**linux防火墙练习**

**iptables练习**

1. 删除已有规则

iptables -F

1. 删除INPUT第三条规则

iptables -D INPUT 3

1. 在INPUT的第四条位置插入新规则，丢弃来自192.168.100.100的数据

iptables -I INPUT 4 -s 192.168.100.100 -j DROP

1. 保存防火墙信息

Iptables-save > /etc/sysconfig/iptables

1. 拒绝192.168.3.1使用ping测试本主机

iptables -t filter -A INPUT -s 192.168.3.1 -p icmp -j DROP

1. 允许本地ping其他主机请求包，且允许其他主机的PING响应回包

iptables -A OUTPUT -p icmp --icmp-type 8 -j ACCEPT

iptables -A INPUT -p icmp --icmp-type 0 -j ACCEPT

1. 只允许192.168.3.0/24网段访问本机192.168.3.10的1394端口。

iptables -t filter -I INPUT -s 192.168.3.0/24 -d 192.168.3.10  -p tcp --dport 1394 -j ACCEPT

iptables -A INPUT ! -s 192.168.3.0/24 -p tcp --dport 1394 -j DROP

1. 设置进站，出站，转发默认规则为拒绝所有

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

1. 使用SNAT使得192.168.3.0/24网段的PC通过本地eth0访问internet

iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -o eth0 -j MASQUERADE

1. 将192.168.3.10的80端口发布到202.106.0.1的80端口上

iptables -t nat -A PREROUTING -d 202.106.0.20 -p tcp --dport 80 -j DNAT --to 192.168.3.10:80

1. 允许转发目标地址192.168.3.10目标端口号80的访问流

iptables   -A FORWARD -d 192.168.2.2 -p tcp --dport 80 -j ACCEPT

1. 允许已存连接的数据流转发通过

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

1. 允许访问本地的IP地址192.168.3.10的80端口

iptables -t filter -A INPUT  -d 192.168.3.10 -p tcp --dport 80 -j ACCEPT

1. 允许本地192.168.3.10的web服务响应其他连接

iptables -t filter -A OUTPUT  -s 192.168.3.10 -p tcp --sport 80 -j ACCEPT

1. 允许192.168.3.0/24网段访问本地的SSH服务，新连接与已存连接放行

iptables -A INPUT -s 192.168.3.0/24 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

1. 允许本地放行所有已存连接返回访问源

iptables -A OUTPUT -m state --state ESTABLISHED -j ACCEPT

1. 允许通过网卡eth0访问本机的80端口和443端口。放行请求连接和应答

iptables -A INPUT -i eth0 -p tcp -m multiport --dports 80,443 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 80,443 -m state --state ESTABLISHED -j ACCEPT

1. 允许本机从eth0出站DNS访问

iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT

iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT

1. 允许从eth0接收来自192.168.3.10的Mysql访问请求

iptables -A INPUT -i eth0 -p tcp -s 192.168.3.1 --dport 3306 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --sport 3306 -m state --state ESTABLISHED -j ACCEP

1. 当访问量本地80端口的访问量达到每分钟100时调整为每分钟放行25个访问量

iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT

**firewalld部分**

1. 查看本地网卡eno16777736位于什么区域

firewall-cmd --get-zone-of-interface=eno16777736

1. 查看本地防火墙的默认区域是哪个

firewall-cmd --get-default-zone

1. 查看防火墙配置内容

firewall-cmd --list-all

1. 将本地网卡eno16777736的默认区域变为internal

firewall-cmd --zone=internal --change-interface=eno16777736

1. 查看internal区域中有哪些接口

firewall-cmd --zone=internal --list-interfaces

1. 查看所有已激活区域

firewall-cmd --get-active-zones

1. 查看public区域中放行的服务

firewall-cmd --list-services --zone=public

1. 为internal区域中添加允许访问http服务

firewall-cmd --add-service=http --zone=internal

1. 从internal区域中删除允许的服务samba-client

firewall-cmd --zone=internal --remove-service=samba-client

1. 向区域internal中添加放行TCP8080端口

firewall-cmd --zone=internal --add-port=8080/tcp

1. 写入动态规则，永久生效

firewall-cmd --runtime-to-permanent

1. 设置本服务器默认区域为DMZ区域

firewall-cmd—set-default-zone=dmz

1. 设置在external区域开启伪装功能

firewall-cmd --zone=external --add-masquerade

1. 来自192.168.3.0网段的访问量替换为external区域接口IP地址访问公网（PAT/SNAT)

firewall-cmd --zone=external --add-rich-rule 'rule family=ipv4 source address=192.168.3.0/24 masquerade'

1. 公网访问external接口IP地址的80端口时，将访问流目标IP地址替换为192.168.10.100

firewall-cmd --zone=external --add-rich-rule='rule family=ipv4 destination address=202.106.0.1 forward-port port=80 protocol=tcp to-addr=192.168.10.100'