中国人民公安大学

实验报告

课程名称 信息安全技术体系

实验项目 Snort的安装与使用

姓名、学号 xxx 2015214600xx

年 级 2015级

专 业 网络安全与执法

指导教师 吴昌明

成 绩

实验日期 2017年11月24号

**实验报告撰写说明**

1.实验报告由参加实验的学生按要求独自（或组）完成。

2.课程名称、实验项目要与实验教学大纲一致。

3.实验数据、曲线、图表和照片等要符合实验指导书的要求，分别插入实验报告的相应部分，内容比较多的也可以作为“附件”附在实验报告的后面。

1. **实验内容**

本实验选择目前最流行的Snort软件，对局域网计算环境进行入侵检测部署，并进行入侵检测规则配置。通过模拟攻击，验证入侵行为是否能被Snort软件成功拦截。

1. **实验目的和要求**

**实验目的：**入侵检测时PDR模型的核心，只有及时发现问题，才能及时反应和回复。通过实验掌握入侵检测工具的使用。

**实验要求：**下载Snort的说明书，了解Snort的功能和使用方法。下载Snort软件，安装并扫描局域网计算机，发现网络环境的脆弱性。

1. **实验设备（软、硬件）**

硬件：PC计算机。

软件：Windows操作系统或者Linux操作系统；

Snort软件。

1. **实验步骤**（记录每步的实验数据）

首先，下载并仔细阅读最新版本的Snort软件使用说明书；

其次，下载并安装Snort的最新版本软件；

然后，在仿真环境下，部署Snort软件；

最后，通过人为的攻击行为，验证Snort系统是否能及时发现入侵。

1. **试验数据记录与处理**

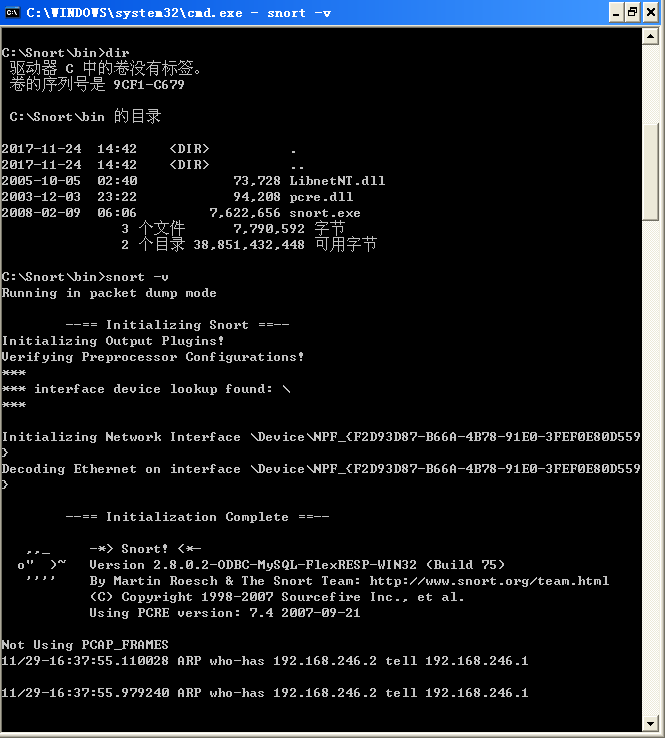
此项可以不填

1. **试验结果及分析**

Snort的配置很简单，在官网下载后安装就可以了。由于snort.org被墙，使用VPN过于慢，因此使用旧版snort2.8版本程序及配套规则集（Community版本）。

