# Snort安装

使用系统CentOS Linux release 7.0.1406 (Core)

安装依赖的软件包

rpm -qa | grep 软件包名(例如dhcp) <== 列出所有被安装的rpm package

1. **flex (**2.5.35) 未安装

下载了flex-2.5.37-3.el7.x86\_64.rpm

flex-2.5.37-3.el7.x86\_64.rpm依赖m4

下载了m4-1.4.16-10.el7.x86\_64.rpm

1. **bison** (2.4.1)未安装

bison-2.7-4.el7.x86\_64.rpm

1. **libdnet** (1.11 or 1.12 including **libdnet-devel**)

libdnet-1.12-13.1.el7.x86\_64.rpm

libdnet-devel-1.12-13.1.el7.x86\_64.rpm

1. **zlib** (1.2.7 including **zlib-devel**)

**zlib-devel**未安装

zlib-devel-1.2.7-13.el7.x86\_64.rpm 对应于zlib-1.2.7-13.el7.x86\_64

1. **libpcap** (1.5.3 including **libpcap-devel**)

升级了libpcap libpcap-1.5.3-8.el7.x86\_64.rpm

安装 libpcap-devel-1.5.3-8.el7.x86\_64.rpm

1. **pcre** (8.32 including **pcre-devel**)

升级了pcre pcre-8.32-15.el7.x86\_64.rpm

安装了 pcre-devel-8.32-15.el7.x86\_64.rpm

Snort解压的路径 /usr/local/src/snort-2.9.8.2 之后configure 和 make （带有参数，具体参看文档）

DAQ解压的路径 /usr/local/src/daq-2.0.6

/usr/local/src/snort-2.9.8.2/etc 路径下内容cp至 /etc/snort/

snortrules-snapshot的文件（规则文件）解压到/etc/snort/路径下

/etc/snort/etc内文件cp至/etc/snort/

**由于bridge网卡配置的是dhcp，所以在snort.conf里需要经常更换保护的主机IP地址**

Locate and modify the following variables in your snort.conf file

(in directory /etc/snort) as follows (usually between lines 40 and 120):

This assumes the network you are going to monitor is 192.168.1.0/24

var RULE\_PATH /etc/snort/rules

ipvar HOME\_NET 192.168.1.0/24

ipvar EXTERNAL\_NET !$HOME\_NET

var SO\_RULE\_PATH /etc/snort/so\_rules

var PREPROC\_RULE\_PATH /etc/snort/preproc\_rules

var WHITE\_LIST\_PATH /etc/snort/rules

var BLACK\_LIST\_PATH /etc/snort/rules

暂时用的是 10.108.113.153/22 22代表子网掩码255.255.252.0



这步骤暂时没做

The file below should be named 'snort' and placed into the /etc/sysconfig directory on

your CentOS 6.x/7.x system:

----- CUT HERE -----

# /etc/sysconfig/snort

# $Id: snort.sysconfig,v 1.8 2003/09/19 05:18:12 dwittenb Exp $

#### General Configuration

INTERFACE=eth0

CONF=/etc/snort/snort.conf

USER=snort

GROUP=snort

PASS\_FIRST=0

#### Logging & Alerting

LOGDIR=/var/log/snort

ALERTMODE=fast

DUMP\_APP=1

BINARY\_LOG=1

NO\_PACKET\_LOG=0

PRINT\_INTERFACE=0

----- CUT HERE -----

之后执行了

chown -R snort:snort snort

chown -R 700 snort

所有配置完成后试运行，报错

ERROR: snort.conf(253) Could not stat dynamic module path "/usr/local/lib/snort\_dynamicrules": No such file or directory. Fatal Error, Quitting.

在常见错误里，第一条即有解决方式

Solution below:  
mkdir -p /usr/local/lib/snort\_dynamicrules <enter>  
chown -R snort:snort /usr/local/lib/snort\_dynamicrules <enter>  
chmod -R 700 /usr/local/lib/snort\_dynamicrules <enter> Copy any dynamic rulesets you have or are using to the above directory. Another method would be to comment out that line in snort.conf if you have no dynamic rules in use

# Snort学习

snort有三种工作模式：嗅探器、数据包记录器、网络入侵检测系统。

嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上。

数据包记录器 模式把数据包记录到硬盘上。

网路入侵检测模式是最复杂的，而且是可配置的。

## Snort Overview

### 嗅探器

snort -v

只把IP TCP/UDP/ICMP包头信息打印在屏幕上。

snort -vd

显示传输的应用数据信息

snort -vde

显示链路层的包头

如图 这是一个HTTP的数据包

snort -v则只显示红框中的内容

snort -vd显示下图内容



snort -vde显示下图内容

可见绿框中的内容为新添的内容，为数据链路层的包头



### 数据包记录器

snort -dev -l ./log

如果要把所有的包记录到硬盘上，你需要指定一个日志目录，snort就会自动记录数据包

snort -dev -l ./log/ -h 10.0.7.118/8

这个命令告诉snort把进入网络10.的所有包的数据链路、TCP/IP以及应用层的数据记录到目录./log中

snort -l ./log -b

如果你的网络速度很快，或者你想使日志更加紧凑以便以后的分析，那么应该使用二进制的日志文件格式。所谓的二进制日志文件格式就是tcpdump程序使用的格式。使用下面的命令可以把所有的包记录到一个单一的二进制文件中：

