**江苏科技大学**

**课程实验报告**

课 程： 计算机网络与安全

课 题： 入侵检测系统IDS的配置与应用

学 院： 计算机学院

姓 名： 陈四贵

班 级： 1822107101

学 号： 182210710119

指导老师： 张笑非

目 录

[一、 实验目的 1](#_Toc59048247)

[二、 实验条件 1](#_Toc59048248)

[三、 实验原理 1](#_Toc59048249)

[四、 实验步骤 4](#_Toc59048250)

[五、 实验结果分析 7](#_Toc59048251)

[六、 思考题 7](#_Toc59048252)

# 实验目的

1.掌握基于Snort的规则编写方法；

2.掌握Snort中IDS的配置方法。

# 实验条件

1.Snort运行环境；

2.网络测试环境。

# 实验原理

参考： https://cs.gmu.edu/~dfleck/classes/csSecurityLab/SnortInstallTest/IntrusionDetection.pdf

Rule Header (rule options)

alert tcp $EXTERNAL\_NET any -> $HOME\_NET any

(msg:"SCAN SYN FIN";flags:SF;reference:arachnids,198;\classtype:attempted-recon;sid624;rev:1;)

Defines "who" the rule applies to (coarsly).

Rule Header

alert tcp $EXTERNAL\_NET any -> $HOME\_NET any

alert(action) tcp(protocol) $EXTERNAL\_NET(Src IP) any(Src Port) ->(Direction) $HOME\_NET(Dst IP) any(Dst Port)

Rule Header Action

表7-1 Snort规则动作

|  |  |  |
| --- | --- | --- |
| **序号** | **动作** | **说明** |
| 1 | alert | 触发警报并记录数据包 |
| 2 | log | 在触发时仅记录数据包。 |
| 3 | pass | 忽略或丢弃数据包或流量匹配 |
| 4 | activate | 告警后激活一个或多个动态规则 |
| 5 | dynamic | 忽略，直到由激活规则开始，这时才充当日志规则。 |
| 6 | drop | 阻止并记录数据包 |
| 7 | reject | 阻止数据包，将其记录下来，如果协议为TCP，则发送TCP重置；如果协议为UDP，则发送ICMP端口不可达消息。 |
| 8 | sdrop | 阻止数据包但不记录 |

Rule Header Protocol

目前支持TCP、UDP、ICMP、及IP，今后会增加ARP、IGRP、GRE、OSPF、RIP、IPX等。

Rule Header IP

alert tcp $EXTERNAL\_NET any -> $HOME\_NET any

alert tcp 192.168.1.0/24 any -> 192.168.1.0/24 1:1024

alert tcp ![192.168.1.0/24,10.1.1.0/24] any -> 192.168.1.44

注意：

$EXTERNAL\_NET是snort.conf中的一个配置值集(config value set)；

IP可以通过点分十进制和CIDR掩码来表示，"any"也是可以的；

!是取反操作符；

多个IP地址范围可以通过中括弧和逗号分开，中间不要加入空格。

Rule Header Port

端口可以通过表7-2中的几种方式来指定。

表7-2 端口表达方式

|  |  |
| --- | --- |
| 表达方式 | 含义 |
| any | 所有端口 |
| 1:1024 | 端口1到1024，inclusive |
| 55: | 等于或大于55的端口 |
| :55 | 端口0到55， inclusive |
| !6000:6001 | 除了6000和6001以外的所有端口 |

Snort Header Direction

表7-3 方向的表达方法

|  |  |
| --- | --- |
| 表达方式 | 含义 |
| -> | 从源套接字向目标套接字 |
| <> | 任意方向 |
| <- | 不允许这样的表达方法 |

Snort Rule Options

(msg:"SCAN SYN FIN";flags:SF;reference:arachnids,198;\classtype:attempted-recon;sid:624;rev:1;)

表7-4 选项设置

表7-4 选项设置

|  |  |  |
| --- | --- | --- |
| 选项名称 | 选项值 | 含义 |
| msg | <sample message> | 将消息记录到/var/snort/log |
| flags | <AFPRSU210> | 匹配特定的TCP标志 |
| content | <text> | 匹配数据包中的指定文本 |
| content | |<hexadecimal>| | 匹配指定的十六进制字符 |
| sid | <snort ID> | 唯一编号，可轻松识别规则。用户的规则应该使用SID> 1,000,000 |
| rev | <revision #> | 规则修订号 |
| reference | <ref> | 从哪里获得有关规则的更多信息 |
| gid | <generator ID> | 标识Snort的哪个部分生成了警报，通过查看/etc/snort/gen-msg.map获得值 |

