《物联网安全》实验课

网络安全配置管理 —— 防火墙

目录

PART 01

基础原理

BASIC PRINCIPLE

防火墙

作为一种访问控制的机制是确保网络安全的重要手段

Linux操作系统上的防火墙软件特点显著

优势

- 系统稳定
- 系统健壮
- 价格低廉

包含了建立Internet所需的所有服务软件包

实验原理

- iptables简介
- iptables基础
- iptables和netfilter的关系
- iptables传输数据包的过程
- iptables的规则表和链

实验原理

- iptables简介
- iptables基础
- iptables和netfilter的关系
- iptables传输数据包的过程
- iptables的规则表和链

netfilter/iptables

免费的包过滤防火墙

代替昂贵的商业防火墙解决方案

封包过滤　　封包重定向　　网络地址转换（NAT）

实验原理

- iptables简介
- iptables基础
- iptables和netfilter的关系
- iptables传输数据包的过程
- iptables的规则表和链

实验原理

- iptables简介
- iptables基础
- iptables和netfilter的关系
- iptables传输数据包的过程
- iptables的规则表和链

iptables 防火墙管理工具，位于/sbin/iptables

netfilter Linux内核中实现包过滤的内部结构

实验原理

- iptables简介
- iptables基础
- iptables和netfilter的关系
- iptables传输数据包的过程
- iptables的规则表和链

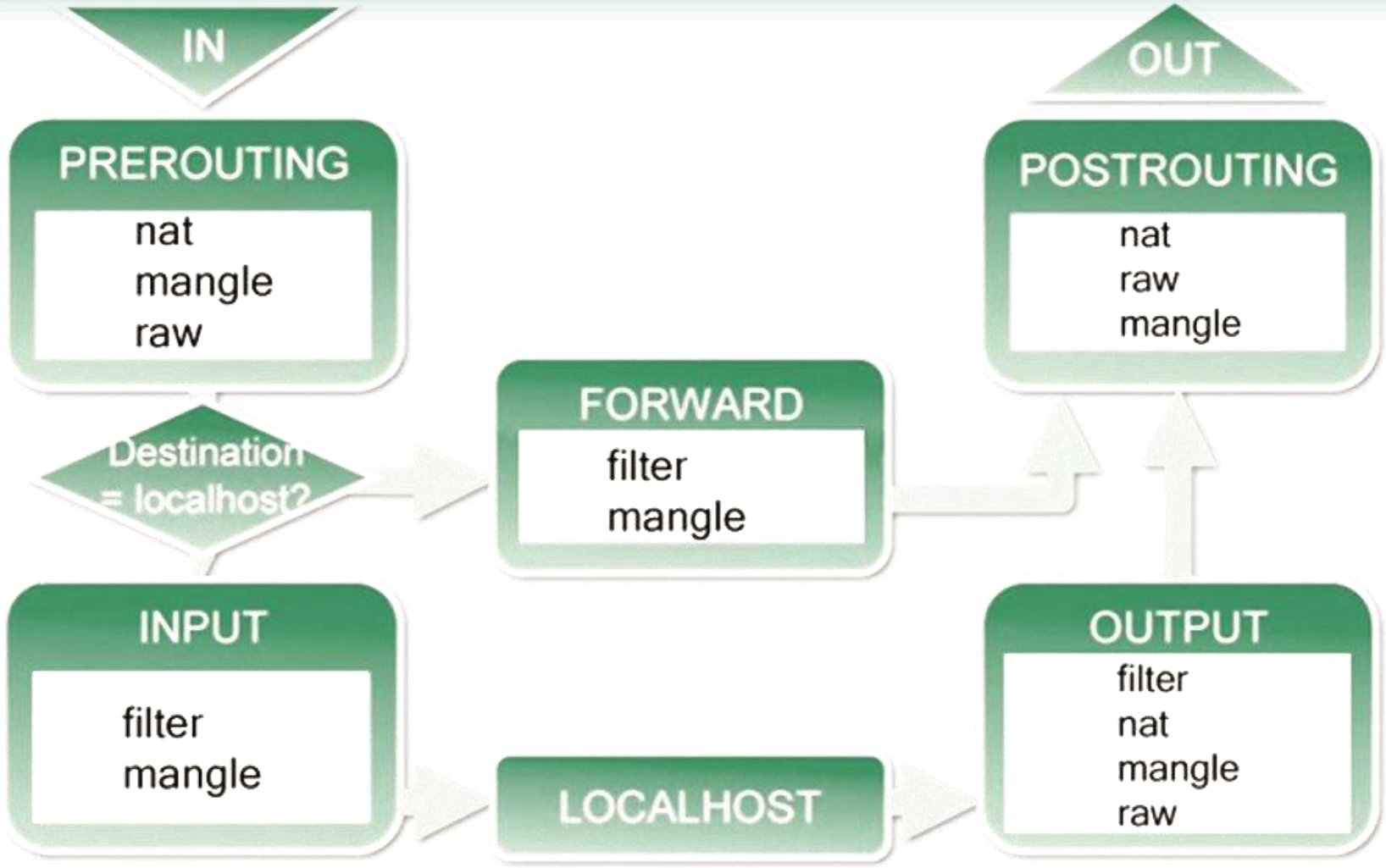
当一个数据包进入网卡时，它首先进入PREROUTING链，内核根据数据包目的IP判断是否需要转送出去。

