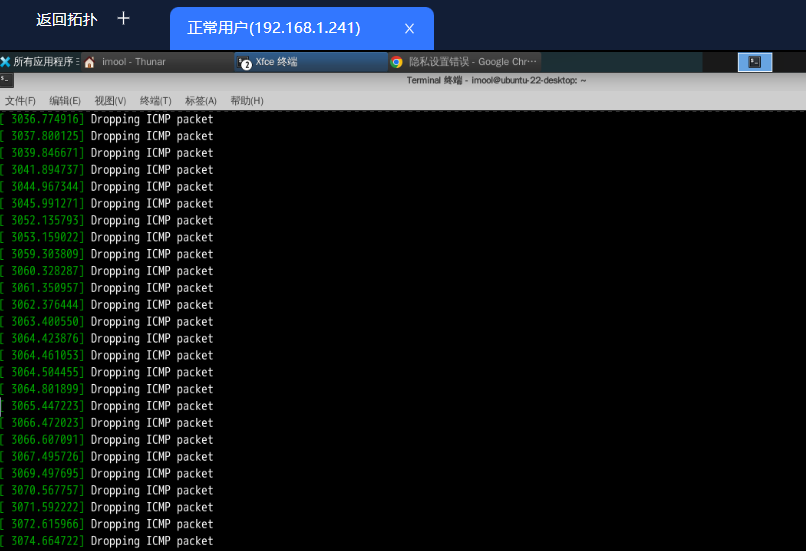
（2）防火墙代码编译并加载至内核

（3）防火墙效果测试



Ping命令是使用ICMP数据包，将内核模块加载到内核中后过滤掉ICMP包，因此无法ping通。

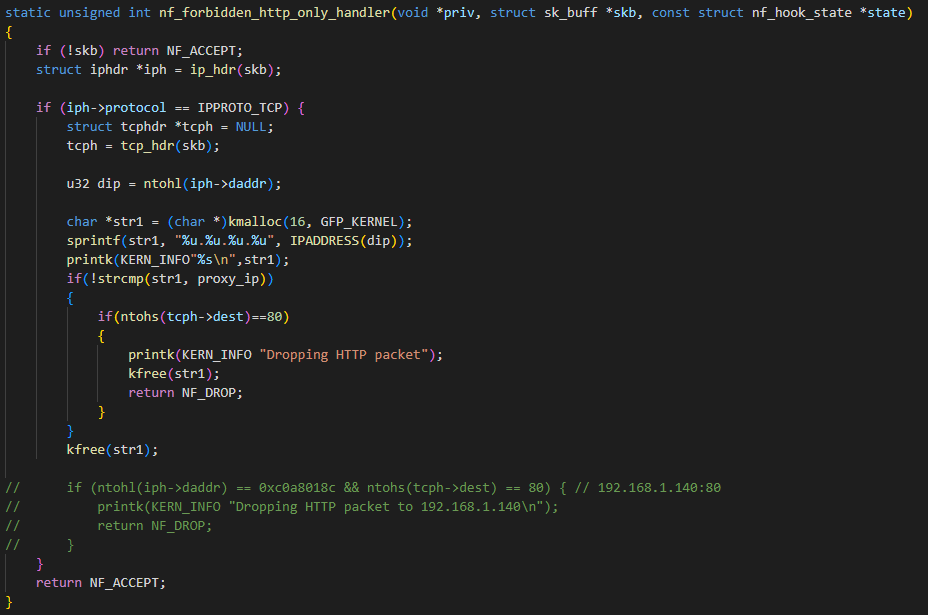
终端运行sudo dmesg -w命令查看实时日志监控：



