**实验一 Linux防火墙 实验**

1. **实验目的**

（1）理解防火墙技术的基本工作原理；

（2）理解Linux环境中Netfilter/IPTables的工作机制；

（3）掌握对Netfilter内核模块进行扩展编程的基本方法；

（4）掌握通过IPTables构建防火墙的基本方法。

**2 实验要求**

（1）对Netfilter内核模块进行扩展编程来实现简单的防火墙；

（2）实现基于协议的数据报过滤功能；

（3）实现基于源IP地址的数据报过滤功能；

（4）实现基于目的端口的TCP包过滤功能。

**3 实验内容**

学习Netfilter和内核模块的相关知识，做三个分别基于协议、IP、端口的内核Netfilter模块。加载内核模块，测试防火墙的功能（丢弃某个协议、端口、IP的数据包）。

1. **实验原理**

基于Netfilter的防火墙包含4个文件， filter\_ip.c、filter\_port.c、 filter\_prot.c、 makefile。其中filter\_ip.c中代码实现的功能就是基于源IP地址过滤，filter\_port.c实现了基于目的端口过滤，filter\_prot.c实现了基于协议过滤的功能。这三个源文件中都包含三个函数：

//linux内核编程中的三个函数，初始化、钩子函数、清除模块函数

int init\_module() //初始化函数

//钩子函数，防火墙的核心模块

unsigned int hook\_func(unsigned int hooknum,

struct sk\_buff \*\*skb,

const struct net\_device \*in,

const struct net\_device \*out,

int (\*okfn)(struct sk\_buff \*))

void cleanup\_module() //清除模块

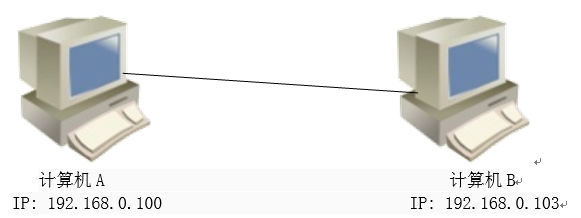
1. **实验环境**

（1）操作系统：Ubuntu 14.04 LTS

（2）编译器：gcc 4.8.4

1. **实验组网**

本实验组网如下图所示：



1. **实验步骤**

**7.1 基于源IP地址过滤的防火墙**

**步骤1** 在计算机A的命令行中开启root权限，否则原始套接字创建会失败。使用命令：su，进入root模式。

**步骤2** 编译源代码。命令行模式下，切换到代码所在目录，输入make后回车即可，编译后将生成三个文件，filter\_ip.ko，filter\_port.ko以及 filter\_prot.ko。

**步骤3** 将相关模块加载到内核。使用命令insmod ./filter\_ip.ko将基于源IP地址的过滤模块加载到内核。

**步骤4** 通过计算机B ping 计算机A，观察 ping 命令结果。

**步骤5** 在计算机A中，通过dmesg命令查看系统内核日志结果。

**7.2基于协议过滤的防火墙**

**步骤1** 在计算机A中，首先移除上个实验中加载的内核模块。使用命令rmmod ./filter\_ip.ko卸载基于源IP地址的过滤模块。

**步骤2** 加载基于协议过滤的内核模块。使用命令insmod ./filter\_prot.ko，加载基于协议过滤的内核模块。

**步骤3** 通过计算机A的浏览器浏览网页，观察结果，并通过dmesg命令查看系统内核日志结果。

**步骤4** 通过计算机B ping 计算机A，观察 ping 命令结果。

**步骤5** 在计算机A中，通过dmesg命令查看系统内核日志结果。

**7.3基于端口的防火墙**

**步骤1** 在计算机A中，首先移除上个实验中加载的内核模块。使用命令rmmod ./filter\_prot.ko卸载基于协议过滤的内核模块。

**步骤2** 加载基于端口过滤的内核模块。使用命令insmod ./filter\_port.ko，加载基于端口过滤的内核模块。

**步骤3** 通过计算机A的浏览器浏览网页，观察结果，并通过dmesg命令查看系统内核日志结果。

**步骤4** 开启计算机A的telnet服务。使用netstat -a | grep telnet命令查看telnet运行状态，如果输出为空，表示没有开启该服务，按下面步骤进行配置，否则跳转到步骤9。

**步骤5** 安装openbsd-inetd。使用命令：

sudo apt-get install openbsd-inetd

**步骤6** 安装telnetd。使用命令：

sudo apt-get install telnetd

安装完成后，查看/etc/inetd.conf的内容，使用命令：

cat/etc/inetd.conf | grep telnet

可以看到输出结果：

telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd。

**步骤7** 重启openbsd-inetd。使用命令：

sudo /etc/init.d/openbsd-inetd restart

**步骤8** 再次查看telnet运行状态。使用命令：

netstat -a | grep telnet

输出结果为：

tcp 0 0 \*:telnet \*:\* LISTEN

**步骤9** 通过计算机B telnet 计算机A。在本实验组网中，应使用命令：telnet 192.168.0.103。观察telnet 结果。

**步骤10** 在计算机A中，通过dmesg命令查看系统内核日志结果。

1. **预期实验结果**

**8.1基于源IP地址过滤的防火墙**

（1）计算机B ping 计算机A，结果为ping不通。

（2）dmesg查看系统内核日志结果：

[15551.780448] <0>A Packet from 192.168.0.103: DROP

[15551.983050] <0>A Packet from 192.168.0.103: DROP

[15552.744910] <0>A Packet from 192.168.0.103: DROP

[15553.507072] <0>A Packet from 192.168.0.103: DROP

[15559.967063] <0>A Packet from 192.168.0.103: DROP

[15564.647126] <0>A Packet from 192.168.0.103: DROP

**8.2基于协议过滤的防火墙**

（1）打开浏览器访问任意网页会出现：TCP Packet: ACCEPT。

（2）计算机B ping 计算机A，结果为ping不通，且会出现：ICMP Packet: DROP。

（3）dmesg查看系统内核日志结果：

[15856.363848] UDP Packet: ACCEPT

[15856.365348] UDP Packet: ACCEPT

[15857.352104] ICMP Packet: DROP

[15857.393037] UDP Packet: ACCEPT

[15858.349136] ICMP Packet: DROP

[15858.619495] Unknown Packet: DROP

[15859.346371] ICMP Packet: DROP

[15859.347516] UDP Packet: ACCEPT

[15859.348672] UDP Packet: ACCEPT

[15859.595523] UDP Packet: ACCEPT

[15860.343313] TCP Packet: ACCEPT

**8.3基于端口的防火墙**

（1）使用计算机A浏览网页时，在终端上用dmesg查看系统内核日志结果：

[16111.147887] <0>PORT Number is not 23: ACCEPT

[16111.151895] <0>PORT Number is not 23: ACCEPT

[16111.191990] <0>PORT Number is not 23: ACCEPT

（2）从计算机B telnet 计算机A时，无法连接，且在计算机A上用dmesg查看系统内核日志结果：

[ 1285.562248] <0>A TCP Packet PORT 23: DROP

[ 1288.560891] <0>A TCP Packet PORT 23: DROP

[ 1294.563451] <0>A TCP Packet PORT 23: DROP