网络安全技术基础实验报告

年 月 日

实验名称： 实验3 防火墙配置与使用 班级： 软件工程2003

姓名： 徐彬涵 学号： 32001272 同组人：

指导教师评定：

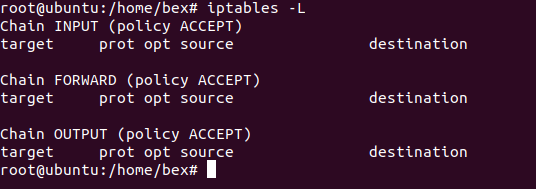
**一、实验目的和要求**

1. 了解防火墙的概念。
2. 使用iptables、firewall-cmd和firewall-config等实现防火墙策略配置。
3. 使用Cockpit监控系统的运行状态，确保Linux系统的安全性。

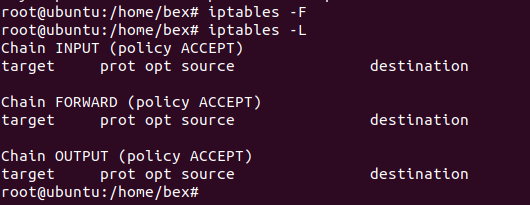
**二、实验内容**

Iptables设置：

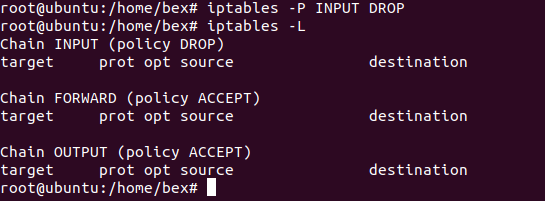
1. 在iptables命令后添加-L参数查看已有的防火墙规则链。



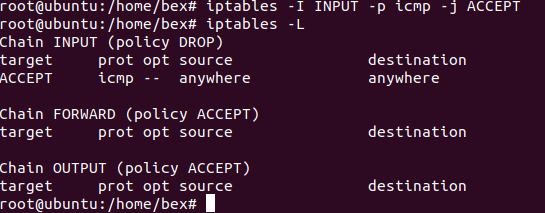
1. 在iptables命令后添加-F参数清空已有的防火墙规则链。



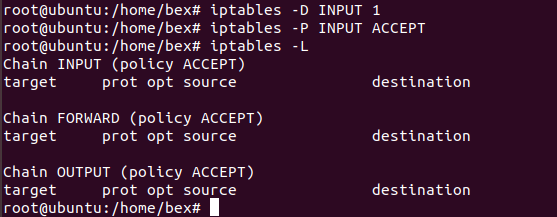