1. 简单Snort Rule示例

alert tcp any any -> any 21 (flow:to\_server,established;\content:"root";pcre:"/user\s+root/i";)

该命令的作用是"查找root用户登录尝试FTP服务器（端口21）"

2. 检测恶意工具的Snort Rule示例

alert tcp $EXTERNAL\_NET any -> $HOME\_NET $HTTP\_PORTS (msg:"MALWARE-TOOLS HOIC http denial of service attack"; flow:to\_server,established; content:"User-Agent|3A 20 20|Mozilla"; fast\_pattern:only;http\_header; content:"Referer|3A 20 20|http";http\_header;content:!"Connection: keep-alive"; nocase;detection\_filter:track by\_src, count 17, seconds 10;metadata:policy balanced-ips drop, policy security-ips drop, service http;reference:url,blog.spiderlabs.com/2012/01/hoic-ddosanalysis-and-detection.html; classtype:denial-ofservice;sid:21513; rev:6;)

3. 黑名单规则示例

alert udp $HOME\_NET any -> any 53 (msg:"BLACKLIST DNS request for known malware domain guest-access.net - Gauss "; flow:to\_server; byte\_test:1,!&,0xF8,2; content:"|0C|guest-access|03|net|00|"; fast\_pattern:only; metadata:impact\_flag red, policy balanced-ips drop, policy security-ips drop, service dns; reference:url,gauss.crysys.hu/; reference:url,www.securelist.com/en/blog/208193767/Gauss\_Nation\_state\_cyber\_surveillance\_meets\_banking\_Trojan; classtype:trojan-activity; sid:23799; rev:2;)

4 Windows操作系统中的规则示例

alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"OS-WINDOWS Microsoft Windows Object Packager ClickOnce object remote code execution attempt"; flow:to\_client,established; flowbits:isset,file.ppsx&file.zip; file\_data; content:"uuid:48fd9e68-0958-11dc-9770-9797abb443b9"; fast\_pattern:only; content:"2007-05-23T15:06:10-03:00"; metadata:policy balanced-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3; reference:cve,2012-0013; reference:url,technet.microsoft.com/enus/security/bulletin/ms12-005; classtype:attempteduser; sid:26068; rev:3;)

# 实验步骤

**步骤一、获取并安装必要的工具**

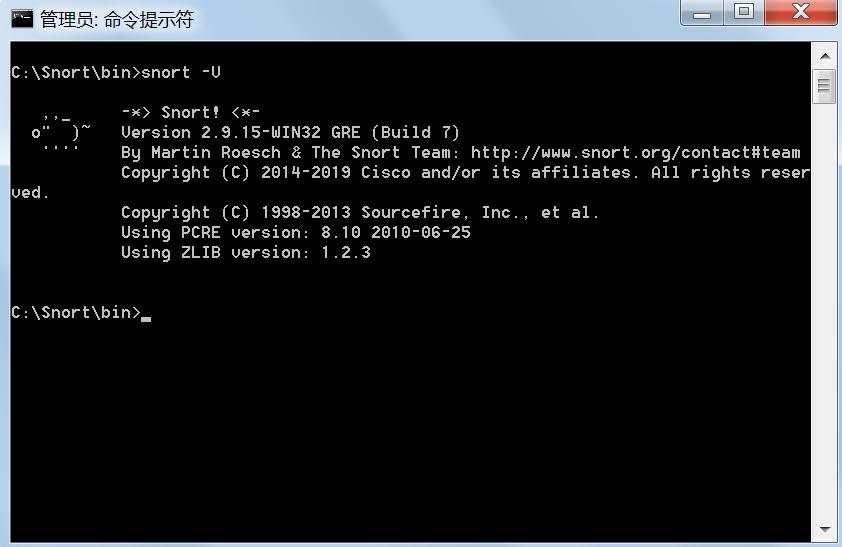
该步骤需要安装三个软件，分别是抓包工具WinPcap、Snort安装程序、以及一组Snort规则（下载规则前必须登录snort网站，否则无法下载指定的rules）。如果需要输出Syslog，则还要安装一个独立的Syslog服务器。因此，在Windows上需要的工具如下表所示：

|  |  |  |
| --- | --- | --- |
| **工具名称** | **工具文件** | **下载链接** |
| Snort | Snort\_2\_9\_12\_Installer.exe | <https://www.snort.org/downloads> |
| WinPcap | WinPcap\_4\_1\_3.exe | http://www.winpcap.org/install/default.htm |
| Snort规则集 | snortrules-snapshot-29120.tar.gz | https://www.snort.org/downloads/#rule-downloads |
| Syslog服务器(可选) | SyslogServer-1.2.3-win32.exe |  |

