Building a Debian/Snort based IDS
Jason Weir – jason.weir@nhrs.org – 8/27/2012

This document installs Debian 6.0.5 (Squeeze), Snort 2.9.3.1, Barnyard2-1.10 and BASE 1.4.5.

Document Roadmap:
1. Install OS and base software
2. Install Snort pre-requisites - libpcap, libdnet, and DAQ
3. Install, configure & test Snort
4. Setup MySQL database
5. Install & configure Barnyard
6. Configure Apache & PHP
7. Install, configure and test BASE
8. Startup script for Snort & Barnyard
9. Keep rules up to date with Pulledpork
10. What I left out

1. Install OS and base software

This document assumes 2 network cards with eth0 being the management interface and eth1 being the collector interface.

Get Debian here: http://www.debian.org/distrib/netinst. I used the small CD version. Burn the iso and boot the CD.

Choose the default options (or as appropriate for your site), when you get to the “Software Selection” screen, unselect all options to get a bare minimum install. After the install finishes, the CD ejects and the system will reboot. Log back in as root.

# apt-get update && apt-get -y install ssh
– This is so we can connect via SSH and copy/paste to the terminal.

Dotdeb.org maintains packages of mysql and php more current than the Debian repository - do the following so apt can use them.

# vi /etc/apt/sources.list
Add the following lines:

deb http://packages.dotdeb.org squeeze all
deb-src http://packages.dotdeb.org squeeze all

Install the dotdeb GnuPG key:

# cd /usr/src && wget http://www.dotdeb.org/dotdeb.gpg
# cat dotdeb.gpg | apt-key add -

Apt will require input – for example MySQL will ask for you to enter a "root" password for the MySQL server. Make it secure and don't forget it.

# apt-get update && apt-get -y install apache2 apache2-doc autoconf automake bison ca-certificates ethtool flex g++ gec gcc-4.4 libapache2-mod-php5 libcrypto-ssl-Perl libmysqlclient-dev libnet1 libnet1-dev libpcre3 libpcre3-dev libphp-adodb libssl-dev libtool libwww-perl make mysql-client mysql-common mysql-server ntp php5-cli php5-gd php5-mysql php-pear sendmail sysstat usbmount vim

Disable "Large Receive Offload" and "Generic Receive Offload" on the collector interface

# ethtool -K eth1 gro off
# ethtool -K eth1 lro off

2. Install Snort pre-requisites - libpcap, libdnet, and DAQ

Install libpcap:

# cd /usr/src && wget http://www.tcpdump.org/release/libpcap-1.3.0.tar.gz
# tar -zxf libpcap-1.3.0.tar.gz && cd libpcap-1.3.0
# ./configure --prefix=/usr --enable-shared && make && make install

Install libdnet:

# tar -zxf libdnet-1.12.tgz && cd libdnet-1.12
# ./configure --prefix=/usr --enable-shared && make && make install

Install daq:

# cd /usr/src && wget http://www.snort.org/dl/snort-current/daq-1.1.1.tar.gz
# tar -zxf daq-1.1.1.tar.gz && cd daq-1.1.1
# ./configure && make && make install

Update the shared library path

# echo >> /etc/ld.so.conf /usr/lib
# echo >> /etc/ld.so.conf /usr/local/lib && ldconfig
3. Install, configure & test Snort

# wget http://www.snort.org/dl/snort-current/snort-2.9.3.1.tar.gz -O snort-2.9.3.1.tar.gz
# tar -zxf snort-2.9.3.1.tar.gz & & cd snort-2.9.3.1
# configure --enable-sourcefire & & make & & make install
# mkdir /etc/snort /etc/snort/rules /var/log/snort /var/log/barnyard2 /usr/local/lib/snort_dynamicrules
# touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules
# groupadd snort & & useradd -g snort snort
# chown snort:snort /var/log/snort /var/log/barnyard2
# cp/usr/src/snort-2.9.3.1/etc/*.conf* /etc/snort
# cp/usr/src/snort-2.9.3.1/etc/*.map /etc/snort
# cp/usr/src/snort.conf /etc/snort
# vi /etc/snort/snort.conf

