# 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TCP/IP包头信息打印在屏幕上，使用这个命令将使snort只输出IP和TCP/UDP/ICMP的包头信息。

snort -vd

显示数据链路层的信息

### 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

### 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

可以在snort.conf文件中使用include包含别的规则文件

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。

# Snort学习

### 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