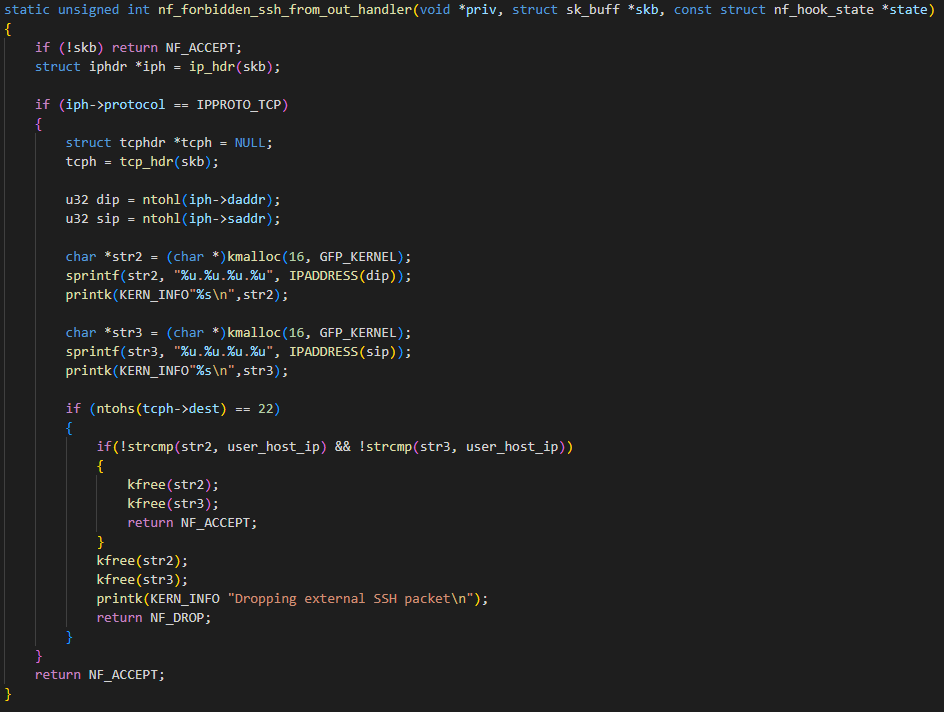
（4）卸载编写的内核模块

（5）编码实现一个基本防火墙

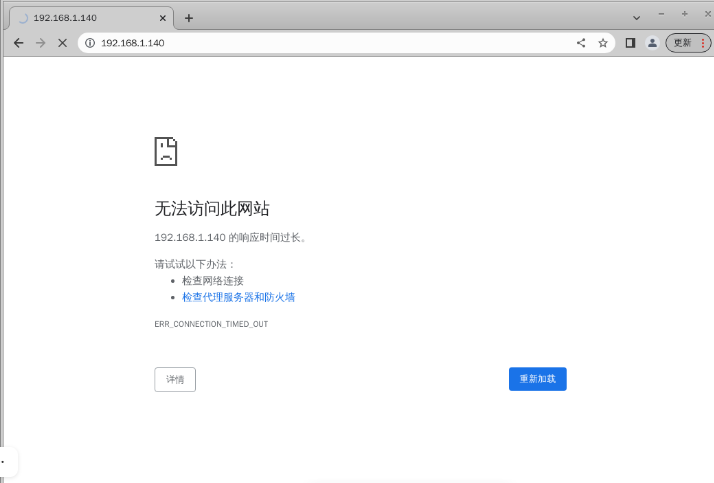
* 规则1：禁止正常用户主机访问代理服务器上的Web服务（http://192.168.1.140/），但允许其访问代理服务器上的其它服务。