Change these lines:
Line #45 - ipvar HOME_NET 172.26.12.0/22 – make this match your internal (friendly) network
Line #48 - ipvar EXTERNAL_NET !HOME_NET
Line #104 - var RULE_PATH /rules
Line #113 - var WHITE_LIST_PATH /rules
Line #114 - var BLACK_LIST_PATH /rules
Line #297 - add this to the end after “decompress_depth 65535” max_gzip_mem 104857600
Line #538 - add this line
output unified2: filename snort.log, limit 128
Line #554 - delete or comment out all of the “include SRULE_PATH” lines except “local.rules”

# vi /etc/snort/rules/local.rules

Enter a simple rule like this for testing:
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001;)

Now we can start and test snort.
# /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

Ping the management IP address from another machine, alerts should be printed to the console like this:

If so congrats – you have Snort working… Use ctrl-c to kill snort.

4. Install & configure Barnyard

# cd /usr/src & & wget https://nodeload.github.com/firnsy/barnyard2/tarball/master
# tar -zxf master & & cd firnsy-barnyard2-*
# autoreconf -fvi -I ./m4 & & ./configure --with-mysql & & make & & make install
# mv /usr/local/etc/barnyard2.conf /etc/snort
# cp schemas/create_mysql /usr/src
# vi /etc/snort/barnyard2.conf

Line #215 change to
output alert_fast

At the end of the file add this line:
output database: log, mysql, user=snort password=<mypassword> dbname=snort host=localhost

5. Setup the MySQL server

# mysql -u root -p
# You will be prompted to enter the password you created during installation.
mysql> create database snort;
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
mysql> SET PASSWORD for snort@localhost=PASSWORD('mypassword'); # set user password different from "root" password
mysql> use snort;
mysql> source /usr/src/create_mysql
mysql> show tables; # you should see the list of new tables you just imported.
mysql> exit

Now start snort and barnyard with these commands:
# /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth0 &
# /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.log -w /etc/snort/bylog.waldo -G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map -C /etc/snort/classification.config &
Again ping the management IP address from another machine

This command shows that barnyard is correctly inserting events into the database:
# mysql -uroot -p -D snort -e "select count(*) from event" # enter password again

6. Configure Apache & PHP

# cp /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled
# vi /etc/php5/apache2/php.ini
Line #521 – change line to read - error_reporting = E_ALL & ~E_NOTICE

# a2enmod ssl
# pear config-set preferred_state alpha & pear channel-update pear.php.net & pear install --alldeps Image_Color Image_Canvas Image_Graph
# /etc/init.d/apache2 restart

7. Install and configure BASE

# cd /usr/src && wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz
# tar -zxf base-1.4.5.tar.gz & cp -r base-1.4.5 /var/www/base
# chmod 777 /var/www/base (just for now)

Open a browser and go to: https://192.168.1.13/base (or whatever the management IP is)

Click Continue, choose English
Path to adodb: /usr/share/php/adodb
Click Continue
Database Name: snort
Database Host: localhost
Database Port: leave blank
Database User Name: snort
Database Password: mypass

Put in values for the authentication system and click submit.
Click “create baseag” which extends the DB to support BASE.

Continue to step 5 to login.
You should see a number next to unique alerts – click on that and you should see alerts like this:

Snort Alert [1:10000001:0] – the test rule we created above

If you see alerts in BASE – Congrats – everything is working as it should be.