注意此处的命令行和上面的有很大的不同。我们勿需指定本地网络，因为所有的东西都被记录到一个单一的文件。你也不必冗余模式或者使用-d、-e功能选项，因为数据包中的所有内容都会被记录到日志文件中。

snort -dv -r packet.log

使用-r功能开关，也能使snort读出包的数据。snort在所有运行模式下都能够处理tcpdump格式的文件。例如：如果你想在嗅探器模式下把一个tcpdump格式的二进制文件中的包打印到屏幕上，可以输入以上的命令

snort -dvr packet.log icmp

在日志包和入侵检测模式下，通过BPF(BSD Packet Filter)接口，可以使用许多方式维护日志文件中的数据。上面的命令行只读取icmp包

### 网络入侵检测系统

snort -dev -l ./log/ -h 10.0.7.118/8 -c /etc/snort/snort.conf

-h 10.0.7.118/8 指定主机 会覆盖conf文件中对主机的配置

但是目前总是得不到日志文件，不知是否是因为没有报警信息

#### 网络入侵检测模式下的输出选项

在默认情况下，snort以ASCII格式记录日志，使用full报警机制。如果使用full报警机制，snort会在包头之后打印报警消息。

snort有7种报警机制：full, fast,socket, syslog, console, cmg, and none。其中有6个可以在命令行状态下使用-A选项设置。这6个是：



用-s选项可以使snort把报警消息发送到syslog，默认的设备是LOG\_AUTHPRIV和LOG\_ALERT。可以修改snort.conf文件修改其配置。例如：

snort -c snort.conf -l ./log -h 192.168.1.0/24 -s

#### 理解报警输出

报警信息形如：

[\*\*] [116:56:1] (snort\_decoder): T/TCP Detected [\*\*]

116 是Generator ID，代表Snort产生报警的部件。etc/generators 可查看GIDs的列表

In this case, we know that this event came from the “decode”(116) component of Snort.

56是SnortID，For a list of preprocessor SIDs, please see etc/gen-msg.map。Rule-based SIDs are written directly into the rules with the sid option. In this case, 56 represents a T/TCP event.

1是版本ID

#### 高性能配置

如果想使Snort做够快(1000Mbps)，需要使用unified2 logging，unified2 logging的读取器是barnyard。这允许Snort使用二进制格式记录alert，这个比写到数据库中要快。

如果想写到一个text文件中，而且还需要尽可能地快，尝试使用binary logging和”fast”输出选项。

./snort -b -A fast -c snort.conf

这个命令将用tcpdump格式记录数据包并产生最少的报警

#### 改变报警顺序

### 包捕获

Snort使用DAQ Data Acquisition library，去捕获IO信号，而不是直接调用libpcap，这样可以保证跨平台时不用修改Snort。

当想使用Snort pcap readback或者inline模式时，DAQ可以选择模式



ethtool -k eth0查看当前状态

ethtool -K eth0 gro off 关闭



#### 配置

./snort \  
[--daq <type>] \  
[--daq-mode <mode>] \  
[--daq-dir <dir>] \  
[--daq-var <var>]  
config daq: <type>  
config daq\_dir: <dir>  
config daq\_var: <var>  
config daq\_mode: <mode>  
<type> ::= pcap | afpacket | dump | nfq | ipq | ipfw  
<mode> ::= read-file | passive | inline  
<var> ::= arbitrary <name>=<value> passed to DAQ  
<dir> ::= path where to look for DAQ module so’s

<type> ::= pcap | afpacket | dump | nfq | ipq | ipfw

例如snort -r select\_tcp.pcap --daq dump -c /etc/snort/snort.conf

使用dump格式，默认是pcap，暂时没看出来区别

pcap是默认模式，Snort可以运行在与tcpdump模式类似的sniffer模式，他可以记录包。

在特别繁忙的网络环境下sniffer模式不是很实用，因为把输出打到console屏幕上很快，不易阅读。

解决办法是使用filter，只看需要的包。

假设你连接在SPAN switch port or a network tap

使用snort –v –i eth0 host 172.16.100.53 而不是使用snort -v -i eth0

假设你担心感染上了网络蠕虫，想观察有哪些别的主机正在连接

snort –v –i eth0 src 172.16.100.53 and ‘tcp[13] & 2!=0 to display only SYN packets

