实验 12 Linux中的iptables防火墙设置

实验目的

掌握Iptables防火墙的工作原理，以及配置使用方法。

实验内容

执行下列步骤，对照结果，思考iptables规则的含义。

实验前提

本实验需要使用ubuntu server 1604虚拟机完成。

请预先建立快照或克隆备份。

实验步骤

1.列出iptables中当前所有的规则。

```
sudo iptables -n -L -v
```

2.列出iptables中当前所有的规则，使用数字形式显示。

```
iptables -n -L -v --line-numbers
```

3.列出所有INPUT链中的规则。

```
iptables -L INPUT
```

4.打印出所有OUTPUT链中的规则。

```
iptables -L OUTPUT -n -v --line-numbers
```

5.删除所有的规则、所有的链、接受所有出入流量。

```
sudo iptables -P INPUT ACCEPT
sudo iptables -P FORWARD ACCEPT
sudo iptables -P OUTPUT ACCEPT

sudo iptables -t nat -F
sudo iptables -t mangle -F
sudo iptables -F
sudo iptables -X
```

6.插入下列规则，说明其含义。

```
iptables -I INPUT 2 -s 202.54.1.2 -j DROP
```

7.允许loopback连接。

```
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A OUTPUT -o lo -j ACCEPT
```

8.允许已经建立的连接和相关连接产生的入站流量

```
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

9.允许已经建立的出站流量。

```
sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

10.删除无效的数据包

```
sudo iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
```

11.阻塞某ip地址发来的数据包

```
sudo iptables -A INPUT -s 192.168.252.10 -j DROP
```

12.阻止连接到某个网卡接口

```
sudo iptables -A INPUT -i ens33 -s 192.168.252.10 -j DROP
```

13.允许所有SSH入站流量

```
sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

14.允许特定IP地址或子网来的SSH流量

```
sudo iptables -A INPUT -p tcp -s 192.168.240.0/24 --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

15.允许出站SSH流量

```
sudo iptables -A OUTPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

16.允许特定IP地址或子网的Rsync

```
sudo iptables -A INPUT -p tcp -s 192.168.240.0/24 --dport 873 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 873 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

17.允许所有入站的HTTP流量。

```
sudo iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

17.允许所有入站的HTTPs流量。

```
sudo iptables -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 443 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

18.允许特定IP地址或子网的MYSQL

```
sudo iptables -A INPUT -i ens33 -p tcp --dport 3306 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -o ens33 -p tcp --sport 3306 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

19.允许流经特定网卡的postgresql流量

```
sudo iptables -A INPUT -i ens33 -p tcp --dport 5432 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -o ens33 -p tcp --sport 5432 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

20.阻塞SMTP mail出站

```
sudo iptables -A OUTPUT -p tcp --dport 25 -j REJECT
```

21.允许所有入站SMTP流量

```
sudo iptables -A INPUT -p tcp --dport 25 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 25 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

22.允许所有入站POP3、POP3S流量

```
sudo iptables -A INPUT -p tcp --dport 110 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 110 -m conntrack --ctstate ESTABLISHED -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 995 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 995 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

23.记日志并扔掉包

```
sudo iptables -A INPUT -i ens33 -s 10.0.0.0/8 -j LOG --log-prefix "IP_SPOOF A: "
sudo iptables -A INPUT -i ens33 -s 10.0.0.0/8 -j DROP
```

24.MAC 地址过滤

```
sudo iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP
sudo iptables -A INPUT -p tcp --destination-port 22 -m mac --mac-source 00:0F:EA:91:04:07 -j ACCEPT
```

25.阻止或允许ICMP ping

```
sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
sudo iptables -A INPUT -i ens33 -p icmp --icmp-type echo-request -j DROP
```

26.使用多端口模块设定多端口规则。

```
sudo iptables -A INPUT -i ens33 -p tcp -m state --state NEW -m multiport --dports ssh,smtp,http,https -j ACCEPT
```

27.基于时间的规则

```
sudo iptables -A FORWARD -p tcp -m multiport --dport http,https -o ens33
 -i ens33 -m time --timestart 21:30 --timestop 22:30
 --days Mon,Tue,Wed,Thu,Fri -j ACCEPT
```

28.SYN-FLOOD保护

```
sudo iptables -N syn_flood

sudo iptables -A INPUT -p tcp --syn -j syn_flood
sudo iptables -A syn_flood -m limit --limit 1/s --limit-burst 3 -j RETURN
sudo iptables -A syn_flood -j DROP

sudo iptables -A INPUT -p icmp -m limit --limit  1/s --limit-burst 1 -j ACCEPT

sudo iptables -A INPUT -p icmp -m limit --limit 1/s --limit-burst 1 -j LOG --log-prefix PING-DROP:
sudo iptables -A INPUT -p icmp -j DROP

sudo iptables -A OUTPUT -p icmp -j ACCEPT
```

29.阻塞来自私网地址的包（防范网络欺骗）

```
_subnets=("224.0.0.0/3" "169.254.0.0/16" "172.16.0.0/12" "192.0.2.0/24" "192.168.0.0/16" "10.0.0.0/8" "0.0.0.0/8'

for _sub in "${_subnets[@]}" ; do
  iptables -t mangle -A PREROUTING -s "$_sub" -j DROP
done
sudo iptables -t mangle -A PREROUTING -s 127.0.0.0/8 ! -i lo -j DROP
```

30.保存规则到文件。

```
sudo sh -c "iptables-save > /etc/iptables.rules"
```