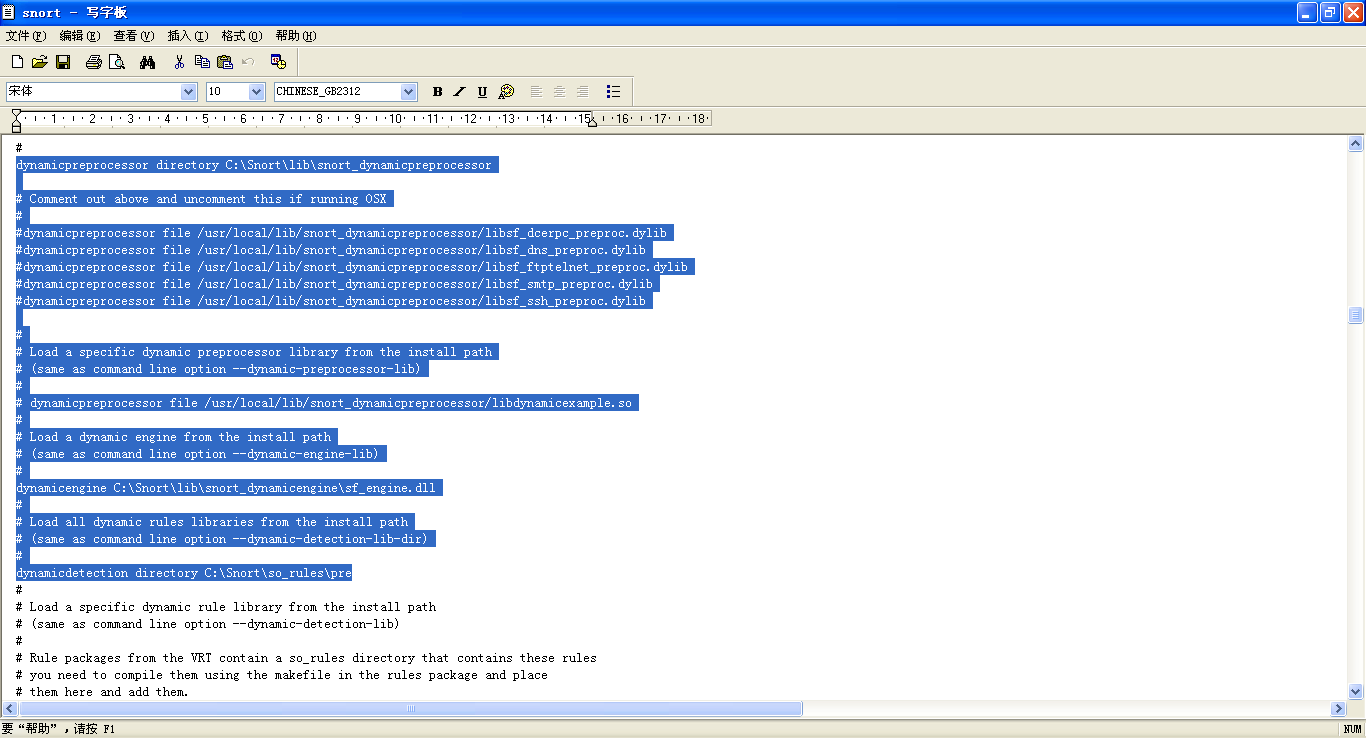
读过Snort说明书的人应该知道，Snort官方推荐在Linux/UNIX环境下使用，不建议在Windows下操作。Windows下的IDS解决方案是一个叫做WinIDS的集成环境，内有Mysql/Portgresql及ACID日志分析系统。但为了本次实验，我们强行使用标准Snort进行操作，并使用nmap扫描模拟攻击行为（真实攻击为metasploit攻击，然而规则库太过陈旧，未能识别，就不演示了）。

本次实验提供IDSCenter，早已不更新的程序，我们不演示了。直接使用Snort命令行进行操作。Snort的安装很简单，跟着安装向导走就可以了。然后需要安装WinPcap。安装结束后测试一下。