短时间内，单一主机向多个主机发送大量SYN包预示着可能有病毒

snort在2.9版本加入了daq，同时引入了afpacket。afpacket是linux2.6开始引入的报文获取接口。其最大的特点是打破以往复制报文传递给用户的方式，而是采用了共享内存的交互方式。并且利用环形缓冲区使用户可以无锁处理。

分析

snort使用afpacket可以实现inline模式， 即IPS，不同于IDS的被动防御模式, IPS可以主动阻断。

snort首先会将配置的接口两两配对,这里以ETH0和ETH1为例.

然后使用afpacket的相关接口（具体可在内核中查找关键字）为每个接口分别建立两个环形缓冲区,

RX为输入缓冲区， TX为输出缓冲区。缓冲区是一块内核和用户共享的内存空间。

缓冲区的处理原理是循环队列，以输入缓冲区为例; 当内核发现RX有空位时就将报文放入空位中并打上可用标志，用户发现有标注可用的单元时就可以对其处理，使用完成后为该单元标注空闲标志内核又可继续利用。因为单消费者和生产者情况所以该队列能够无锁处理。

从ETH0进入的报文如红线所示，内核将报文放入RX中，snort获取该报文并进行匹配后返回通过和丢弃两种结果。如果是通过，则将该数据拷贝进ETH1的发送缓冲区TX并将在ETH0的RX中的该单元标志位空闲，否则不进行拷贝直接将ETH0的RX中的该单元标志为空闲。



### Reading Pcap file



### Basic Output

### Tunneling Protocol Support

### 杂项

#### 2.1.8.5 Snort模式

三种

1. Inline

IPS ，允许触发drop规则 ，命令行下使用-Q代表Inline模式

conf文件中 config policy\_mode:inline

1. Passive

IDS，不触发drop规则（-treat-drop-as-alert除外）

conf文件中 config policy\_mode:tap

1. Inline-Test

与Inline模式相似，允许在不影响数据流的情况下评估Inline的性能，Drop规则触发的流量会被触发为Wdrop (Would Drop) alert

snort --enable-inline-test  
config policy\_mode:inline\_test

## Configuring Snort

### Include

可以在snort.conf文件中使用include包含别的规则文件

#### Variables

规则变量名可以用多种方法修改。可以在"$"操作符之后定义变量。"?" 和 "-"可用于变量修改操作符。

$var - 定义变量。

$(var) - 用变量"var"的值替换。

$(var:-default) - 用变量"var"的值替换，如果"var"没有定义用"default"替换。

$(var:?message) - 用变量"var"的值替换或打印出错误消息"message"然后退出。

#### Config

太多了

### Preprocessor

预处理程序从Snort版本1.5开始引入，使得Snort的功能可以很容易地扩展，用户和程序员能够将模块化的插件方便地融入Snort之中。预处理程序代码在探测引擎被调用之前运行，但在数据包译码之后。通过这个机制，数据包可以通过额外的方法被修改或分析。使用preprocessor关键字加载和配置预处理程序。在Snort规则文件中的preprocessor指令格式如下：

preprocessor <name>: <options> 例子：

preprocessor minfrag: 128

### Decoder and Preprocessor Rule

Decoder和preprocessor rules允许基于规则启用和禁用decoder和preprocessor事件。

Decoder config选项会决定是否产生decoder事件。例如：如果snort.conf中有disable\_decode\_alerts，无论是否有匹配事件的规则，都不会产生decoder事件（alert之类）。

config\_enable\_decode\_drops优先于其他事件的规则。

#### Configuring

decoder和preprocessor规则位于preproc rules/

想启用的话去掉conf文件中关于这部分的注释



规则文件中的alert也可更换为别的，例如log pass drop sdrop reject

#### Reverting to original behavior

config autogenerate\_preprocessor\_decoder\_rules 回复到旧的行为

还需要conf文件中decoder和preprocessor的rules和相关的规则

### Event Processing

1. Detection Filter

用来配置阈值，只有匹配rule超过了这个次数才会产生事件。详见4.7.10

1. Rate Filter

使用rate filter改变一个规则的行为，当时间的次数或是频率意味着可能发生了攻击

1. Event Filter

减少noisy rules带来的logged events的数量。这个能明显降低误报率

1. Event Suppression

完全禁止不感兴趣事件的logging

#### Rate Filtering

在rule规则文件之外单独配置

#### Event Filtering

#### Enent Supression

#### Event Logging

#### Event Trace

### Performance Profiling性能剖析

Snort可以为rule和preprocessor的性能提供统计，只需要在snort.conf中config，snort就会在退出的时候统计。可指定文件名、可指定创建新文件或者append。