接着需要安装WinPcap和Snort和提取规则文件，***我们建议在安装Snort前先装好WinPcap***，但这也不是必须的。在Snort安装过程的最后也会提示用户安装WinPcap。如果用户之前装过类似Wireshark这样的抓包软件，那么WinPcap也已经装好了。

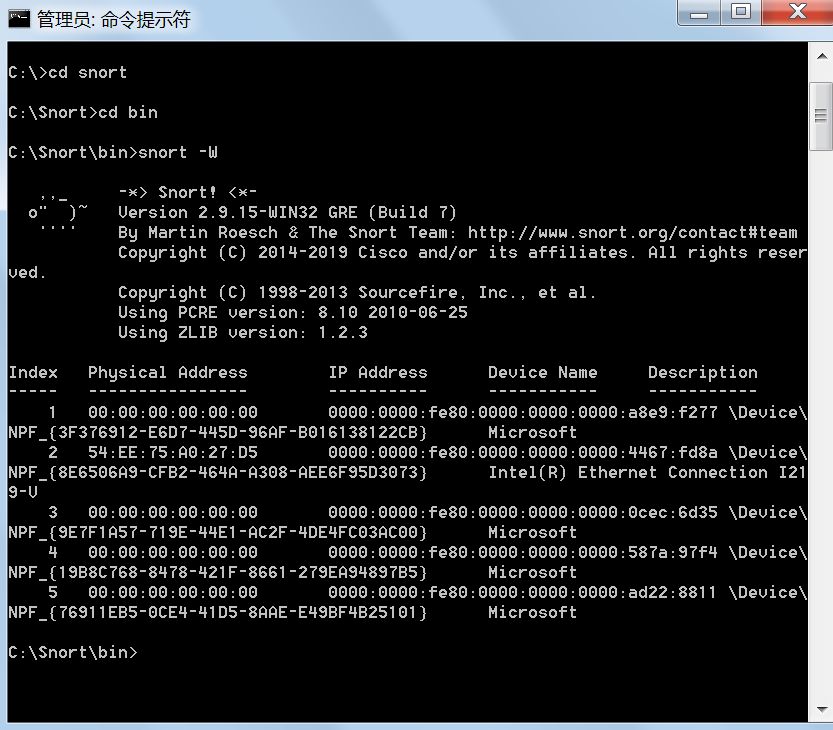
Snort安装的缺省路径是'c:\snort'。之后在安装规则文件时，在'c:\snort'下分别创建两个子目录，分别为'c:\snort\rules'，和'c:\snort\preproc\_rules'。将下载得到的规则压缩包中rules和preproc\_rules文件下的规则文件分别拷贝到两个目录中去。规则压缩包中的'so\_rules'和'etc'文件夹可以忽略。

完成安装后，可以切换到snort的目录'c:\snort\bin'，运行'snort -V'查看当前的版本，如下图所示：



注意：一定要以管理员权限运行CLI。

运行'snort -W'确认系统中有哪些网络适配器可以使用。



具体细节参考<https://www.securityarchitecture.com/learning/intrusion-detection-systems-learning-with-snort/getting-and-installing-tools/>

**步骤二、Snort配置**

为了来能够让Snort正确运行，我们需要修改缺省的配置文件，以匹配用户的本地环境和运行偏好，该文件的位置在路径'c:\snort\etc'中。该配置文件可以通过记事本进行编辑，它一般包括了9个部分：

具体细节参考https://www.securityarchitecture.com/learning/intrusion-detection-systems-learning-with-snort/configuring-snort/

**步骤三、生成告警**

用记事本编辑'c:\snort\rules\local.rules'，创建下列3条规则。

alert icmp any any -> any any (msg:"ICMP Testing Rule"; sid:1000001; rev:1;)

alert tcp any any -> any 80 (msg:"TCP Testingn Rule"; sid:1000002; rev:1;)

alert udp any any -> any any (msg:"UDP Testing Rule"; sid:1000003; rev:1;)

