

哈尔滨工业大学

信息安全概论课程实验报告

实验四

## 学院：计算机学院

## 班级：11403202

## 学号：1140320206

## 姓名：霍峻杰

1. 实验目的

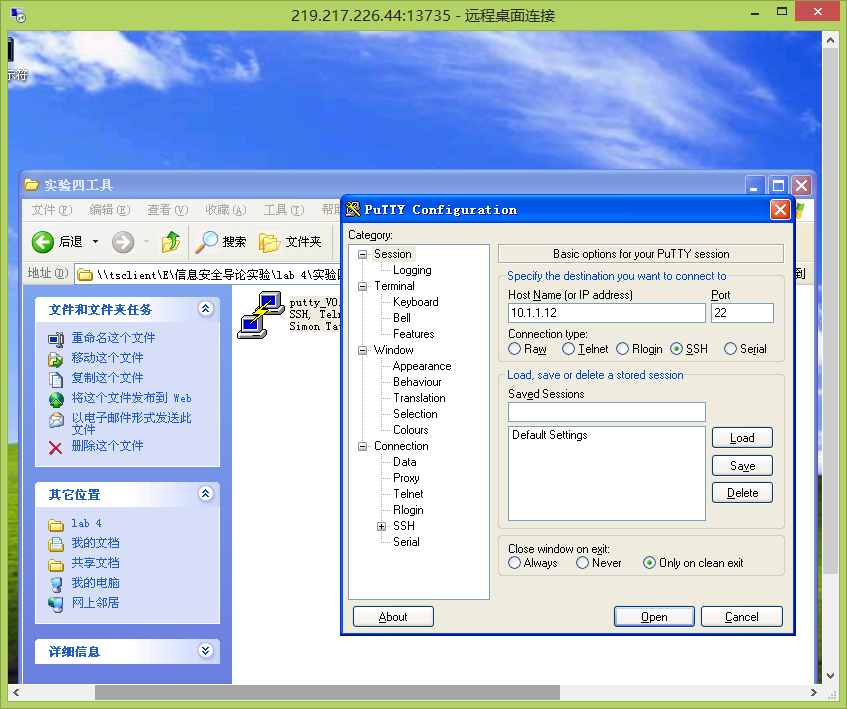
通过该实验可以:

