Installation Guide

SNORT/BARNYARD/SNORBY

Snort

- Snort is Network Intrusion Detection System (NIDS). Snort can sniff your network and alert you based on his rule DB if there is an attack on your computers network. It is an opensource system that is build from tcpdump (linux sniffer tool).

Prerequisite

- Update your system using yum update and reboot

  yum update -y reboot
- Install rpm forge repository
- On i386 system

  rpm -Uhv http://apt.sw.be/redhat/el5/en/i386/rpmforge/RPMS/rpmforge-release-0.5.2-2.el5.rf.i386.rpm

- On x86_64 system

  rpm -Uhv http://apt.sw.be/redhat/el5/en/x86_64/rpmforge/RPMS/rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm

- Install PCRE, libdnet and more prerequisite packages

  yum install libdnet libdnet-devel pcre pcre-devel gcc make flex byacc bison kernel-devel libxml2-devel -y

- Create dir for Snort prerequisite sources

  mkdir /usr/local/src/snort
- Change dir to the new created directory

  cd /usr/local/src/snort
- Download and install libpcap

  wget http://www.tcpdump.org/release/libpcap-1.2.1.tar.gz -O libpcap.tar.gz tar zxvf libpcap.tar.gz cd libpcap-* ./configure && make && make install

- Add /usr/local/lib line to ld

  echo "/usr/local/lib" >> /etc/ld.so.conf
  ldconfig –v
- Download and install DAQ

  cd /usr/local/src/snort wget http://www.snort.org/downloads/1221 -O daq.tar.gz tar zxvf daq.tar.gz cd daq-* ./configure && make && make install ldconfig -v

- Create snort user and group

  groupadd snort useradd -g snort snort

Install Snort

- Download Snort

  cd /usr/local/src/snort wget http://www.snort.org/downloads/1416 -O snort.tar.gz

- Extract and install Snort

  tar zxvf snort.tar.gz cd snort-2* ./configure --prefix /usr/local/snort && make && make install

- Create links for Snort files

  ln -s /usr/local/snort/bin/snort /usr/sbin/ ln -s /usr/local/snort/etc /etc/snort
- Configure Snort startup script to run at startup

  cp rpm/snortd /etc/init.d/ chmod +x /etc/init.d/snortd cp rpm/snort.sysconfig /etc/sysconfig/snort chkconfig --add snortd

- Delete following lines from snort startup file

  vi /etc/init.d/snortd
- Comment out the following variable in /etc/sysconfig/snort and add / to the LOGDIR variable

  vi /etc/sysconfig/snort

... LOGDIR=/var/log/snort/ ... #ALERTMODE=fast ... #BINARY_LOG=1 ...

- Download Snort rules files from http://www.snort.org/snort-rules to /usr/local/src/snort
- Extract rules file in the new created directory

  cd /usr/local/snort tar zxvf /usr/local/src/snort/snortrules-snapshot-2*

Create directory for snort logging

mkdir -p /usr/local/snort/var/log chown snort:snort /usr/local/snort/var/log ln -s /usr/local/snort/var/log /var/log/snort

- Create links for dynamic rules files and directories

ln -s /usr/local/snort/lib/snort_dynamicpreprocessor /usr/local/lib/snort_dynamicpreprocessor ln -s /usr/local/snort/lib/snort_dynamicengine /usr/local/lib/snort_dynamicengine ln -s /usr/local/snort/lib/snort_dynamicrules /usr/local/lib/snort_dynamicrules

- Set snort permissions

chown -R snort:snort /usr/local/snort

- Comment out or delete all reputation preprocessor configuration lines from snot.conf and configure ouput plugin

  vi /usr/local/snort/etc/snort.conf

... #preprocessor reputation: \ # memcap 500, \ # priority whitelist, \ # nested_ip inner, \ # whitelist $WHITE_LIST_PATH/white_list.rules, \ # blacklist $BLACK_LIST_PATH/black_list.rules ... output unified2: filename snort.log, limit 128 ...

- Create Dynamicrules directory

mkdir /usr/local/snort/lib/snort_dynamicrules

- Copy dynamicrules files
- On i386 system

cp /usr/local/snort/so_rules/precompiled/RHEL-5-5/i386/2.9.2.1/*so
/usr/local/snort/lib/snort_dynamicrules/

- On x86_64 system

cp /usr/local/snort/so_rules/precompiled/RHEL-5-5/x86-64/2.9.2.1/*so
/usr/local/snort/lib/snort_dynamicrules/

- Dump the stub rules

snort -c /usr/local/snort/etc/snort.conf --dump-dynamic-rules=/usr/local/snort/so_rules

- Enable snort dynamic rules configuration in the end of snort.conf file

vi /usr/local/snort/etc/snort.conf

... # dynamic library rules include $SO_RULE_PATH/bad-traffic.rules include $SO_RULE_PATH/chat.rules include $SO_RULE_PATH/dos.rules include $SO_RULE_PATH/exploit.rules include $SO_RULE_PATH/icmp.rules include $SO_RULE_PATH/imap.rules include $SO_RULE_PATH/misc.rules include $SO_RULE_PATH/multimedia.rules include $SO_RULE_PATH/netbios.rules include $SO_RULE_PATH/nntp.rules include $SO_RULE_PATH/p2p.rules include $SO_RULE_PATH/smtp.rules include $SO_RULE_PATH/snmp.rules include $SO_RULE_PATH/specific-threats.rules include $SO_RULE_PATH/web-activex.rules include $SO_RULE_PATH/web-client.rules include $SO_RULE_PATH/web-iis.rules include $SO_RULE_PATH/web-misc.rules ...