1. 把INPUT规则链的默认策略设置为拒绝。



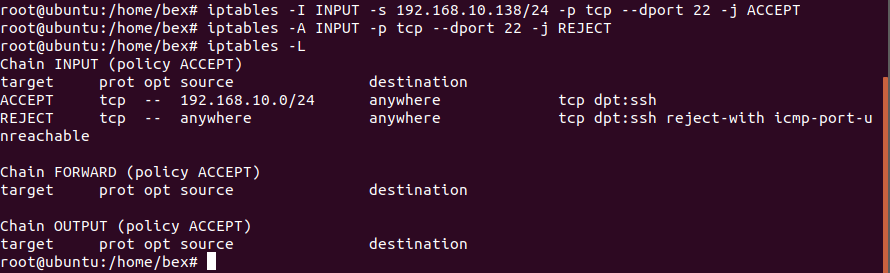
1. 向INPUT链中添加允许ICMP流量进入的策略规则。



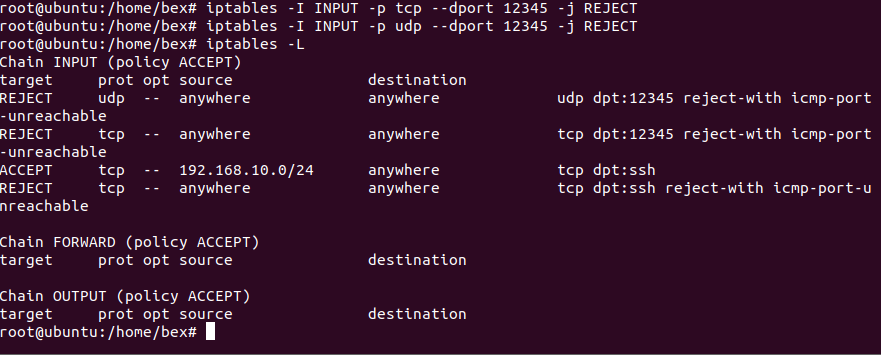
1. 删除INPUT规则链中刚刚加入的那条策略（允许ICMP流量），并把默认策略设置为允许。



1. 将INPUT规则链设置为只允许指定网段的主机访问本机的22端口，拒绝来自其他所有主机的流量。

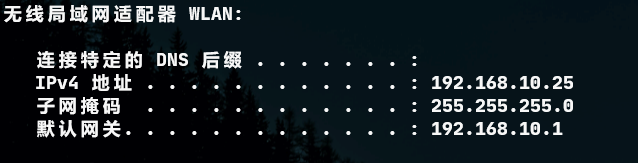


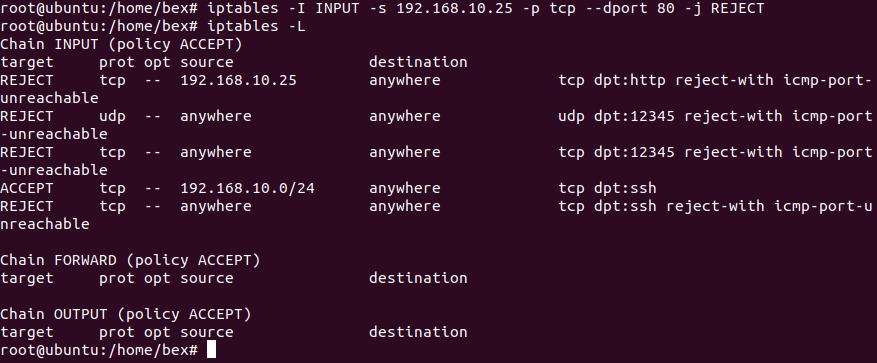
1. 向INPUT规则链中添加拒绝所有人访问本机12345端口的策略规则。



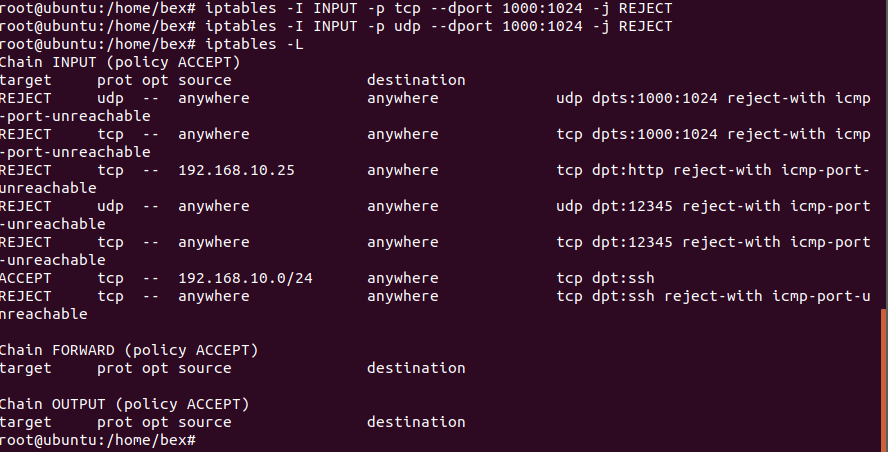
1. 向INPUT规则链中添加拒绝192.168.10.5（自行根据实验环境选择）主机访问本机80端口（Web服务）的策略规则。