1. 加深理解Snort的系统架构以及工作原理;
2. 掌握Snort与Iptables联动的实现方法。
3. 实验内容及实现

# 一、

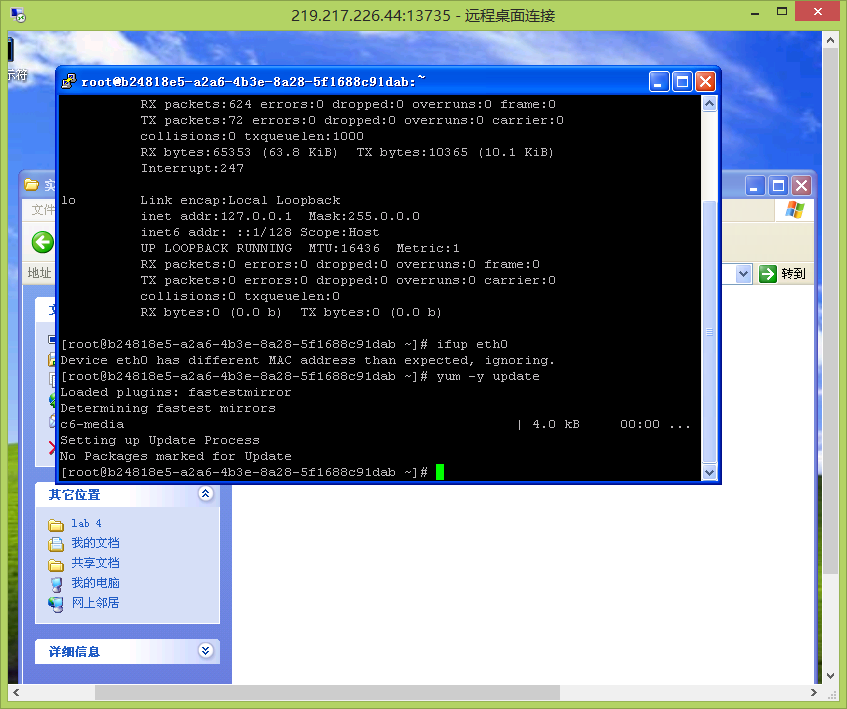
# Snort安装与配置

SSH登录centos6.5主机

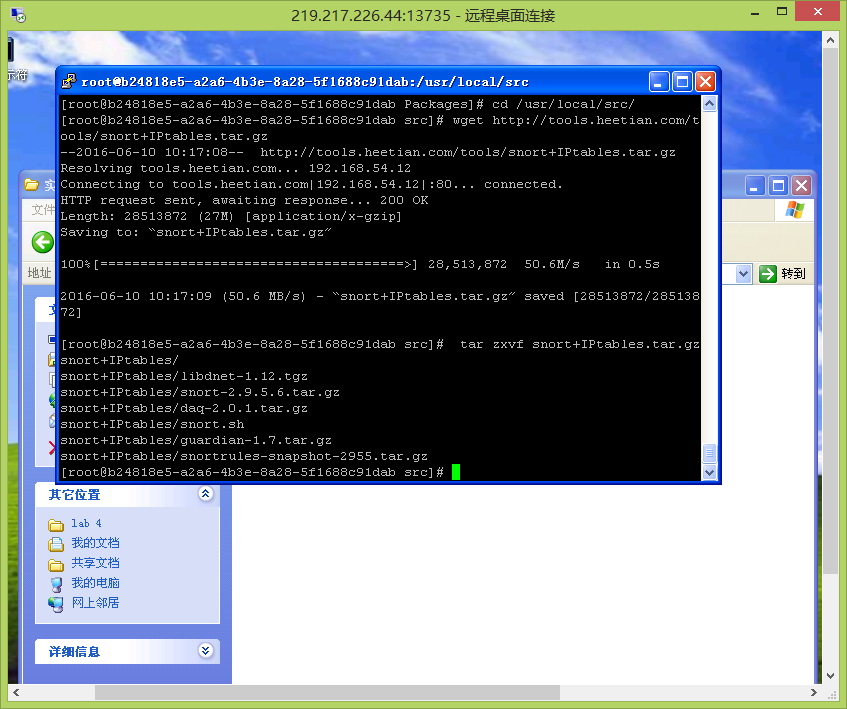
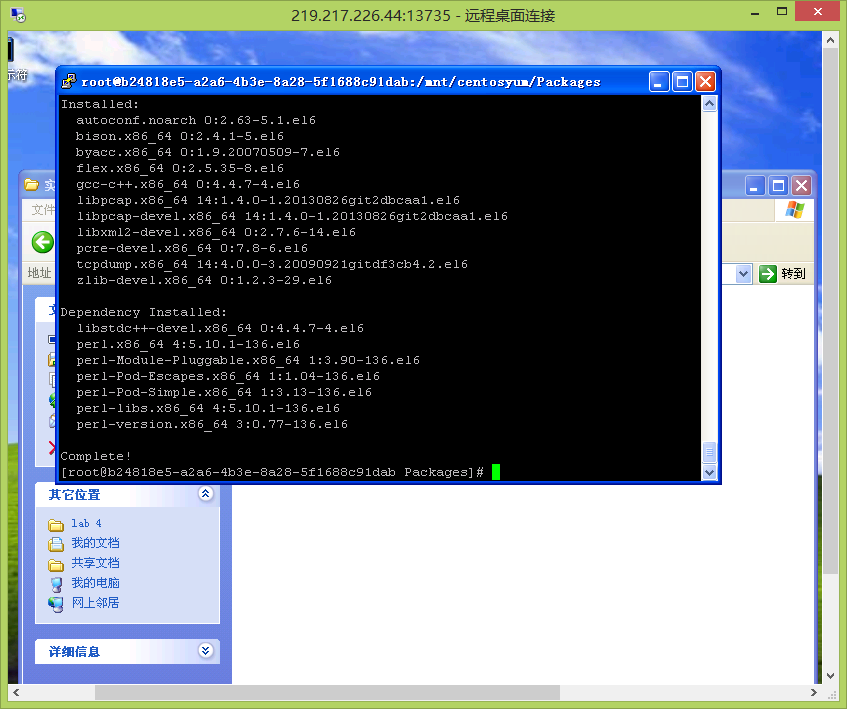