如果数据包就是进入本机的，它就会沿着图向下移动，到达INPUT链。数据包到了INPUT链后，任何进程都会收到它。本机上运行的程序可以发送数据包，这些数据包会经过OUTPUT链，然后到达POSTROUTING链输出。

如果数据包是要转发出去的，且内核允许转发，数据包就会如图所示向右移动，经过FORWARD链，然后到达POSTROUTING链输出。

实验原理

- iptables简介
- iptables基础
- iptables和netfilter的关系
- iptables传输数据包的过程
- iptables的规则表和链



实验原理

- iptables简介
- iptables基础
- iptables和netfilter的关系
- iptables传输数据包的过程
- iptables的规则表和链

表 (tables)

提供特定的功能

- filter表：包过滤
- nat表：网络地址转换
- mangle表：包重构(修改)
- raw表：数据跟踪处理

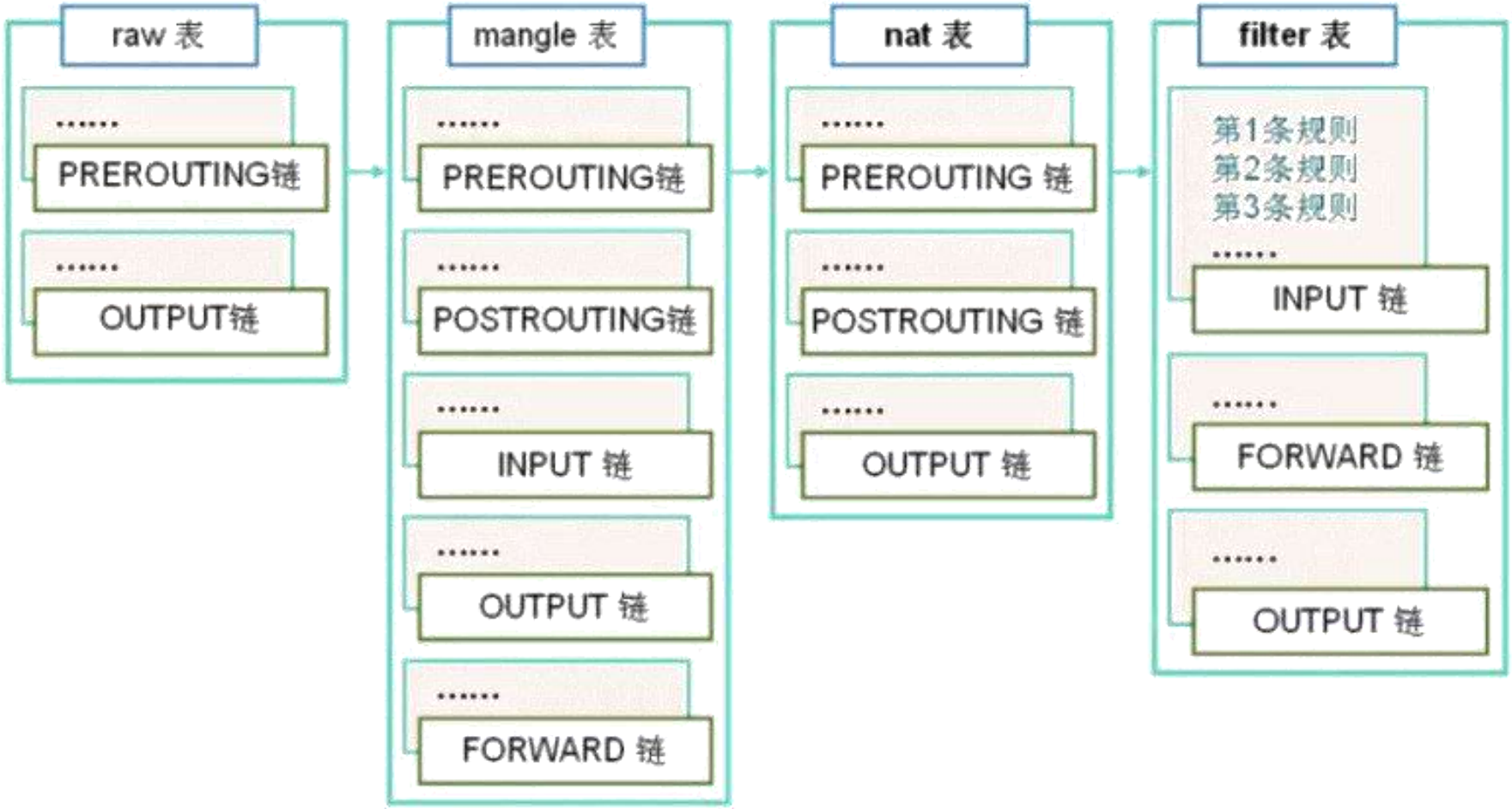
链 (chains)