- Test Snort configuration

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

Install Barnyard

- Barnyard is an addon for snort. Barnyard let snort to write its log and alert data very fast in a binary files and then Barnyard read those files and send them to whatever output you configure it, here we will configure to output the data to a mysql database in oreder to watch the data using php application called BASE.

Prerequisite

- Snort

- Install MySQL

yum install mysql mysql-devel –y

- Download Barnyard

cd /usr/local/src/snort wget http://www.securixlive.com/download/barnyard2/barnyard2-1.9.tar.gz

- Extract Barnyard

tar zxvf barnyard2-1.9.tar.gz cd barnyard2-1.9

- Configure Barnyard
- On i386 system

./configure --with-mysql --with-mysql-libraries=/usr/lib64/mysql

- Install Barnyard

make && make install

- Configure Barnyard start script to run at startup

cp rpm/barnyard2 /etc/init.d/ chmod +x /etc/init.d/barnyard2 cp rpm/barnyard2.config /etc/sysconfig/barnyard2 chkconfig --add barnyard2

- Create links for Barnyard files and create archive directory

ln -s /usr/local/etc/barnyard2.conf /etc/snort/barnyard.conf ln -s /usr/local/bin/barnyard2 /usr/bin/ mkdir /var/log/snort/etho/archive/

- Change barnyard running time and change -L to -l in barnyard2 startup script on "BARNY_OPTS=" line

vi /etc/init.d/barnyard2

... # chkconfig: 2345 70 60 ... BARNYARD_OPTS="-D -c $CONF -d $SNORTDIR/${INT} -w $WALDO_FILE -l $SNORTDIR/${INT} -a $ARCHIVEDIR -f $LOG_FILE -X $PIDFILE $EXTRA_ARGS" ...

- Edit LOG_FILE variable in Barnyard sysconfig file

vi /etc/sysconfig/barnyard2

… LOG_FILE="snort.log" …

- Start Snort and Barnyard

service snortd start

service barnyard2 start

Installation Snorby

- Snorby is a frontend application for Snort. Snorby let you check and analyze your Snort events and alerts from a web browser.

Prerequisite

- Snort
- Barnyard

- Install apache and prerequisite packages

yum install libyaml-devel httpd git imagemagick ImageMagick-devel libxml2-devel libxslt-devel gcc-c++ curl-devel httpd-devel apr-devel apr-util-devel –y

- Download and install Ruby

cd /usr/local/src/snort wget http://ftp.ruby-lang.org/pub/ruby/1.9/ruby-1.9.3-p194.tar.gz tar xvzf ruby-1* cd ruby-1* ./configure && make && make install

- Install openssl extension

cd ext/openssl/ ruby extconf.rb make && make install

- Install gem dependencies

gem install thor i18n bundler tzinfo builder memcache-client rack rack-test erubis mail rack-mount rails gem install rake --version=0.9.2 gem uninstall rake --version=0.9.2.2

- Download and install wkhtmltopdf

cd /usr/local/src/snort wget http://wkhtmltopdf.googlecode.com/files/wkhtmltopdf-0.11.0_rc1-static-i386.tar.bz2 tar jxvf wkhtmltopdf-0.11.0_rc1-static-i386.tar.bz2 mv wkhtmltopdf-i386 /usr/local/bin/wkhtmltopdf chown root:root /usr/local/bin/wkhtmltopdf

- Download and configure snorby
- cd /var/www/html/ git clone http://github.com/Snorby/snorby.git cd /var/www/html/snorby/config/ cp database.example.yml database.yml cp snorby_config.example.yml snorby_config.yml chown -R apache:apache /var/www/html/snorby
- Set mysql root password

mysqladmin password humus

- Configure snorby database username and password

vi database.yml

…. snorby: &snorby adapter: mysql username: root password: humus host: localhost …

- Install Snorby

cd /var/www/html/snorby bundle install --deployment rake snorby:setup

- Configure Barnyard to output alerts to snorby database

vi /etc/snort/barnyard.conf

- Restart Barnyard

service barnyard2 stop service barnyard2 start

- Install Passenger module for apache

gem install passenger cd
/usr/local/lib/ruby/gems/1.9.1/gems/passenger-3.0.12/bin
./passenger-install-apache2-module

- Configure and restart apache

vi /etc/httpd/conf/httpd.conf

- Members
- Fernando Lajom
- Kevin Vasquez
- Edgar Sebuk
- Angelo Garcia
- Kevin Garcia