### Output Modules

在1.6版本后更新。允许snort在formatting和presentation上更灵活。Output modules在探测引擎和预处理器之后，alert或logging规则触发时调用。

例如：

Output modules are loaded at runtime by specifying the output keyword in the config file:  
output <name>: <options>  
output alert\_syslog: log\_auth log\_alert

#### alert\_syslog

#### alert\_fast

#### Log\_tcpdump

等等等等。。。。

### Host Attribute Table主机属性表

### Dynamic Modules

snort2.6之后加进去的，可在conf文件和命令行中配置

### Reloading a Snort Configuration

### Multiple Configurations

snort允许一个Snort实例对VLAN或IP子网进行多重配置，而不需要为了多种配置而运行多个snort。

### Active Response

snort2.9为inline模式下提供了更好的响应模式

# Snort源码分析

### 主函数（SnortMain函数）流程分析

1. 调用初始化函数SnortInit();
2. 获得数据包，确定链路协议类型，调用GetPacketSource 🡪 返回的是eth0或者是数据包名称
3. 注册控制处理器的句柄，调用ControlSocketRegisterHandler
4. 根据所选择的工作模式，初始化进程文件和权限操作

snort –r读取pcap模式下，运行



直接获取流量的情况下，运行



InlineFailOpen输出0 即为INLINE\_FAIL\_OPEN\_NOT\_USED

1. 调用解码函数SetPkPresessor



目前-r 和 直接捕获dlt值都为1 即为DLT\_EN10MB



实时抓包的话还会输出：



SnortUnprivilegedInit();会输出



直到Commencing packet processing (pid=20512)

下面接着的就是抓到的数据包显示

1. 循环抓包 PacketLoop()



在DAQ\_Acquire()中实现的循环抓包。

例如snort –r读取了一个有六个报文的pcap包，输出信息为



DAQ\_Acquire调用回调函数PacketCallback

PacketCallback中调用ProcessPacket对每一个数据包进行处理

### 每一个数据包

先走ProcessPacket()函数。snort.c中1877行左右。

在ProcessPacket()函数中第四行(\*grinder) (p, pkthdr, pkt); 调用解码引擎，对于以太网，即调用DecodeEthPkt()

再走DecodeEthPkt()函数（因为是以太网的数据包）。decode.c中876行左右。



感叹号为ProcessPacket中打的输出

Begin DecodeEthPkt为DecodeEthPkt输出

### ProcessPacket函数

1. 在读取文件snort -r 和实时监测时，无论是否运行于snort -c入侵检测模式，都不会触发



1. p->proto\_bits
2. NTP (UDP)输出8
3. ICMP输出10
4. TCP、HTTP输出4
5. Profinet实时数据输出0 之后变为0x8000.
6. 0变8000的会走if ( !p->proto\_bits )方法，别的不走if ( !p->proto\_bits )也不走else if
7. 只要不是被标记的忽略的端口的数据，都进入



调用检测引擎

1. 下面的Active\_SessionWasDropped()内都没有走

### DecodeEthPkt函数

### SnortInit函数（功能为初始化Snort各项配置）流程分析

① 解析命令行，调用ParseCmdLine函数

② 根据选择的工作模式，输出相应信息

③ 注册输出模块、预处理模块、规则选项模块

④ 打印所有网卡、接口

⑤ 加载动态插件

# Snort实验

## 入门级

编辑/etc/snort/rules/local.rules

添加

alert tcp any any -> 10.0.6.59/8 8000 (msg: "Sample alert";classtype:misc-attack;sid: 2002973; rev:1;)

alert icmp any any -> 10.0.6.59/8 any (msg:"Got an ICMP Packet"; classtype:not-suspicious;sid:2000001; rev:1;)

这个ip是公司电脑的。

第一个alert所有连接到10.0.6.59:8000 的tcp包（在10.0.6.59上起了一个web2py）

第二个是检测icmp的

编辑/etc/snort/snort.conf

去掉了Step #7: Customize your rule set 中除local.rules外其他所有的rules

snort -dv -c /etc/snort/snort.conf -l /root/study/Snort/log/ 启动snort

ping主机 或者访问web2py网站即可看到报警信息

/root/study/Snort/log路径下 tail -f alert 可实时观察alert文件的信息变化

产生的报警形如



# 备忘

uint\_8 代表一个字节

以太网头部

typedef struct \_EtherHdr

{

uint8\_t ether\_dst[6];

uint8\_t ether\_src[6];

uint16\_t ether\_type;

} EtherHdr;

const DAQ\_PktHdr\_t \*pkth; // packet meta data 捕获包的包头

const uint8\_t \*pkt; // raw packet data 指向捕获到的数据包