更新系统

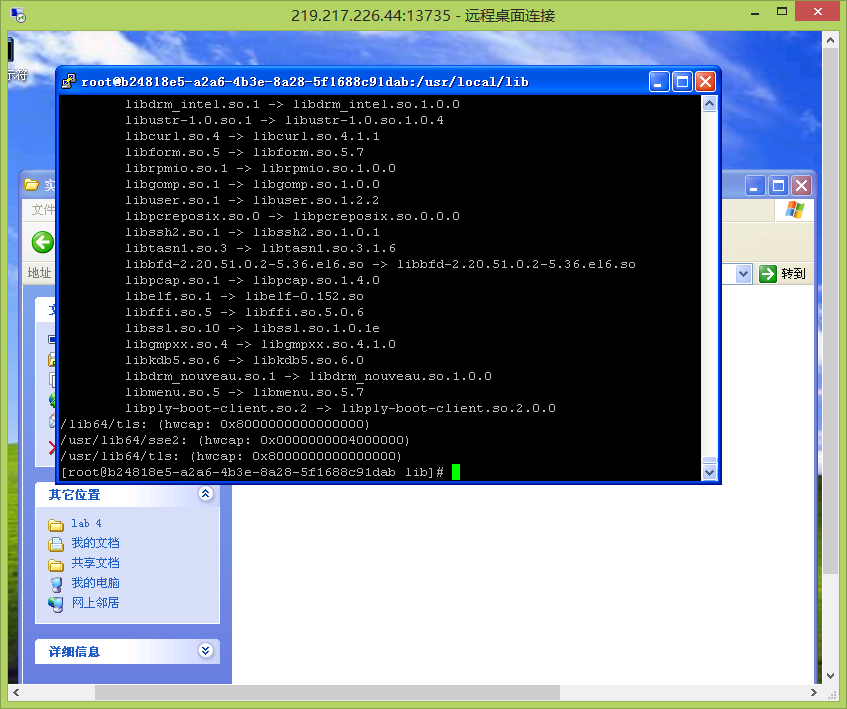
      yum –y update



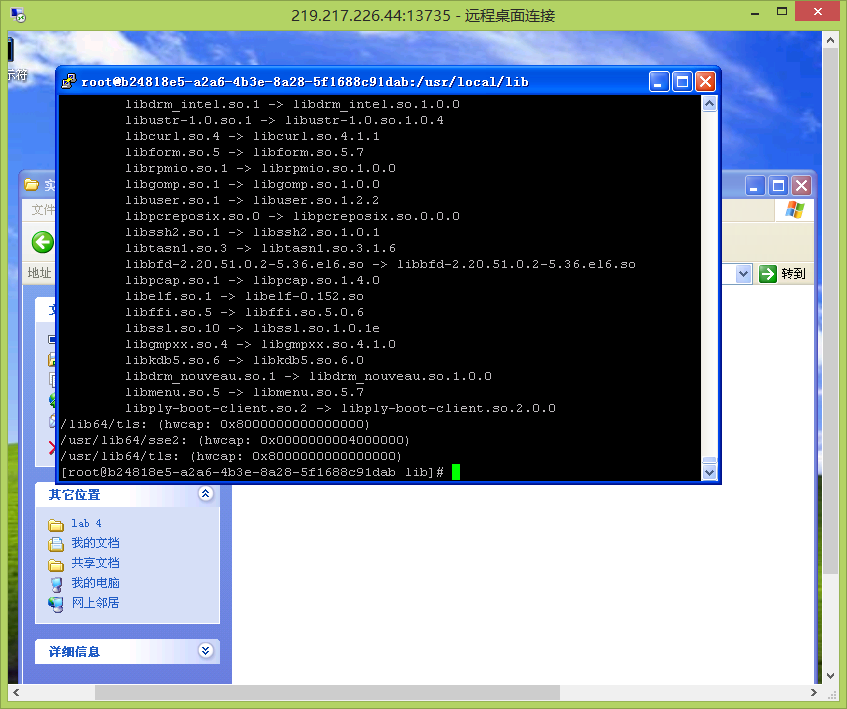
安装snort依赖包



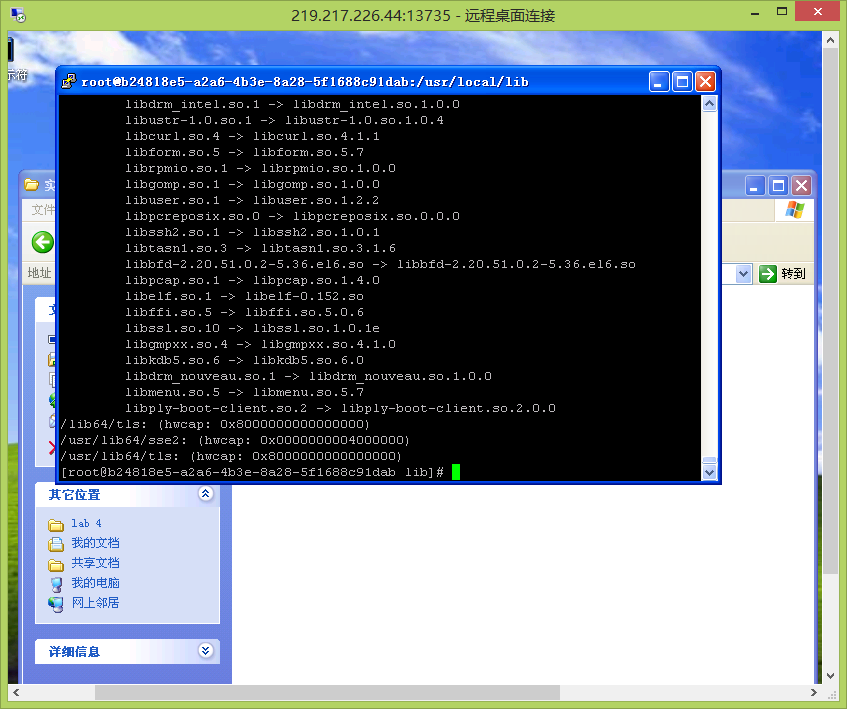
安装libdnet



安装DAQ

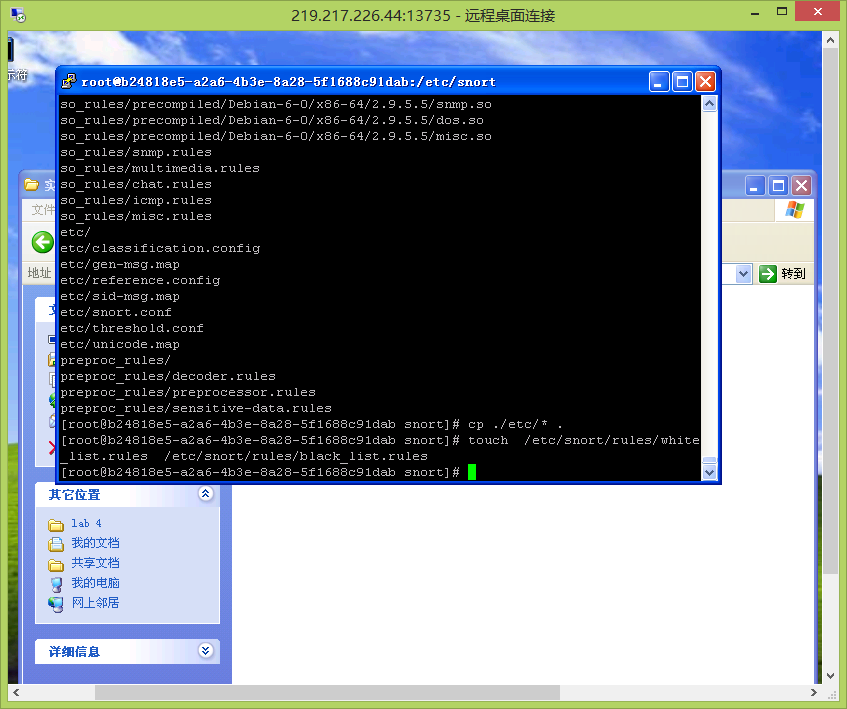


安装Snort

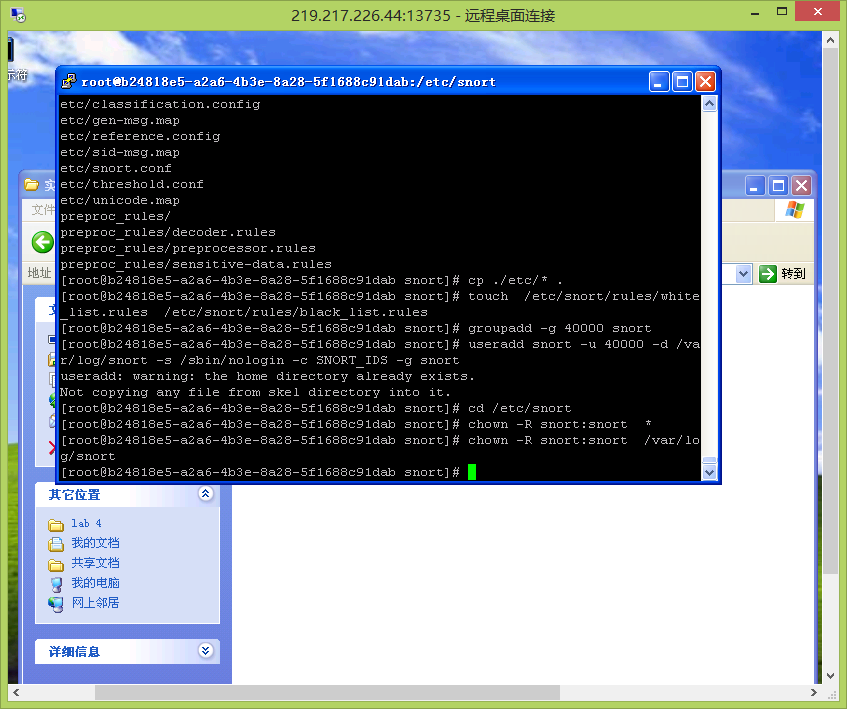


Snort配置