此外可以添加更多的测试规则。下面开始进行测试：

以管理员的权限运行CLI，进入到'c:\snort\bin'路径下，执行下面的命令,注意-i后的值根据实际的网卡进行设置：

c:\snort\bin\snort -i 2 -c c:\snort\etc\snort.conf -A console

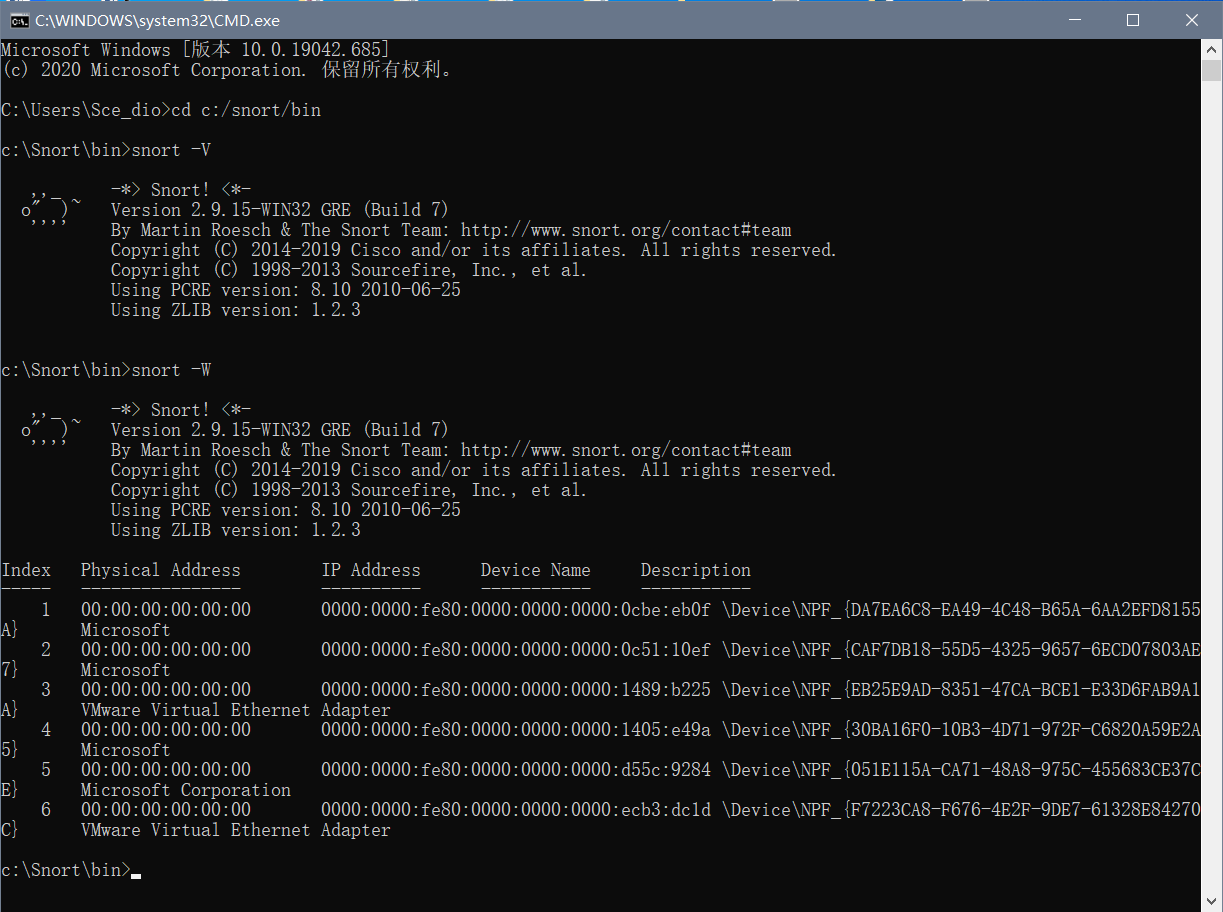
打开另一个CLI，ping自己的主机；打开浏览器浏览自己任意的主页。记录之前的CLI的输出。

具体细节参考https://www.securityarchitecture.com/learning/intrusion-detection-systems-learning-with-snort/generating-alerts/

**步骤四、安装Syslog服务器**

参考 <https://www.securityarchitecture.com/learning/intrusion-detection-systems-learning-with-snort/installing-syslog/>

# 实验结果分析



# 思考题

1.如何在URI长度超过250个字节时进行告警？

答：从服务器端下手，限制header头长度。