* 规则2：禁止任何外部主机通过SSH连接正常用户主机，但允许正常用户主机通过SSH连接自己。



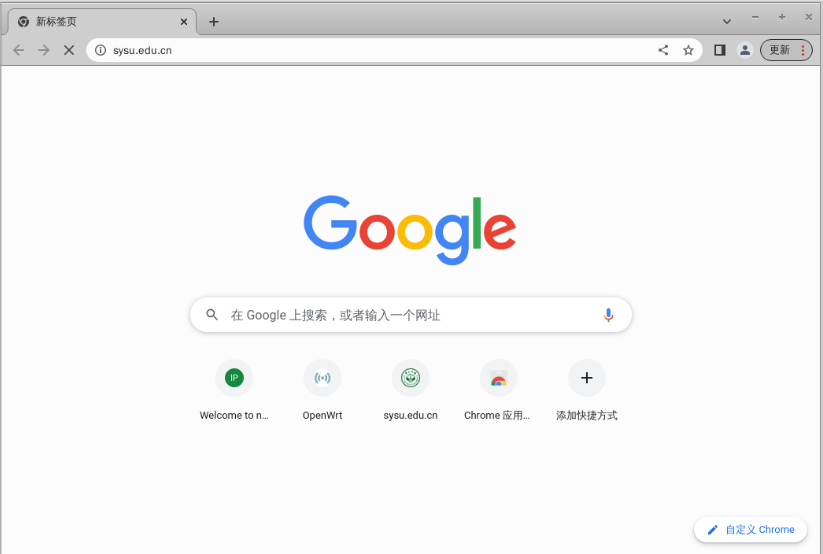
**3.测试并验证包过滤防火墙效果**

****

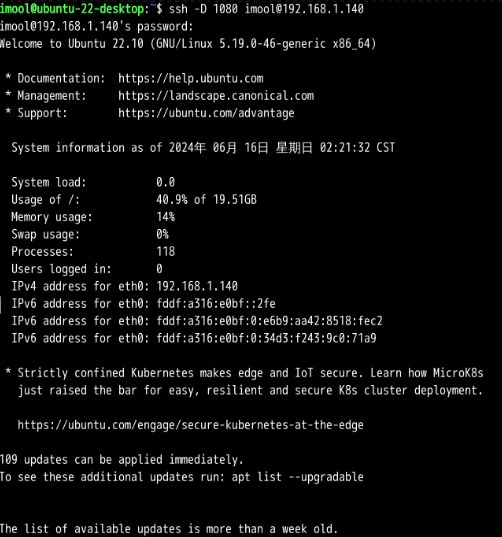
****

**4.包过滤防火墙绕过**

**无法访问**[**http://www.sysu.edu.cn**](http://www.sysu.edu.cn)

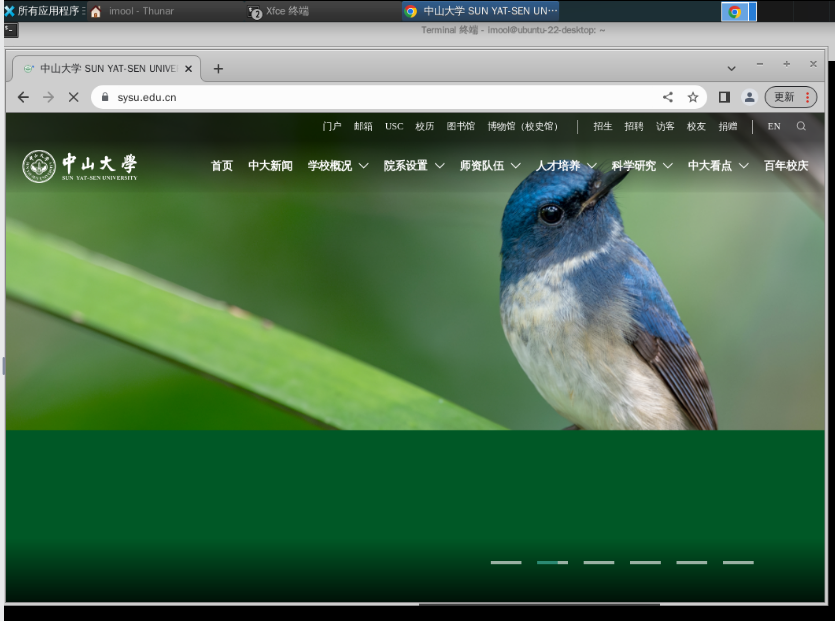
****

开启socks代理服务

****

****

**成功访问**[**http://www.sysu.edu.cn**](http://www.sysu.edu.cn)

****

**5.思考：如何用Netfilter实现状态检测防火墙**

通过实验，总结出以下步骤：  
（1）定义钩子点：在 Netfilter 中注册钩子点，这些钩子点决定了数据包在网络栈中流动时的处理时机。

（2）编写处理函数：为每个钩子点编写处理函数，这些函数将决定数据包是否被允许通过、被拒绝或进行其他操作。

（3）实现规则匹配：定义防火墙规则，并在处理函数中实现对这些规则的匹配逻辑，以决定数据包的命运。