**创建snort系统必要的文件夹，导入规则库，建立黑名单和白名单文件**



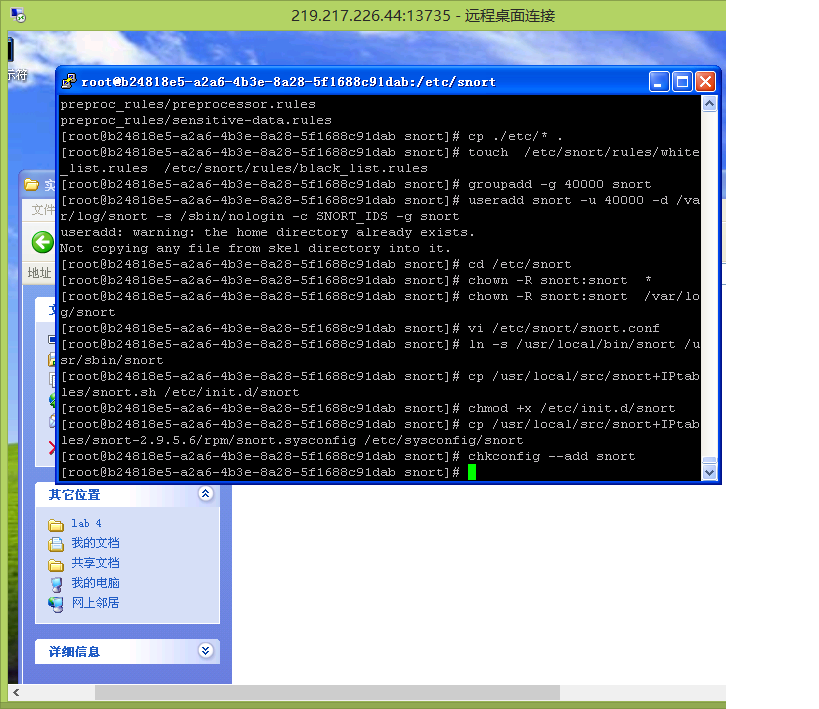
**为snort添加一个用户和组**



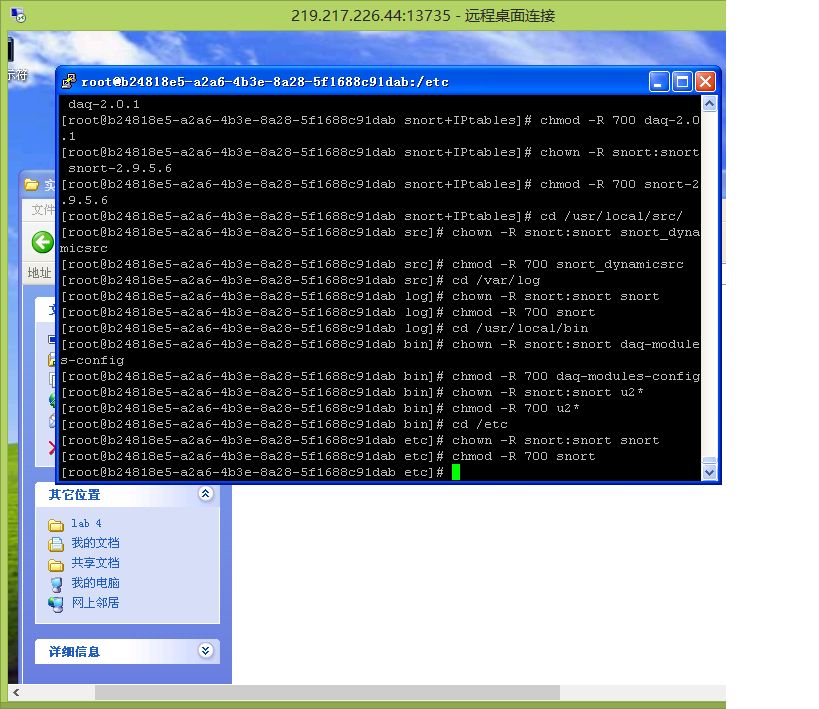
**修改snort配置文件**

**为snort的文件在另一个位置创建一个同步链接**

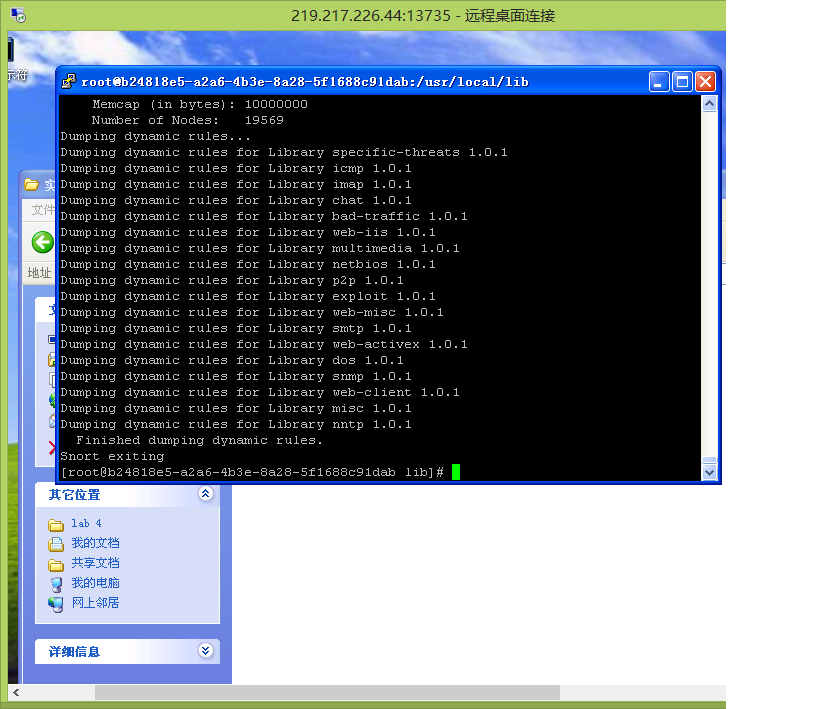
**配置snort启动文件**



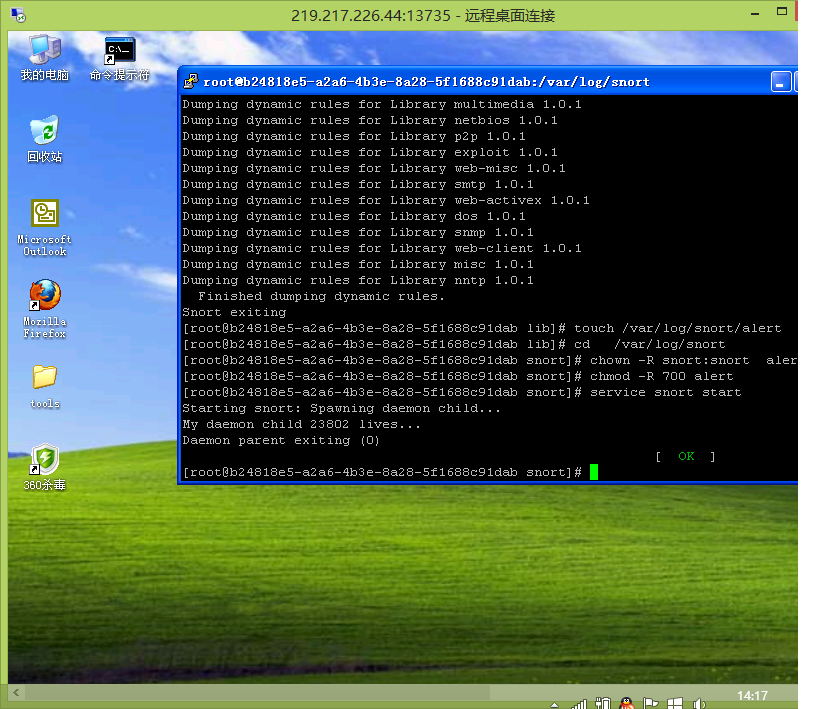
**修改snort及daq等相关目录和文件权限**



**配置动态规则**



导出动态规则文件



