Linux安装snort

以Ubuntu18.04为例，也可以在其他Linux系统上安装，可参考网上教程。

## 修改Ubuntu源

修改源之后下载更新包速度会更快，也可以不做。

1. 将系统自带的该文件做个备份：

sudo cp /etc/apt/sources.list /etc/apt/sources.list.backup

2、修改配置：

打开/etc/apt/sources.list后在最开头加上清华大学开源镜像站：https://mirrors.tuna.tsinghua.edu.cn/help/ubuntu/ 中的18.04LTS sources.list内容。

sudo gedit /etc/apt/sources.list

sudo apt-get update -y

#这一步是更新源列表，换源后必须执行

sudo apt-get dist-upgrade -y

#这一步是更新软件

参考：https://blog.csdn.net/xiangxianghehe/article/details/80112149

## 安装Lamp

1、首先，需要安装Apache 2 Web服务器。

sudo apt install apache2 -y

默认情况下，所有Web内容都位于/var/www/html中。此外，/var/www/html目录中的所有内容都需要由www-data用户和www-data组拥有，以便Apache Web Server能够读取文件。

2、接下来，将安装MySQL数据库。MySQL是一个非常强大的开源关系数据库。运行以下命令安装MySQL。

sudo apt install mysql-server libmysqlclient-dev mysql-client autoconf libtool -y

#安装完成后，需要保护它。 运行此命令以保护MySQL。

sudo mysql\_secure\_installation

这个脚本会问你几个问题。第一个问题将要求您安装验证密码插件。

VALIDATE PASSWORD PLUGIN can be used to test passwords   
and improve security. It checks the strength of password   
and allows the users to set only those passwords which are   
secure enough. Would you like to setup VALIDATE PASSWORD plugin?   
Press y|Y for Yes, any other key for No: N

回答“N”，因为知道密码是安全的。 如果愿意，可以回答“Y”。

接下来的问题均回答Y。最后，脚本完成。MySQL现已安装。

3、安装PHP（注意：PHP必须安装5及其以下的版本）

在Ubuntu 18.04上安装LAMP的最后一步是安装PHP超文本预处理器。PHP添加了支持动态网页的服务器端网页处理。运行以下命令以安装PHP。

sudo add-apt-repository ppa:ondrej/php

sudo apt-get update -y

sudo apt-get install -y libapache2-mod-php5.6 php5.6 php5.6-common php5.6-gd php5.6-cli php5.6-xml php5.6-mysql

sudo apt-get install -y php-pear libphp-adodb

最后，我们需要重新启动Apache Web服务器。

sudo systemctl restart apache2

4、测试PHP

我们应该确保PHP工作正常。在/var/www/html中创建一个名为info.php的新文件。

使用以下内容调用info.php：

<?php

phpinfo();