（4）处理超时和资源清理：实现超时机制来清理长时间未活动的连接，以及释放相关资源。

（5）测试与验证：测试验证防火墙效果。

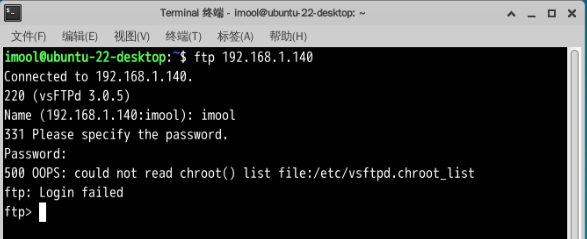
## 实验2：用iptables命令设置包过滤防火墙

**1.测试网络连通性，以便验证防火墙效果**

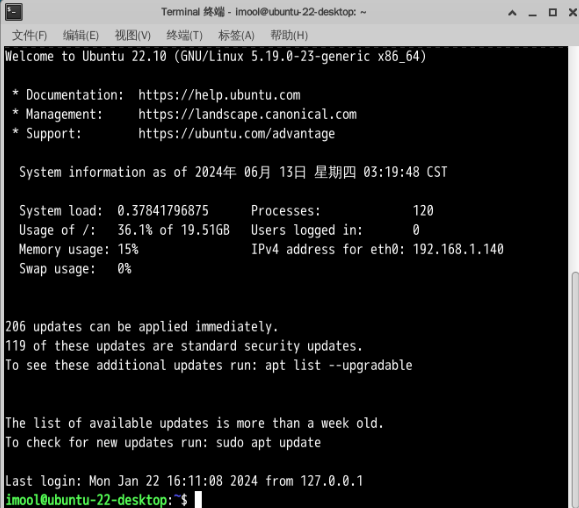
浏览器正常访问192.168.1.140

****

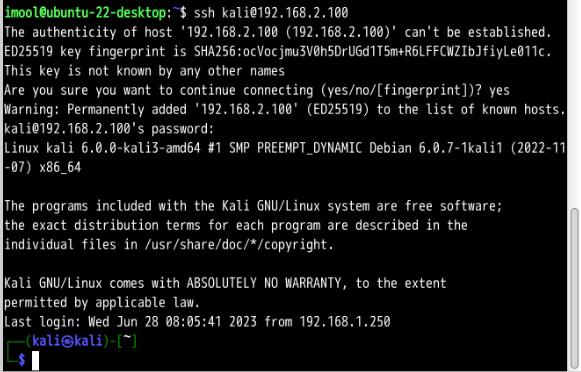
正常连接ftp服务器



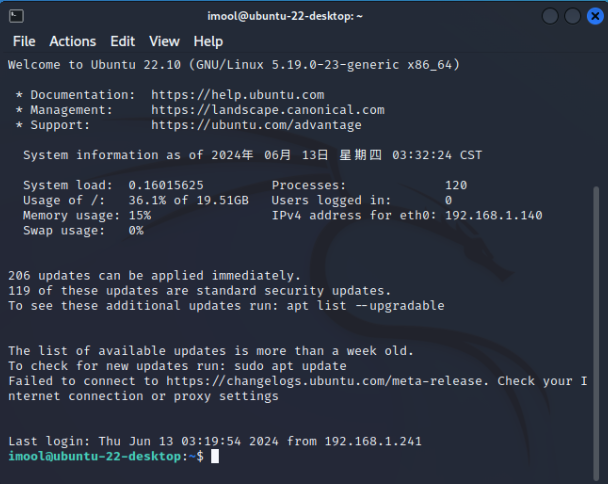
ssh正常连接192.168.1.140

****

正常to kali



Kali to 140



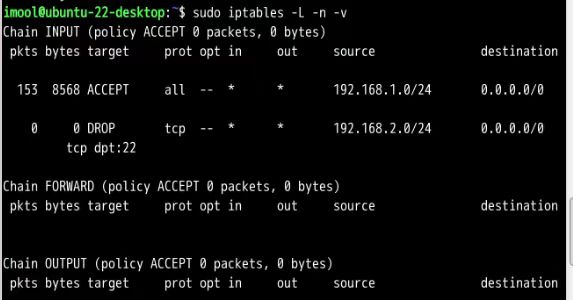
**2.使用iptables设置防火墙**

* 规则1：外网主机可以访问Web&FTP服务器上提供的WEB服务和FTP服务
* 规则2：允许内网主机主动连接外网主机，但禁止外网内网主机连接内网主机

（1）user防火墙配置

iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT

