本学期实验总体安排

- **课程主页及指导书**地址：https://hitsz-cslab.gitee.io/net-work-security/
- **SEED实验室的链接：**https://seedsecuritylabs.org/
- **实验提交地址（校内网/VPN）：** http://grader.tery.top:8000/#/login

网络安全实验

Lab6　Firewall

CONTENTS

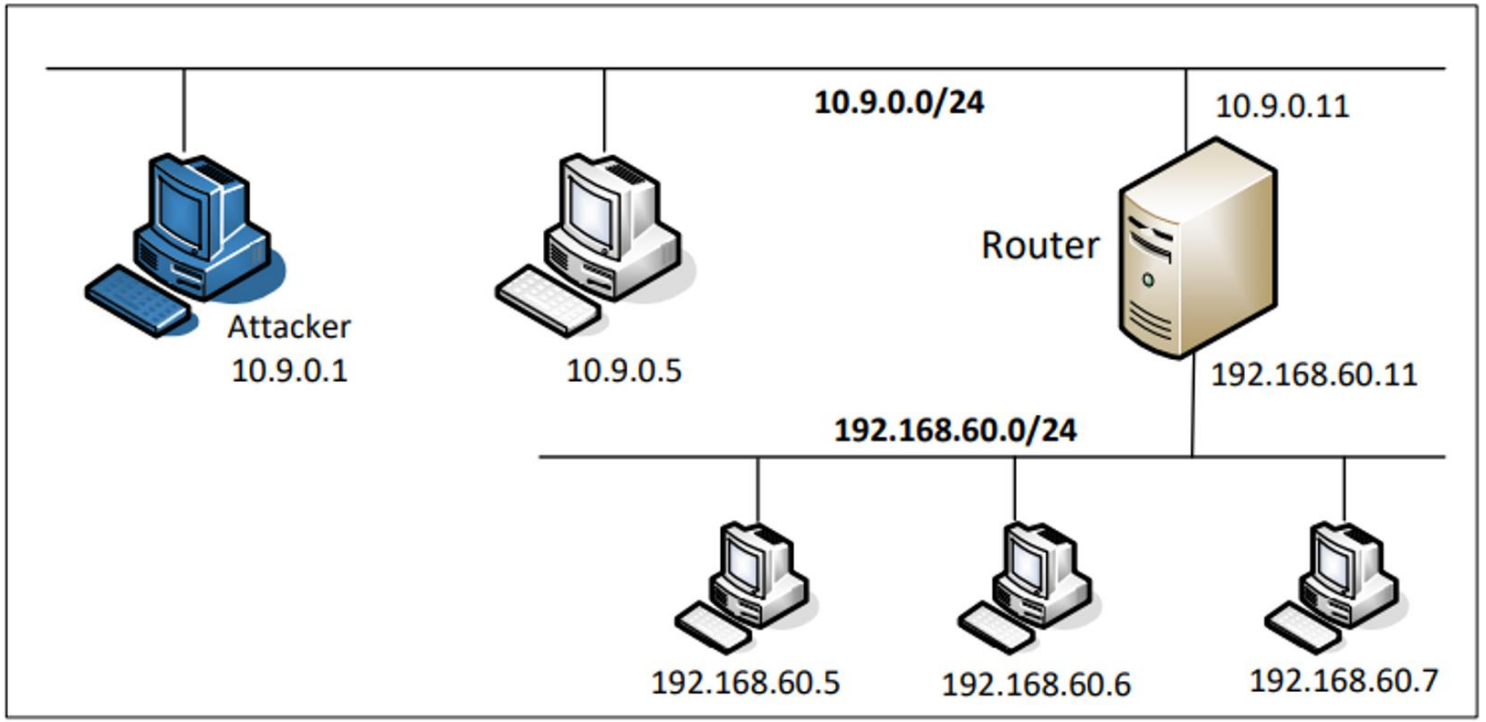
目录

实验目的

- 理解防火墙和入侵检测的机制和作用
- 掌握iptable防火墙设置
- 了解Netfilter架构

实验任务

本次实验通过使用Netfilter实现一个简单的数据包过滤器，并用Linux内置的防火墙iptables搭建一个简单的防火墙。网络拓扑图如下所示。



实验原理

1 什么是防火墙

- 对经过的数据流进行解析，并实现访问控制及安全防护功能的网络安全产品。
- 根据安全目的、实现原理的不同，又将防火墙分为网络型防火墙、Web应用防火墙、数据库防火墙和主机型防火墙等。
- 网络防火墙主要保护整个内部网络，Web应用防火墙保护的是Web应用服务器，数据库防火墙保护的是数据库管理系统，而主机防火墙则要保护的对象是个人主机或服务器。