使用宿主机ip





1. 向INPUT规则链中添加拒绝所有主机访问本机1000～1024端口的策略规则。

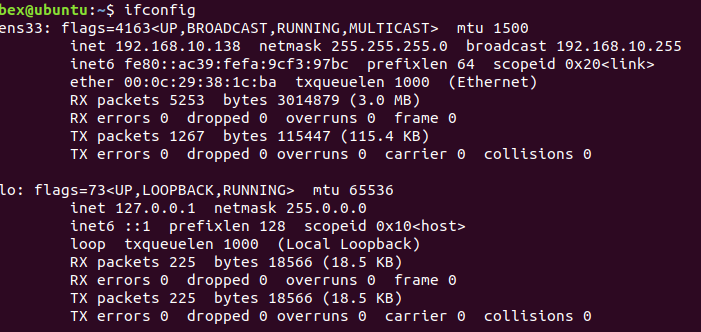


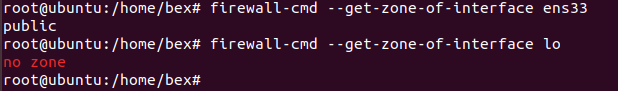
使用终端管理工具firewall-cmd：

1. 查看firewalld服务当前所使用的区域。

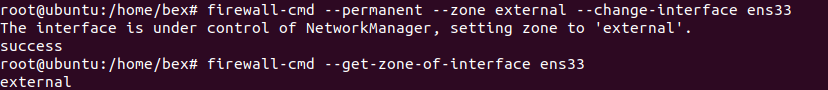


1. 查询指定网卡在firewalld服务中绑定的区域。

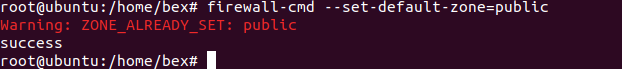




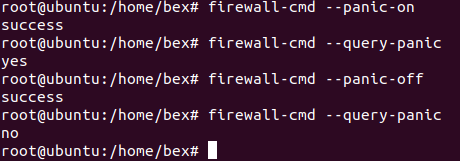
1. 把网卡默认区域修改为external，并在系统重启后生效。



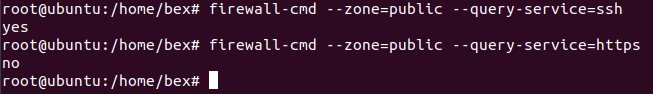
1. 把firewalld服务的默认区域设置为public。



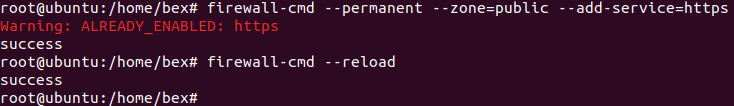
1. 启动和关闭firewalld防火墙服务的应急状况模式。



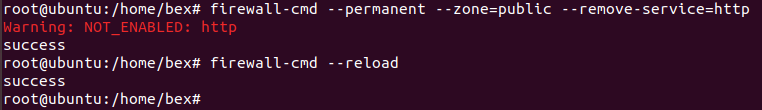
1. 查询SSH和HTTPS协议的流量是否允许放行。



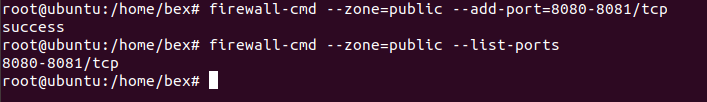
1. 把HTTPS协议的流量设置为永久允许放行，并立即生效。



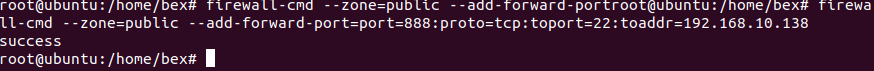
1. 把HTTP协议的流量设置为永久拒绝，并立即生效。



1. 把访问8080和8081端口的流量策略设置为允许，但仅限当前生效。



1. 把原本访问本机888端口的流量转发到22端口，要且求当前和长期均有效。



1. 富规则的设置。它的优先级在所有的防火墙策略中也是最高的。