?>

保存并退出该文件。现在浏览到以下URL：

http://localhost/info.php

应该看到PHP信息页面。

## 安装Snort

1. 安装DAQ。解压编译。

tar -xvzf daq-2.0.6.tar.gz

cd daq-2.0.6

./configure

sudo make & make install

2、安装Snort。解压编译。

tar -xvzf snort-2.9.12.tar.gz

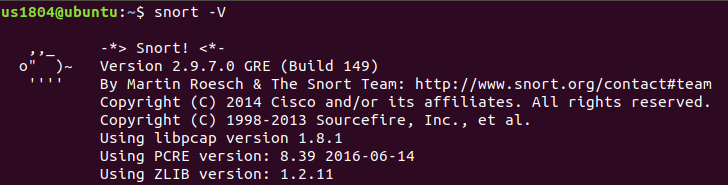
cd snort-2.9.12

./configure --enable-sourcefire

sudo make & make install

修复链接sudo ldconfig

3、测试snort -V。



4、配置用户和目录。

# 创建用户和用户组:

sudo groupadd snort

sudo useradd snort -r -s /sbin/nologin -c SNORT\_IDS -g snort

# 创建Snort目录

sudo mkdir /etc/snort

sudo mkdir /etc/snort/rules

sudo mkdir /etc/snort/rules/iplists

sudo mkdir /etc/snort/preproc\_rules

sudo mkdir /usr/local/lib/snort\_dynamicrules

sudo mkdir /etc/snort/so\_rules

# 创建文件来存储规则

sudo touch /etc/snort/rules/iplists/black\_list.rules

sudo touch /etc/snort/rules/iplists/white\_list.rules

sudo touch /etc/snort/rules/local.rules

# 创建日志目录

sudo mkdir /var/log/snort

sudo mkdir /var/log/snort/archived\_logs

# 修改文件权限

sudo chmod -R 5775 /etc/snort

sudo chmod -R 5775 /var/log/snort

sudo chmod -R 5775 /var/log/snort/archived\_logs

sudo chmod -R 5775 /etc/snort/so\_rules

sudo chmod -R 5775 /usr/local/lib/snort\_dynamicrules

#修改文件的归属用户

sudo chown -R snort:snort /etc/snort

sudo chown -R snort:snort /var/log/snort

sudo chown -R snort:snort /usr/local/lib/snort\_dynamicrules

#复制配置文件

cd ~/snort-2.9.11/etc/

sudo cp \*.conf\* /etc/snort

sudo cp \*.map /etc/snort

sudo cp \*.dtd /etc/snort

cd ~/snort-2.9.11/src/dynamic-preprocessors/build/usr/local/lib/snort\_dynamicpreprocessor/

sudo cp \* /usr/local/lib/snort\_dynamicpreprocessor/

5、修改配置文件。（查看本机ip和网卡的名字，命令ifconfig。）

sudo vi /etc/snort/snort.conf

# ipvar HOME\_NET修改为本机的内部网络

ipvar HOME\_NET 192.168.0.45/24

#设置以下配置文件路径

var RULE\_PATH /etc/snort/rulesvar

SO\_RULE\_PATH /etc/snort/so\_rulesvar

PREPROC\_RULE\_PATH /etc/snort/preproc\_rulesvar

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

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

# 在output unified2: filename merged.log, l imit 128, nostamp, mpls event types, vlan event types 之后添加

output unified2: filename snort.u2, limit 128

#启用local.rules文件，其后的include文件均注释掉

include $RULE\_PATH/local.rules

6、添加规则。

tar -xzf community-rules.tar.gz

cp community-rules/\* /etc/snort/rules/

#检查规则

snort -T -c /etc/snort/snort.conf

在规则中添加一条对icmp包的规则，以便测试。

sudo vi /etc/snort/rules/local.rules

alert icmp any any -> $HOME\_NET any (msg:"ICMP Test detected!!!"; classtype:icmp-event; sid:10000001; rev:001; GID:1; )

设置sid对应信息，添加sid-msg文件或者将common-rules的sid-msg文件copy到/etc/snort目录中，以下为添加sid-msg文件的方法。

sudo touch /etc/snort/sid-msg.map

sudo vi /etc/snort/sid-msg.map

1 || 10000001 || 001 || icmp-event || 0 || ICMP Test detected || url,tools.ietf.org/html/rfc792

7、测试配置文件和功能。

sudo snort -T -c /etc/snort/snort.conf -i eth1

sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth1

#关闭防火墙

ufw disable

此时从外面ping网口eth1的IP，snort会记录受到攻击，信息保存在/var/log/snort中，文件名为snort.u2.xxx。

## 安装Barnyard2

1、解压编译。

tar zxvf barnyard2-2-1.13.tar.gz

cd barnyard2-2-1.13autoreconf -fvi -I ./

# 选择下面两条命令中的一个

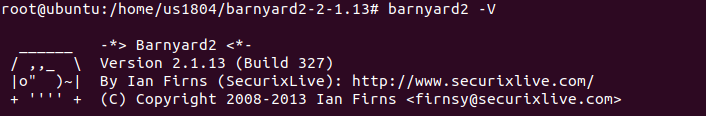
./configure --with-mysql --with-mysql-libraries=/usr/lib/x86\_64-linux-gnu

