日志审计与分析

实验三-Linux日志收集

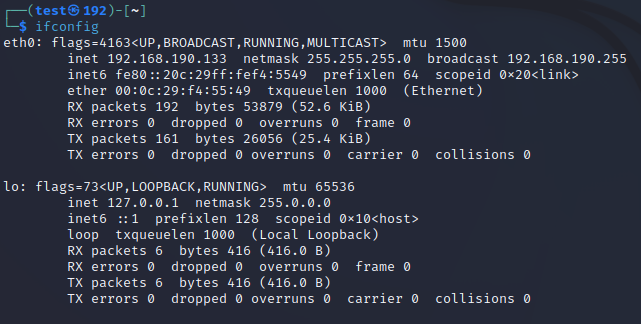
实验目的：1、掌握rsyslog配置方法

2、配置rsyslog服务收集其他Linux服务器日志

1. **配置rsyslog服务器**

**配置前提：所有Linux均默认安装rsyslog服务。**

**确定rsyslog服务器IP地址：**



**192.168.190.133**

**修改rsyslog服务器配置文件：**

**vim /etc/rsyslog.conf**

**将红色部分前的#号删除后，保存退出**

**# Provides UDP syslog reception**

**# for parameters see http://www.rsyslog.com/doc/imudp.html**

**module(load="imudp") # needs to be done just once**

**input(type="imudp" port="514")**

**# Provides TCP syslog reception**

**# for parameters see http://www.rsyslog.com/doc/imtcp.html**

**module(load="imtcp") # needs to be done just once**

**input(type="imtcp" port="514")**

电脑萤幕的截图

描述已自动生成

**重启rsyslog服务**

**systemctl restart rsyslog.service**

文本

描述已自动生成

1. **配置rsyslog客户端**

**配置前提：所有Linux均默认安装rsyslog服务。**

**修改rsyslog客户端配置文件：**

**vim /etc/rsyslog.conf**

**在文件最底部添加配置后，保存退出**

**\*.\*@服务器IP地址**

**\*.\*@@服务器IP地址**

文本

描述已自动生成

1. **验证rsyslog配置**

**查看服务器日志是否能收集到客户机日志，重点检查/var/log/secure文件，正常收集后，应该能看到客户机登录日志。**

电脑屏幕截图

描述已自动生成