实验原理

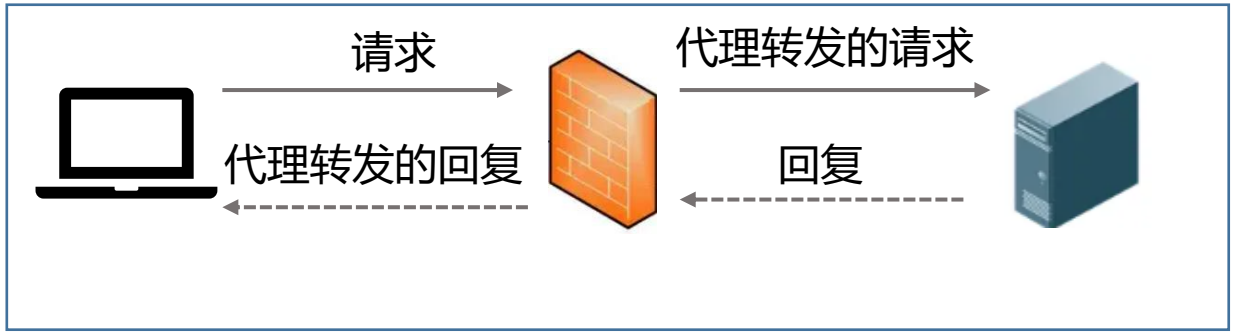
2 ➢ 常见的三种防火墙技术

包过滤技术

包头信息（源和目的IP地址、端口号、标志位等）

状态检测技术

应用代理技术



实验原理

3 开源防火墙Linux iptables

- 从内核2.4开始之后使用实现了一个具有包过滤、数据包处理、网络地址转换等防火墙功能的iptables，iptables也是基于Nefilter框架。

- Netfilter在数据包经过的路径上放置了一些钩子（hook），它们位于内核中。自行编写的函数可以通过内核模块放进内核，并挂在那些钩子上。当数据包到达某个钩子时，挂在钩子上面的函数就会被调用，可以在函数中对数据包进行审查和过滤，并告诉Netfilter如何处理。

实验原理

4 ➢ Netfilter中对数据包的5种处理结果

(1) NF_ACCEPT: 允许数据包通过。

(2) NF_DROP: 丢弃数据包，这样数据包将不会在网络协议种继续传输。

(3) NF_QUEUE: 使用 nf_queue 机制将数据包传递到用户空间处理。

(4) NF_STOLEN: 告知 Netfilter 框架忽略这个数据包。

(5) NF_REPEAT: 请求 Netfilter 框架再次调用这个模块。

实验原理

5 ➢ Netfilter中对数据包的5种处理结果

(1) NF_INET_PRE_ROUTING: 除了混杂模式，所有数据包都将经过这个钩子点

(2) NF_INET_LOCAL_IN: 数据包要进行路由判决，以决定需要被转发还是发往本机

(3) NF_INET_FORWARD: 需要被转发的数据包会到达这个钩子点

(4) NF_INET_LOCAL_OUT: 这是本机产生的数据包到达的第一个钩子点

(5) NF_INET_POST_ROUTING: 需要被转发或由本机产生的数据包都会经过这个钩子点

6 ➢ Netfilter中的表

1、Filter是默认的规则表，用于一般数据包的过滤

- INPUT链里的规则用于处理目的地址是本地主机的数据包。
- OUTPUT链里的规则用于处理从本地主机发出的数据包。
- FORWORD链里的规则用于处理在一个网络接口收到的，而且需要转发到另一个网络接口的所有数据包。