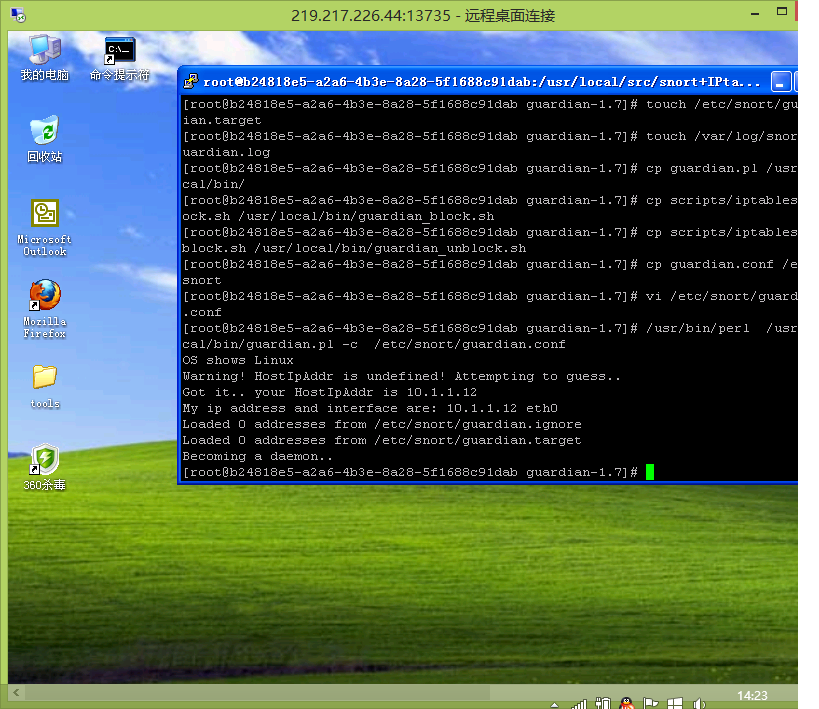
**二、**

**安装配置guardian**

**安装配置**

**编辑guardian配置文件**

**guardian启动**



**三、**

**联动测试**

      Snort与本地iptables联动

**启动snort，查看alert是否有日志**

      snort -c /etc/snort/snort.conf -i eth0

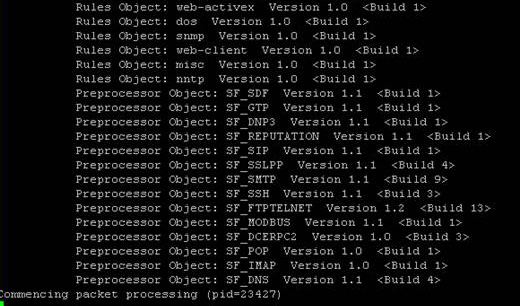
      cd /var/log/snort