iptables -A INPUT -p tcp --dport 22 -s 192.168.2.0/24 -j DROP



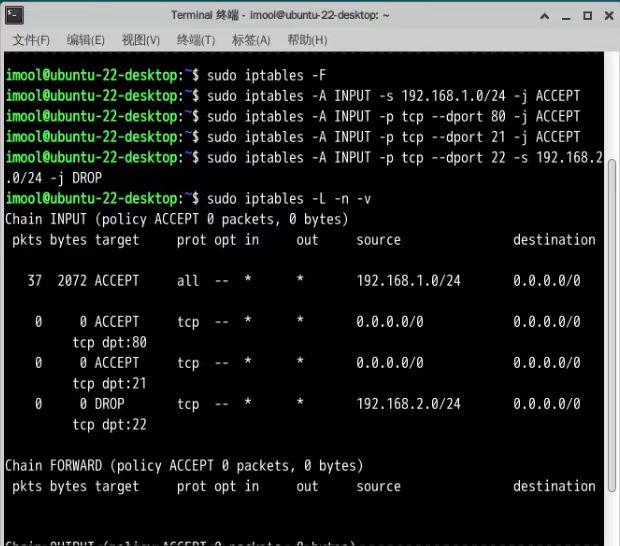
（2）服务器防火墙配置

iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 21 -j ACCEPT

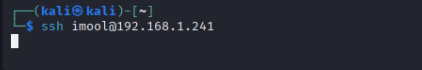
iptables -A INPUT -p tcp --dport 22 -s 192.168.2.0/24 -j DROP



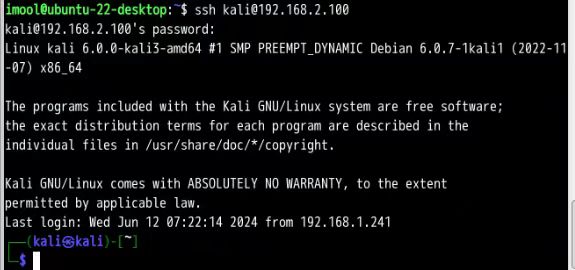
**3.测试并验证防火墙效果**

配置防火墙后：

kali to user

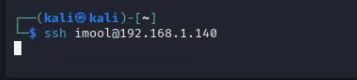


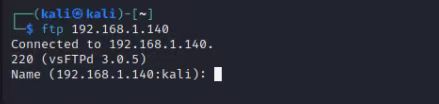
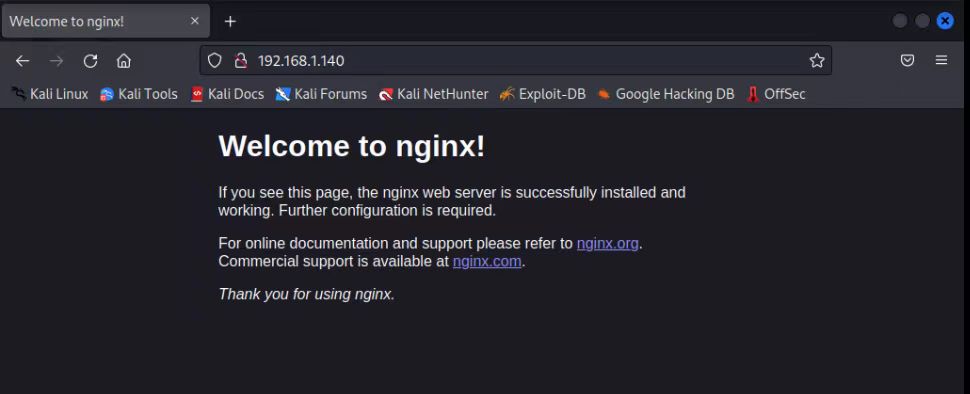
user to kali



配置防火墙后：

kali to 服务器





服务器 to kali