8. Startup script for snort & barnyard

# vi /etc/init.d/snortbarn

Paste the following into the file:

```bash
#!/bin/sh
# This script will be run as a startup script
#
### BEGIN INIT INFO
# Provides: snortbarn
# Required-Start: $remote_fs $syslog mysql
#  Required-Stop: $remote_fs $syslog
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# X-Interactive: true
# Short-Description: Start Snort and Barnyard
### END INIT INFO

# . /lib/init/vars.sh
# . /lib/lsb/init-functions

mysqld_get_param() {
  /usr/sbin/mysqld --print-defaults | tr " " "\n" | grep -- "--$1" | tail -n 1 | cut -d= -f2
}

do_start()
{
  log_daemon_msg "Starting Snort and Barnyard"
  # Make sure mysql has finished starting
  ps alive=0
  while [ $ps alive -lt 1 ];
```
do
    pidfile=`mysqld_get_param pid-file`
    if [ -f "$pidfile" ] && ps 'cat $pidfile' >/dev/null 2>&1; then ps_alive=1; fi
    sleep 1
    done

/sbin/ifconfig eth1 up
/usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth1 &
/usr/local/bin/barnyard2 -q -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.log -w /etc/snort/hylog.waldo -G /etc/snort/gen-msg.map –S /etc/snort/sid-msg.map -C /etc/snort/classification.config 2> /dev/null &

    log_end_msg 0
    return 0
}

do_stop()
{
    log_daemon_msg "Stopping Snort and Barnyard" ""
    kill $(pidof snort) 2>/dev/null
    kill $(pidof barnyard2) 2>/dev/null
    log_end_msg 0
    return 0
}

case "$1" in
    start)
        do_start
        ;;
    stop)
        do_stop
        ;;
    restart)
        do_stop
        do_start
        ;;
    *)
        echo "Usage: snort-barn {start|stop|restart}" >&2
        exit 3
        ;;
esac
exit 0

---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Make it executable and create the startup symlinks.

# chmod +x /etc/init.d/snortbarn
# insserv -f -v snortbarn

Snort & Barnyard will now start automatically at boot.

9. Keep your rules up to date with pulledpork


# cd /usr/src && wget http://pulledpork.googlecode.com/files/pulledpork-0.6.1.tar.gz
# tar -xf pulledpork-0.6.1.tar.gz && cd pulledpork-0.6.1
# cp pulledpork.pl /usr/local/bin && cp etc/*.conf /etc/snort
# vi /etc/snort/pulledpork.conf

Comment out lines 22 & 26

To use the Sourcefire VRT Certified Rules, go to snort.org, register for an account and get an "oinkcode", this will allow you to download their Registered User rule set.

Nothing additional needs to be done to use the Emerging Threats Open rule set.

Line 20: enter your "oinkcode" where appropriate or comment out the line if you didn't get one above
Line 23: leave alone (uncommented) to use the Emerging Threats rule set
Line 71: change to: rule_path=/etc/snort/rules/snort.rules
Line 86: change to: local_rules=/etc/snort/rules/local.rules
Line 89: change to: sid_msg=/etc/snort/sid-msg.map
Line 112: change to: config_path=/etc/snort/snort.conf
Line 124: change to: distro=Debian-Lenny
Line 171: Uncomment and change to: enablesid=/etc/snort/enablesid.conf
Line 173: Uncomment and change to: disablesid=/etc/snort/disablesid.conf
Line 174: Uncomment and change to: modifysid=/etc/snort/modifysid.conf

# echo pcre:fwsam >> /etc/snort/disablesid.conf  # disables all block (fwsam) rules

Run pulledpork
#/usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf -T -l
You should now see local.rules and snort.rules in /etc/snort/rules.

Clean Up:
# rm /var/www/index.html
# chmod 755 /var/www/base
# pkill snort && pkill barnyard2
# rm -rf /var/log/snort/* /var/log/barnyard2/*
# vi /etc/snort/rules/local.rules -- Comment out the test rule
# vi /etc/snort/snort.conf -- Line 553: add: include $RULE_PATH/snort.rules

Plug a span port or tap into eth1 and restart snort

#/etc/init.d/snortbarn restart