      tail -f alert

      如果可以看到日志，则表明snort.conf配置没有问题，可以继续下面的测试，否则请检查snort.conf的配置，以及snort目录和文件权限设置。

**联动测试**

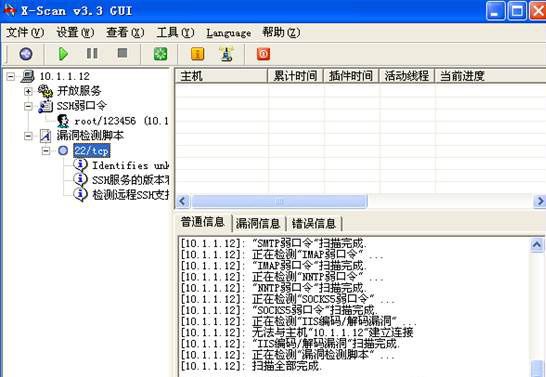
**启动Snort**



      登录另一台windows 测试主机

      设置扫描参数

       点击开始按钮，开始扫描

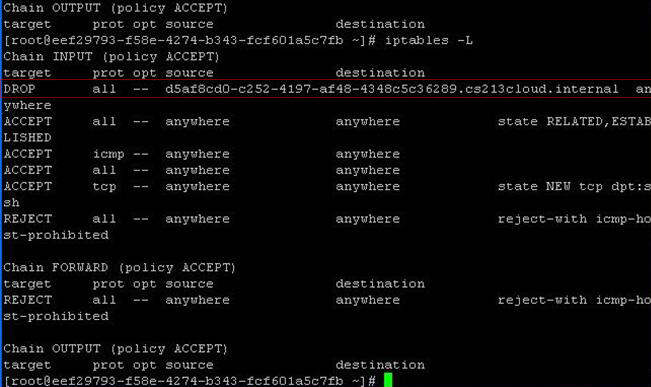


**观察alert是否有告警日志**

**发现告警日志，启动guardian与iptables联动**