数据包传播的路径

每一条链其实就是众多规则中的一个检查清单，每一条链中可以有一 条或数条规则。当一个数据包到达一个链时，iptables就会从链中第一条规则开始检查，看该数据包是否满足规则所定义的条件。

实验原理

- iptables简介
- iptables基础
- iptables和netfilter的关系
- iptables传输数据包的过程
- iptables的规则表和链



PART 02

实验环境

EXPERIMENTAL ENVIRONMENT

实验环境

装有Linux系统的虚拟机

Wireshark等抓包工具

Nmap端口扫描工具

PART 03

实验步骤

EXPERIMENTAL PROCEDURE

实验步骤

01 搭建实验环境

将虚拟机IP地址配置到和宿主机一个网段即可，
注意地址不可与其他地址冲突。
关闭宿主机防火墙后，此时A和B是可以互ping的。

02 启动虚拟机的防火墙

```
sudo modprobe ip_tables
sudo ufw enable
sudo ufw reload
```

03 清除filter表中的规则

```
sudo iptables –F
sudo iptables -P INPUT DROP
sudo iptables -P OUTPUT DROP
sudo iptables -P FORWARD DROP
```

04 进行ping命令限制并检验

05 防止端口扫描

实验步骤

06 防止 ping 攻击（1）

允许一个包每秒，触发条件是10个包
sudo iptables -A INPUT -p icmp -m limit --limit 1/s --limit-burst 10 -j ACCEPT
sudo iptables -A OUTPUT -s 192.168.19.133 -d 192.168.19.1 -p icmp -j ACCEPT

07 防止 ping 攻击（2）

允许一个包每分钟，触发条件是10个包
sudo iptables -A INPUT -p icmp -m limit --limit 1/m --limit-burst 10 -j ACCEPT
sudo iptables -A OUTPUT -s 192.168.19.133 -d 192.168.19.1 -p icmp -j ACCEPT

08 防止 ping 攻击（3）

sudo iptables -A FORWARD -f -m limit --limit 100/s --limit-burst 100 -j ACCEPT
sudo iptables -A OUTPUT -s 192.168.19.133 -d 192.168.19.1 -p icmp -j ACCEPT

09 丢弃坏的 TCP 包

sudo iptables -A FORWARD -p TCP ! --syn -m state --state NEW -j DROP
sudo iptables -N syn-flood
sudo iptables -A INPUT -p tcp --syn -j syn-flood
sudo iptables -A syn-flood -p tcp -m limit --limit 3/s --limit-burst 6 -j RETURN
sudo iptables -A syn-flood -j REJECT

10 屏蔽指定IP

BLOCK_THIS_IP="x.x.x.x"
iptables -A INPUT -i eth0 -p tcp -s "$BLOCK_THIS_IP" -j DROP

实验步骤

11 配置服务项

```
iptables -A INPUT -i eth0 -p tcp -s
192.168.100.0/24 --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22 -
m state --state ESTABLISHED -j ACCEPT
```

12 网口转发配置

```
iptables -A FORWARD -i eth0 -o eth1 -j
ACCEPT
```

PART 04

验收考核

Inspection And Acceptance

验收考核

1.按照实验指导书独立完成实验

2.完成实验报告及思考题

谢谢观看