./configure --with-mysql --with-mysql-libraries=/usr/lib/i386-linux-gnu

sudo makesudo make install

1. 测试。

barnyard2 -V



3、设置配置文件

sudo cp ~/barnyard2-2-1.13/etc/barnyard2.conf /etc/snort/

sudo mkdir /var/log/barnyard2

sudo chown snort.snort /var/log/barnyard2

sudo touch /var/log/snort/barnyard2.waldo

sudo chown snort.snort /var/log/snort/barnyard2.waldo

1. 配置数据库

mysql -u root -p

mysql> create database snort;

mysql> use snort;

mysql> source ~/barnyard2-2-1.13/schemas/create\_mysql;

mysql> CREATE USER 'snort'@'localhost' IDENTIFIED BY '123456';

mysql> grant create, insert, select, delete, update on snort.\* to 'snort'@'localhost';

mysql> exit;

1. 添加数据库配置

sudo vi /etc/snort/barnyard2.conf

#在末尾添加数据库配置

output database: log, mysql, user=snort password=123456 dbname=snort host=localhost sensor name=sensor01

#修改barnyard2.conf权限防止被修改

sudo chmod 644 /etc/snort/barnyard2.conf

1. 测试

#启动mysql

service mysql start

# 开启snort，并向eth1发送ping数据包

sudo snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth1

# 开启barnyard2，将日志信息存入数据库

# 1.连续处理模式，设置barnyard2.waldo为书签

sudo barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo -g snort -u snort

# 2.文件处理模式，处理单个日志文件（snort.u2.xxx修改为日志名字）

sudo barnyard2 -c /etc/snort/barnyard2.conf -o /var/log/snort/snort.u2.xxx

# 查看数据库条目数量，看是否增加

mysql -u snort -p -D snort -e "select count(\*) from event"