**可以看到，执行了block脚本**

**在snort主机上执行，iptables -L即可看到新加入的规则。**



1. 实验总结

通过这次实验，我对IDS入侵检测及防火墙防御技术有个一个实践性的理解。首先，我熟悉了一些linux系统的shell操作命令，在环境中成功安装了IDS snort和主动防火墙guardian。并通过guardian扫描snort产生的入侵检测日志，将入侵信息传送给iptables，（snort和iptables的联动）从而达到入侵检测并进行防火墙隔离的目的。操作中遇到了许多小问题，比如进行到alert日志的时候会导致崩溃，需要重置完成，解决方法是将host主机的ip加入到白名单中（经大神指导）。

思考题：

1. snortsam与guardian相比，前者是属于snort的一个插件，snort可以直接将收集到的IDS检测数据传送给snortsam进行防火墙处理，这种处理相对于guardian的扫描snort日志，要节省很多的计算资源。而且作为内部插件，snortsam得到的是加密的包，相对日志扫描更加安全。但是，作为snort的插件，snortsam的可移植性很差，只能对snort进行防火墙检测防护，而guardian可以结合不同的IDS进行防护。
2. 这是一种“亡羊补牢”的方式，也就是一个ip已经入侵了，被检测到后，防火墙才将规则写入，防护系统，而在这期间，系统处于如被入侵状态。