广西大学

网络安全课程实验

题目：简易 linux 防火墙设计

学　　院　计算机与电子信息学院

专　　业　信息安全

班　　级　[redacted]

姓　　名　[redacted]

学　　号　[redacted]

2020　年　7　月 6 日

一、 实验目的

开发一个简单的防火墙来过滤发送到 Linux 主机的网络数据包。防火墙必须由一个内核模块和一个应用层控制程序组成。用户可以为防火墙定义过滤规则。

二、 程序设计思路

为实现简单的 linux 包过滤防火墙，需要使用其内置的子系统 netfiter 来完成数据包的过滤操作。Netfiter 在整个网络流程中的若干位置部署了 hook 钩子，可以使用 hook 函数挂载来进行数据包的管理。

为实现过滤发送到 Linux 主机的网络数据包，需要在 INPUT 包过滤点(NF_IP_LOCAL_IN)上部署过滤函数。包含此函数的程序需要运行在内核态中，因安全要求不能在内核模块直接进行配置文件的读取操作，故设计一个用户态的控制程序来进行防火墙配置的加载。

用户态程序和内核态模块通信方式很多，设计之初曾采用 netlink 来进行通信，但存储防火墙规则的结构为结构体定义，使用 netlink 这种类 socket 通信需要将结构体转换为字符串进行传输，在内核模块再将字符串还原成结构体。在此过程中出现了数据丢失变空的问题，多天尝试修复无果，改用 proc 虚拟文件系统来进行配置文件的通信。

内核模块在加载时使用/proc 文件系统创建了存储规则的文件存放于/proc 目录下，用户态控制程序在读取解析用户输入的控制参数后将规则存储进/proc 文件夹下的配置文件中，同时调用了内核模块的读取规则的回调函数，让内核模块进行了规则的读取。

三、 程序测试

内核模块装载：

```
[ 1460.341905] fw: loading out-of-tree module taints kernel.
[ 1460.341908] fw: module license 'unspecified' taints kernel.
[ 1460.341909] Disabling lock debugging due to kernel taint
[ 1460.341942] fw: module verification failed: signature and/or required key mi
ssing - tainting kernel
[ 1460.343990] fw: fw proc entry succesfully registered
[ 1460.343991] fw: fw read_write module loaded successfully
[ 1460.343999] fw: rule match module loaded
mrzhang76@ubuntu:~/TEST/LKM$
```

控制程序输入规则：

1、获取帮助信息

```
mrzhang76@ubuntu:~/TEST/Userspace$ ./app -h
/proc/fw successfully opened for writing
./app: invalid option -- 'h'
Set hook entry: --in --out
Set protol: --protol ALL/TCP/UDP/ICMP
Set ip: --srcip --destip
Set port: --destport --srcport
Set netmask: --srcnetmask --destnetmask
Set action: --action UNBLOCK/BLOCK
Delete rule: --delete
Print rule: --print
help: --help
```

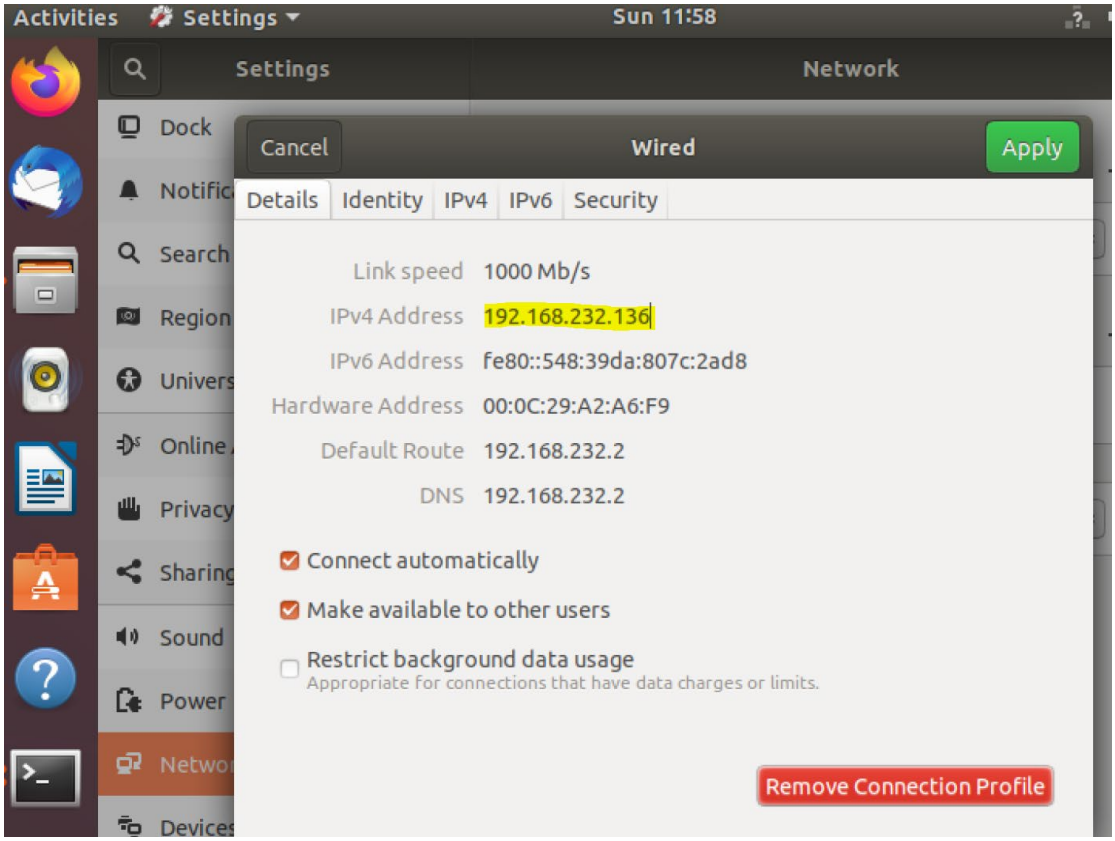
2、输入规则参数

截获所有输入的数据包：./app -in -proto ALL -action BLOCK

```
mrzhang76@ubuntu:~/TEST/Userspace$ ./app --in --proto ALL --action BLOCK
/proc/fw successfully opened for writing
Protocol set
Action set
Hook entry set for this rule: 1
```

3、查看测试结果

测试主机已经不能被 ping 通




```
C:\Users\mrzhang76>ping 192.168.232.136

正在 Ping 192.168.232.136 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.232.136 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，

C:\Users\mrzhang76>
```

输入测试参数：
截取所有出站通讯包./app -out -proto ALL -action BLOCK

```
mrzhang76@ubuntu:~/TEST/Userspace$ ./app --out --proto ALL --action BLOCK
/proc/fw successfully opened for writing
Protocol set
Action set
Hook entry set for this rule: 3
```

查看测试结果：
测试主机已经无法 ping 通外部主机

```
mrzhang76@ubuntu:~/TEST/Userspace$ ping www.baidu.com
ping: www.baidu.com: Name or service not known
mrzhang76@ubuntu:~/TEST/Userspace$ ping www.126.com
ping: www.126.com: Name or service not known
mrzhang76@ubuntu:~/TEST/Userspace$
```

因为所有包都不能出站，连 DNS 查询都无法进行
因实验代码过长，另附代码文件