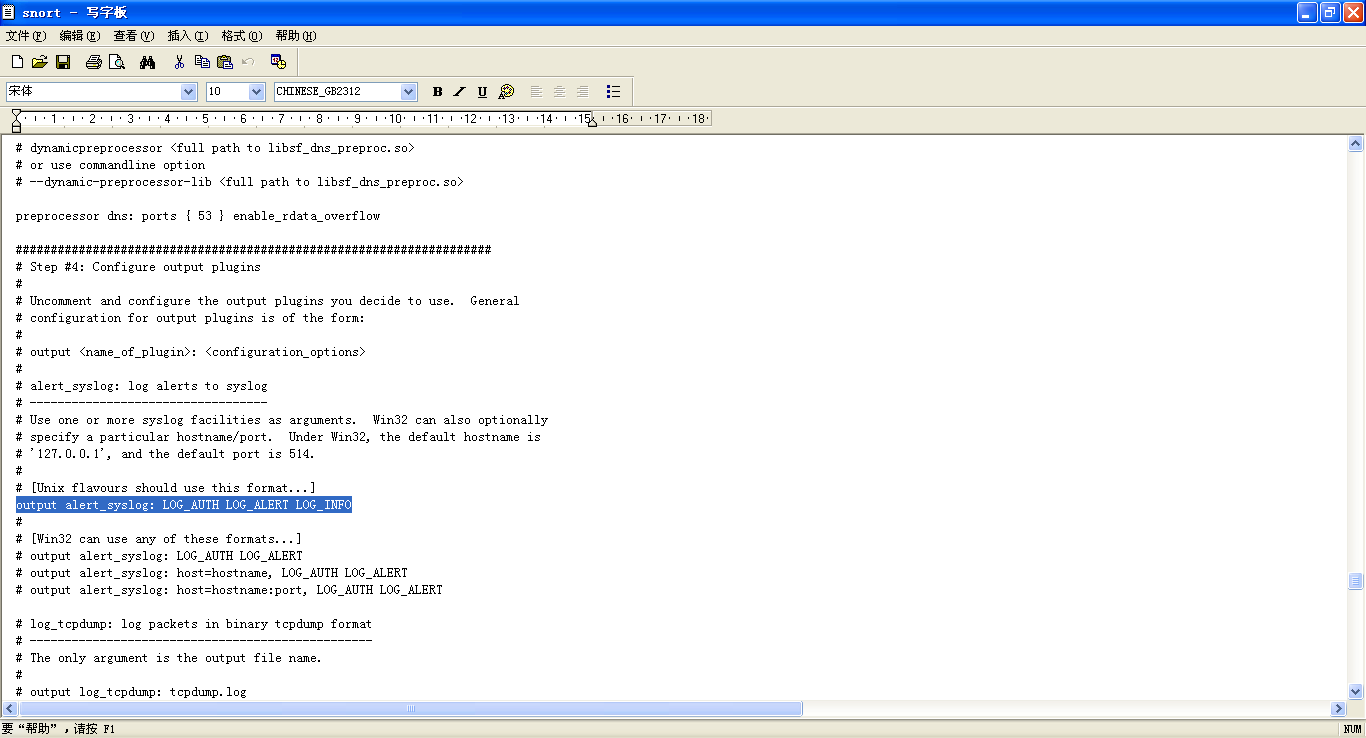


Snort -v默认是Sniffer模式，因此输出经过默认网卡的数据包信息。

然后配置snort配置文件及规则。将snortrules-snapshot解压后，完整覆盖snort安装目录，对etc\snort.conf进行修改。



将Linux风格目录改成Windows式的。

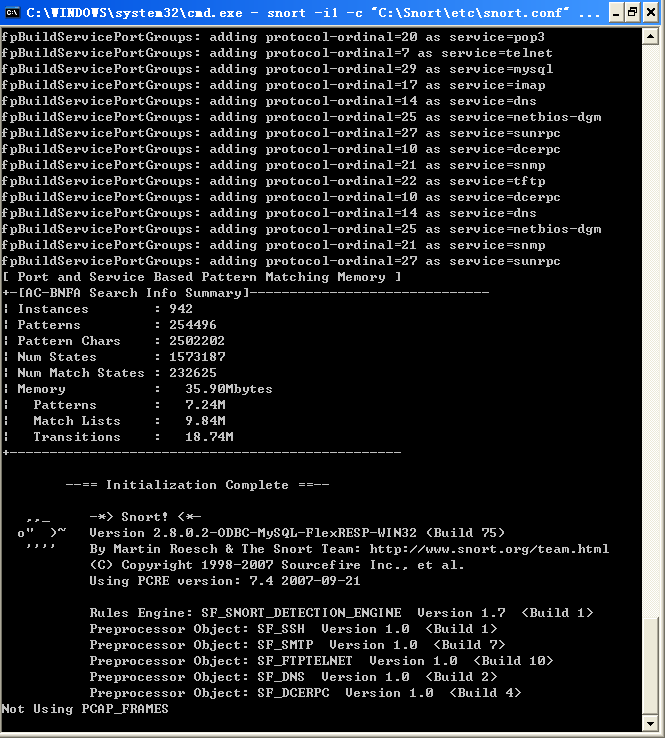


启用Syslog日志输出

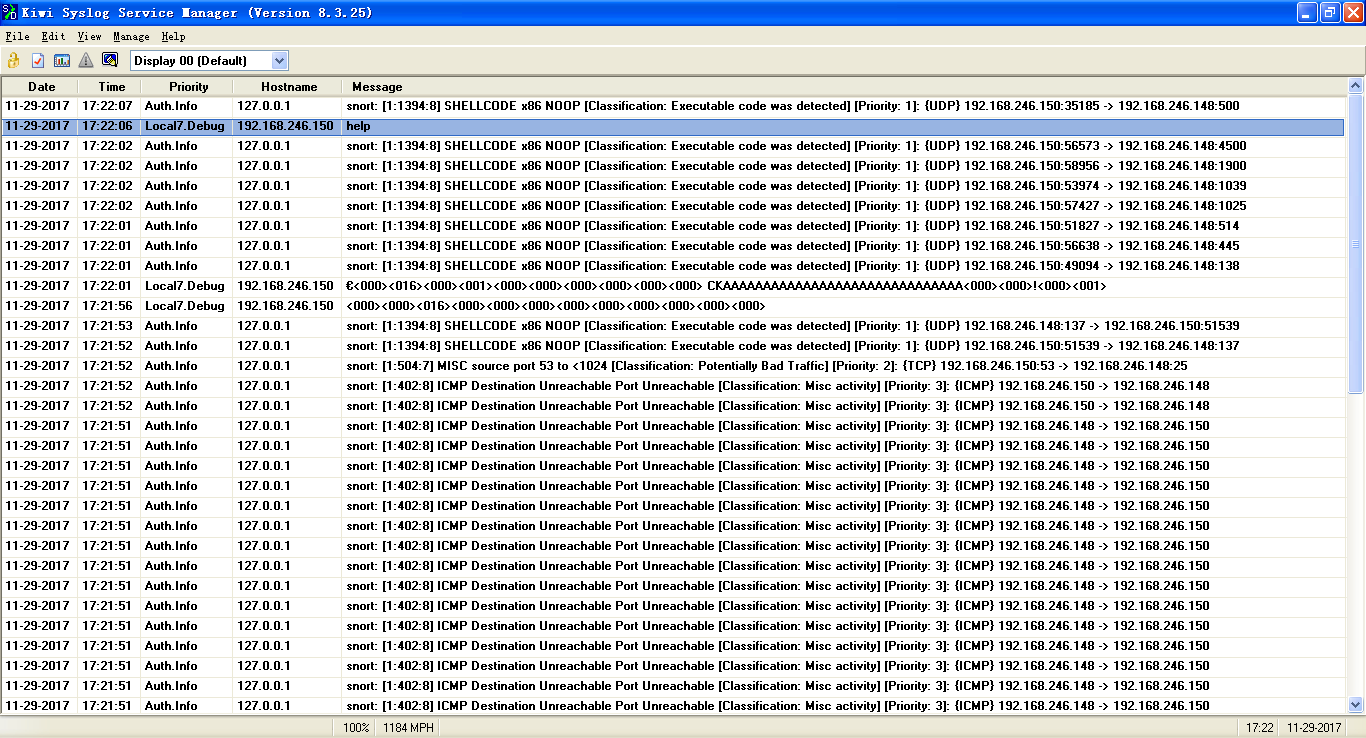
然后安装Kiwi Syslog Daemon,接受日志。

使用nmap进行扫描。首先开启snort:snort -c “C:\Snort\etc\snort.conf” -l “C:\Snort\log\alert.ids” -i1 -s

“



出现一只猪的时候意味着成功开启Snort IDS模式。Nmap命令行为：”nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 192.168.246.148”



没有加-v，snort控制台看不到信息，但是我们已经将警报输出到syslog中了。

1. **实验总结**
2. Snort是一个入侵检测系统，有三种工作模式：Sniffer,Packet Logger,Network Intrusion Detector.通过配置文件获得其规则。
3. 监听NPcap列表第一块网卡流量，以“C:\Snort\etc\snort.conf”做配置文件，记录保存在“C:\Snort\log”目录下，将192.168.1.3主机作为家用主机，忽略其流量。
4. 任何对对192.168.1.0/24网段主机的111TCP端口访问，数据包内容为“00 01 86 a5”发出警告信息：“mountd access”

**八、 参考资料**

Snort使用说明书

谢希仁. 《计算机网络》（第五版）.电子工业出版社，2010