## 安装BASE

1、安装adodb

$sudo tar zxvf adodb-5.20.14.tar.gz -C /var/www/html

$sudo mv /var/www/html/adodb5 /var/www/html/adodb

2、安装base

$sudo tar zxvf base-1.4.5.tar.gz -C /var/www/html

$sudo mv /var/www/html/base-1.4.5 /var/www/html/base

sudo /etc/init.d/apache2 restart

3、配置。

修改/etc/php.ini。

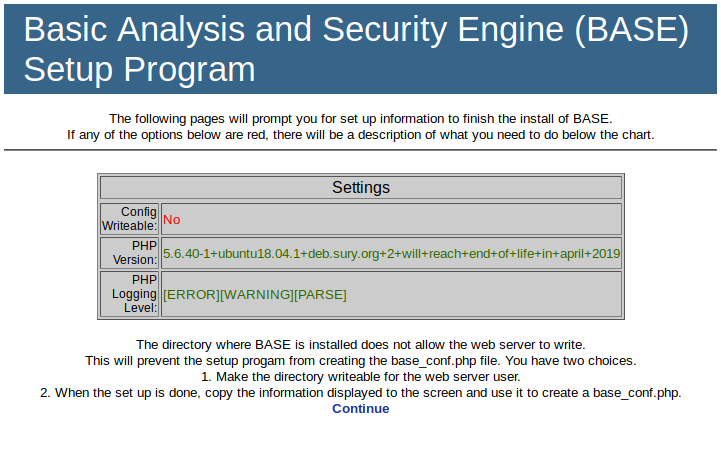
Error\_reporting = E\_ALL & ~E\_NOTICE

设置目录权限。

chown -R apache:apache /var/www/html

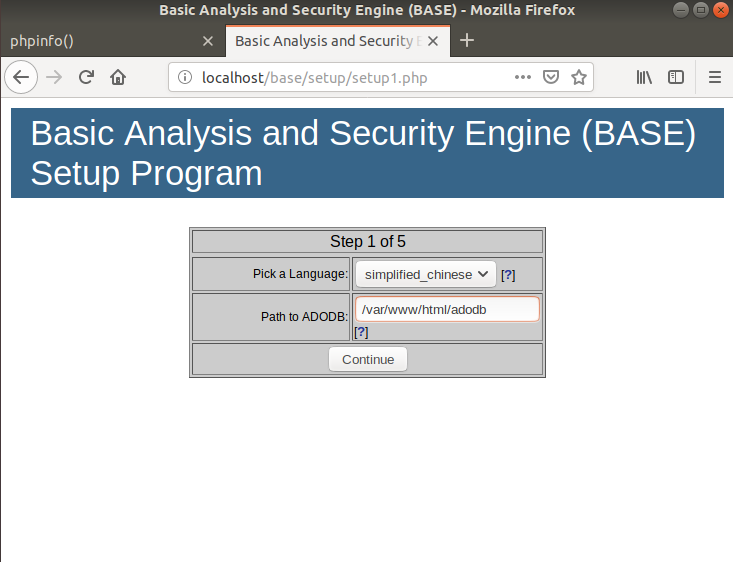
chomod 755 /var/www/html/adodb

打开<http://localhost/base/>setup/setup.php。（最好是全部为绿色，都通过，我这里有一个显示不可读，但是可以按其下的提示在之后创建base\_conf.php）



