

哈尔滨工业大学

网络安全课程实验报告

实验二

## 学院：计算机学院

## 班级：1403202

## 学号：1140320206

## 姓名：霍峻杰

## 实验：IPtables

1. **原理。**

IPTABLES 是与最新的 3.5 版本 Linux [内核](https://baike.baidu.com/item/%E5%86%85%E6%A0%B8)集成的 IP 信息包过滤系统。如果 Linux 系统连接到因特网或 LAN、服务器或连接 LAN 和因特网的[代理服务器](https://baike.baidu.com/item/%E4%BB%A3%E7%90%86%E6%9C%8D%E5%8A%A1%E5%99%A8)， 则该系统有利于在 Linux 系统上更好地控制 IP 信息包过滤和[防火墙](https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99)配置。

防火墙在做信息包过滤决定时，有一套遵循和组成的规则，这些规则存储在专用的信 息包过滤表中，而这些表集成在 Linux 内核中。在信息包过滤表中，规则被分组放在我们所谓的链（chain）中。而netfilter/iptables IP 信息包过滤系统是一款功能强大的工具，可用于添加、编辑和移除规则。

虽然 netfilter/iptables IP 信息包过滤系统被称为单个实体，但它实际上由两个组件netfilter 和 iptables 组成。

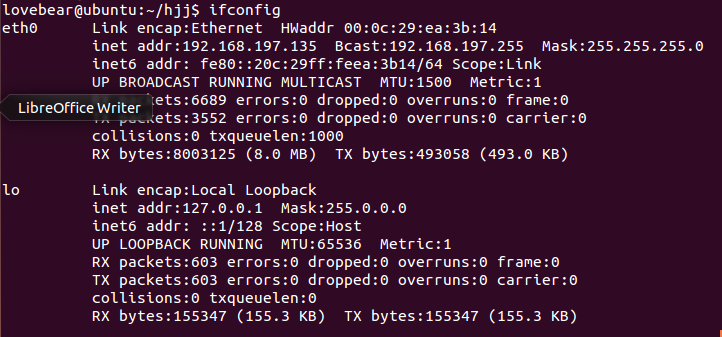
netfilter 组件也称为内核空间（kernelspace），是内核的一部分，由一些信息包过滤表组成，这些表包含内核用来控制信息包过滤处理的规则集。

Iptables 组件是一种工具，也称为用户空间（userspace），它使插入、修改和除去信息包过滤表中的规则变得容易。除非您正在使用 Red Hat Linux 7.1 或更高版本，否则需要下载该工具并安装使用它。

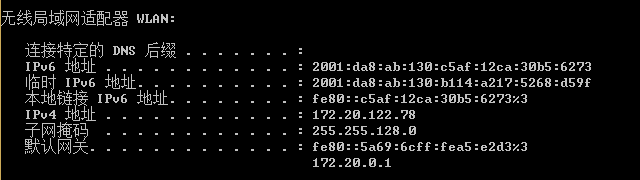
1. **实验结果**

**1.查看ip**

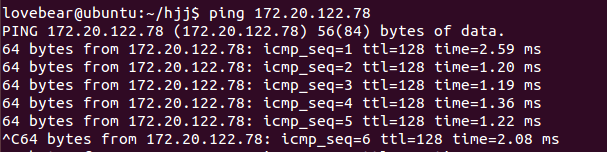
主机1：

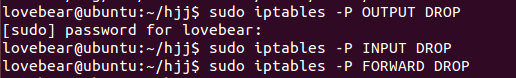


主机2：

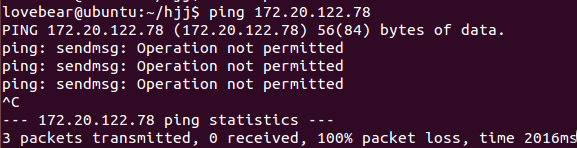


2.测试连通性

3. 任务一：拒绝所有报文



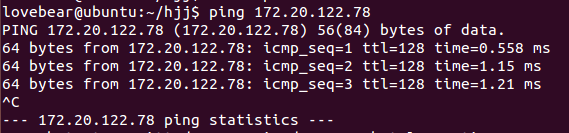
结果：ping不通了



取消配置：

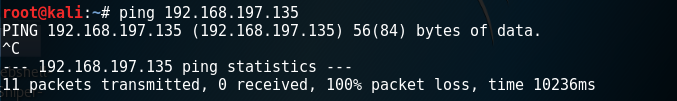


又能ping通

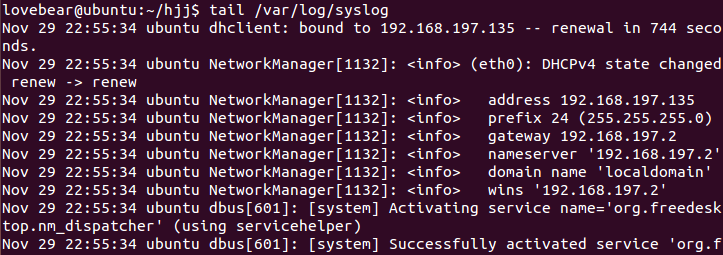


4. 任务二：拒绝某一ip



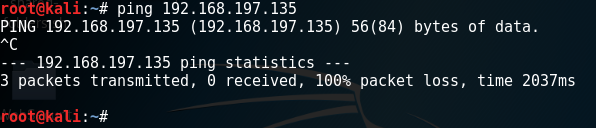


5. 任务三：把对本机的ssh访问通过iptables记录下来，并查看



6.任务四：限制某段时间对本机的访问





三、实验总结

这次实验非常的简单，但是可以利用挖掘的地方很多，由于要考研，就没有深入的挖掘，简单的iptables配置，配置的是linux的默认防火墙（netfilter），比较实用，好多服务器都是linux的，对于网络安全配置非常有用。