实验原理

6 ➢ Netfilter中的表

2、Nat表：Nat表主要用于网络地址转换NAT，该表可以实现一对一、一对多和多对多的NAT工作，iptables就是使用该表实现共享上网功能的。

- PREROUTING链是在包刚刚到达防火墙时改变它的目的地址。
- OUTPUT链是改变本地产生的包的目的地址。
- POSTROUTING链是在包就要离开防火墙之前改变其源地址。

实验原理

6 ➢ Netfilter中的表

3、Mangle表：Mangle表主要用于对指定的包进行修改。

- PREROUTING链是在包进入防火墙以后、路由判断之前改变包。
- POSTROUTING链是在所有路由判断之后改变包。
- OUTPUT链是在确定包的目的之前更改数据包.
- INPUT链是在包被路由到本地之后，但在用户空间的程序看到它之前改变包。
- FORWORD链是在最初的路由判断之后、最后一次更改包的目的之前改变数据包包头。

实验原理

6 ➢ Netfilter中的表

Table 1: `iptables` Tables and Chains

Table	Chain	Functionality

filter	`INPUT`
	`FORWARD`
	`OUTPUT`
		Packet filtering

nat	`PREROUTING`
	`INPUT`
	`OUTPUT`
	`POSTROUTING`
		Modifying source or destination network addresses

mangle	`PREROUTING`
	`INPUT`
	`FORWARD`
	`OUTPUT`
	`POSTROUTING`
		Packet content modification

实验原理

7 ➢ iptables

iptables命令的一般格式为

iptables [-t table] -CMD chain CRETIRIA -j ACTION

iptables命令用法举例

[root@tp ~]# iptables -F　//清除预设表filter中的所有规则链的规则

[root@tp ~]# iptables -X　//清除预设表filter中使用者自定链中的规则

[root@tp ~]# /etc/rc.d/init.d/iptables save //写到/etc/sysconfig/iptables文件里

[root@tp ~]# service iptables restart　//重启防火墙

实验原理

7 ➢ iptables

iptables命令示例

```
[root@tp ~]# iptables -p INPUT DROP  //设定预设规则 INPUT DROP
[root@tp ~]# iptables -p OUTPUT ACCEPT  //设定预设规则 OUTPUT ACCEPT
[root@tp ~]# iptables -p FORWARD DROP  //设定预设规则 FORWARD DROP
[root@tp ~]# iptables -A INPUT -p tcp --dport 22 -j ACCEPT  //开启远程SSH 22端口
[root@tp ~]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT  //开启WEB服务器 80端口
[root@tp ~]# iptables -A INPUT -p tcp --dport 110 -j ACCEPT //开启邮寄服务器110端口
[root@tp ~]# iptables -A INPUT -p tcp --dport 25 -j ACCEPT  //开启邮寄服务器25端口
[root@tp ~]# iptables -A INPUT -p tcp --dport 21 -j ACCEPT  //开启FTP服务器21端口
[root@tp ~]# iptables -A INPUT -p tcp --dport 20 -j ACCEPT  //开启FTP服务器20端口
[root@tp ~]# iptables -A INPUT -p tcp --dport 53 -j ACCEPT  //开启DNS服务器53端口
[root@tp ~]# iptables -A INPUT -p icmp -j ACCEPT //允许icmp包通过
[root@tp ~]# iptables -A OUTPUT -p tcp --sport 31337 -j DROP //减少不安全的端口连接
[root@tp ~]# iptables -A OUTPUT -p tcp --dport 31337 -j DROP //减少不安全的端口连接
```

实验步骤

Task1 使用Netfilter技术实现一个简单的防火墙

Task1.1 实现一个简单的内核模块

Task1.2 使用Netfilter 搭建阻止 UDP, ICMP 和 TCP的防火墙

Task2 使用 iptables 配置无状态防火墙规则

Task2.1 配置防火墙规则，保护 Router，只能 ping 命令通过

Task2.2 配置防火墙规则，保护内网

作业提交

提交内容：实验报告（有模板）

截止时间：

下周一提交至HITsz Grader 作业提交平台，具体截止日期参考平台发布。

- 登录网址：： http://grader.tery.top:8000/#/login
- 推荐浏览器： Chrome
- 初始用户名、密码均为学号，登录后请修改

注意

上传后可自行下载以确认是否正确提交

同学们
请开始实验吧！