按continue继续填信息。

第一步选择语言和填入adodb所在目录。

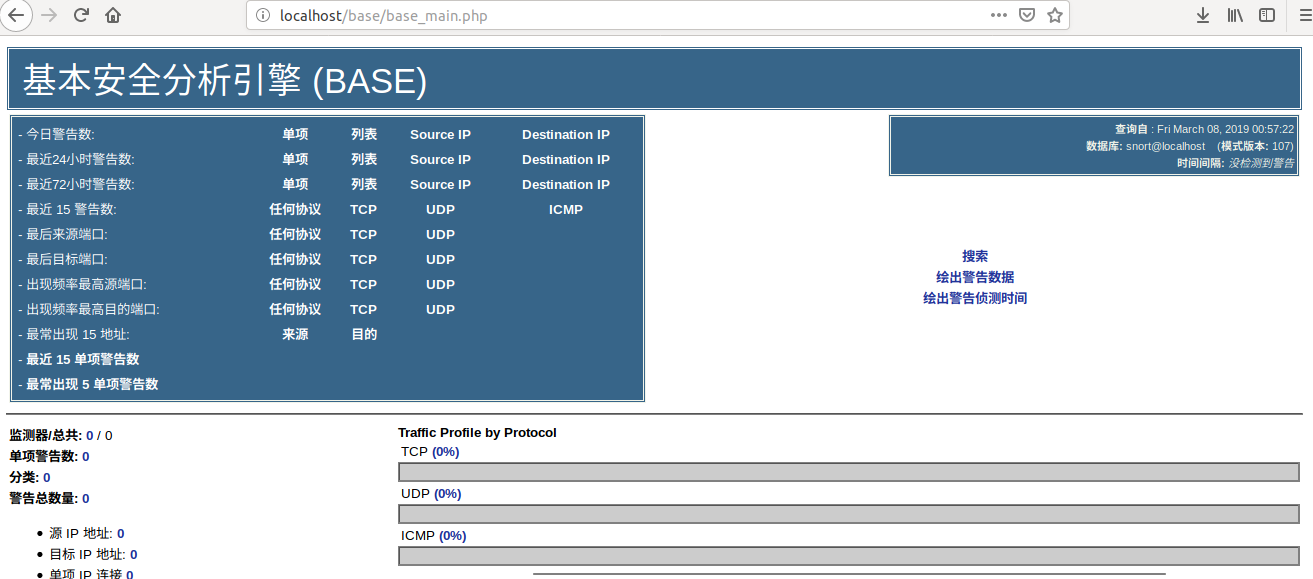


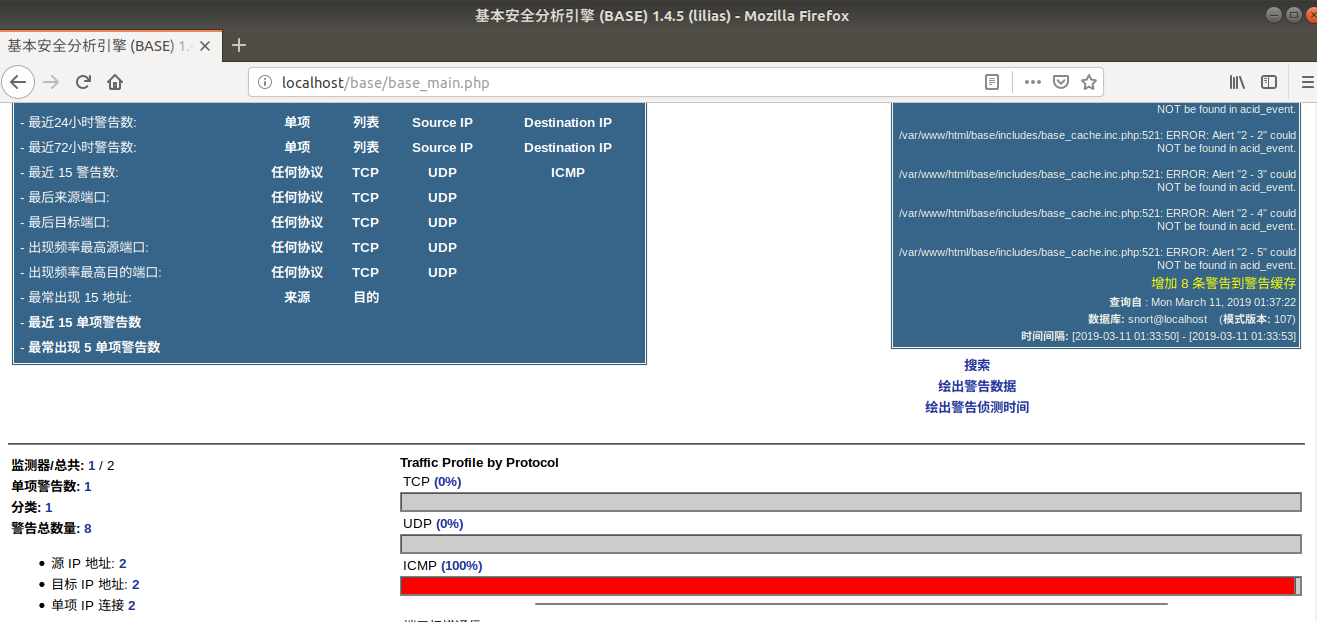
第2步填入数据库的信息，按之前配置的信息填即可。（archive数据库的信息可以不填。）

第3步填入管理账号：snort，密码：123456。

第4、5步确认，提示已经创建了相应的数据表。

点击之后可以看见这个页面，代表创建成功，将页面划到最低点击可以看到这个页面，代表BASE安装成功。如果mysql的snort已经有数据的话，将会显示其中的数据。





## 使用snort

Snort有三种工作模式， sniffer，packet logger，network intrusion detection system。1、sniffer模式只是简单地从网络上抓取数据包并在终端显示出来；

如果只是想在屏幕上打印出TCP/IP包的头信息，可以用：snort -v。这条命令只是显示IP和TCP/UDP/ICMP数据包的头信息。

如果想显示数据包的头信息，并且想显示应用程序传输的数据，可用：snort -vd。

如果想显示链路层的信息，如网卡Mac地址，可用以下命令：snort -vde。

1. packet logger模式可把数据包保存在磁盘中；

如果想把数据包信息存在磁盘上，就要用Packet Logger Mode。用以下命令可使Snort自动把数据包信息存到磁盘中：snort -vde -l log\_directory。

当snort运行在该模式下时，它会把所有抓取的数据包按IP分类地存放到log\_directory中。可用-h指定本地网络，以使snort记录与本地网络相关的数据包：snort -vde -l log\_directory -h 192.168.1.0/24。

如果在一个高速网络中，或者想记录数据包以备分析，你就可以二进制方式记录数据包，在这里不用指定-vde，因为二进制方式将记录整个包的信息。如：snort -l log\_directory -b。

二进制模式把数据包存成tcpdump格式，如：snort -dv -r snort.log。

3、network intrusion detection模式是最复杂，具有高可配置性。它可使Snort根据用户定义的规则分析网络流量，并作出反应。

用以下命令开启NIDS模式：

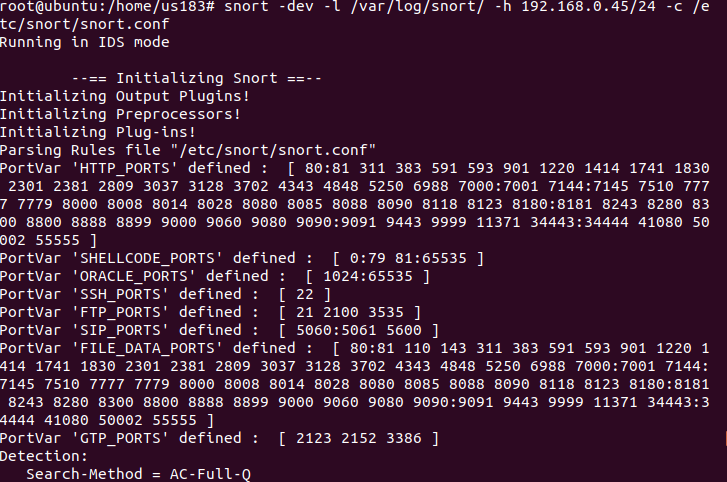
snort -dev -l log\_directory -h 192.168.1.0/24 -c snort.conf

snort.conf是规则集配置文件，为了不影响NIDS速度，我们可把-v和-e选项取消。如：

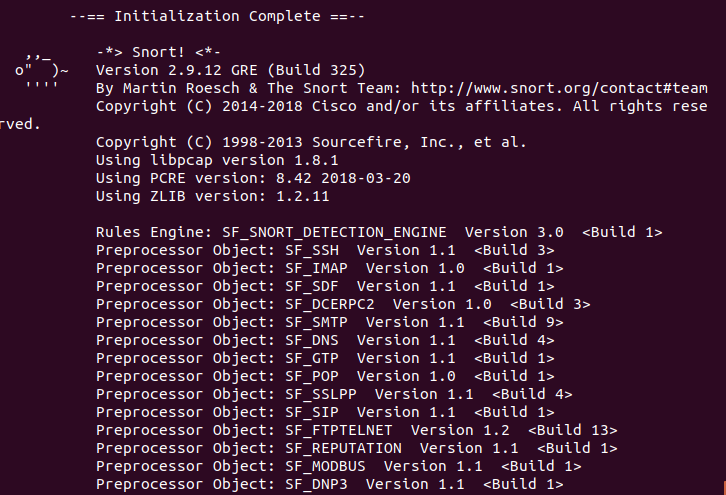
snort -d -l log\_directory -h 192.168.1.0/24 -c snort.conf

log\_directory目录下会生成alter日志，记录入检测的警报信息。

尝试进行，会有一系列的初始化信息。



然后初始化成功。



其后也有打印出的包信息。

