Installation instructions for ACID

(Analysis Console for Intrusion Databases)

Updated

29 Apr 2002

Chris Payne

chris@whitehats.ca

http://www.whitehats.ca

http://members.rogers.com/chrispayne

(This page intentionally left blank)

Introduction

This is a work in progress. It is based on my experience getting ACID configured and working on a Slackware 8.0 box. To quote CERT/CC " The Analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of security events generated by various IDSes, firewalls, and network monitoring tools."

It is assumed you already have a running Linux distribution as installing/configuring a Linux box is beyond the scope of this document. These instructions should work on any Linux distribution with only minor (if any) modifications. Please forward any inconsistencies to the author for inclusion in a future version of this document. The installation was based on the following versions of files (please be aware that the location of these files likely change frequently and might not be as follows by the time you read this):

gd-1.8.4
http://www.boutell.com/gd/http/gd-1.8.4.tar.gz

mysql-3.23.42
http://www.mysql.com/Downloads/MySQL-3.23/mysql-3.23.42.tar.gz

openssl-0.9.6b
http://www.openssl.org/source/openssl-0.9.6b.tar.gz

mod_ssl-2.8.4-1.3.20
http://www.modssl.org/source/mod_ssl-2.8.4-1.3.20.tar.gz

apache_1.3.20
http://httpd.apache.org/dist/httpd/apache_1.3.20.tar.gz

php-4.0.6
http://www.php.net/do_download.php?download_file=php-4.0.6.tar.gz&source_site=www.php.net

acid-0.9.6b15
http://www.andrew.cmu.edu/~rdanyliw/snort/acid-0.9.6b15.tar.gz

adodb131
http://phplens.com/lens/dl/adodb131.tgz

phplot-4.4.6
http://ftp1.sourceforge.net/phplot/phplot-4.4.6.tar.gz

snort-1.8.1-RELEASE
http://www.snort.org/releases/snort-1.8.1-RELEASE.tar.gz

snort-rules-current
http://www.snort.org/downloads/snortrules.tar.gz

snort DB-Plugin
http://www.incident.org/snortdb/snortdb-extra.gz

Getting Started

Note: If you are reading this document and you are using the Shadow IDS v1.5 package powered by Slackware Linux put together by Guy Bruneau which is available from: http://www.whitehats.ca/main/members/Seeker/seeker_shadow/seeker_shadow.html please note that there are some additional files required before you can continue on.

Shadow users, please click here for more information.

- It is recommended you copy all of the source files we require into some sort of temporary directory like: /usr/local/acid_setup_files

- In this document, sometimes in the display of how to configure a file for installation, you will see a line that ends with a \ this only to show you the command continues on the next line. If you enter a \ in your command, it will not always work. It is used here to convey one command.

- Install gd

```
cd /usr/local/acid_setup_files
tar –zxvf gd*
rm gd*.tar.gz
cd gd*
make  &&  make install
```

- build and install mysql

```
cd /usr/local/acid_setup_files
tar –zxvf  mysql-VERSION-OS*.gz
rm mysql-VERSION-OS*.tar
cd mysql-VERSION-OS
./configure --prefix=/usr/local/mysql  \  make && make install  \
scripts/mysql_install_db  \
echo /usr/local/mysql/lib/mysql  >>  /etc/ld.so.conf  &&  ldconfig  \
groupadd mysql  \ useradd –g mysql mysql  \ chown –R root:mysql /usr/local/mysql \
chown –R mysql /usr/local/mysql/bin  \  chown –R mysql /usr/local/mysql/var  \
cp support-files/my-medium.cnf   /etc/my.cnf

cd  /usr/local/mysql
bin/safe_mysqld –-user=mysql &
bin/mysqladmin  –u  root  password  ‘a_password_for_sql_user_root’
```

- Note: The single quotes around the root users password is ***very*** *important.*

- Setting up the database and its users

```
vi /etc/profile  and add the following to your path:
/usr/local/mysql/bin:/usr/local/apache/bin
source /etc/profile
```

```
mysql –p
\u mysql
DELETE FROM user WHERE User=’’;                              (2 single quotes)
DELETE FROM user WHERE Password=’’;                          (2 single quotes)
GRANT ALL PRIVILEGES ON *.* TO dba@localhost IDENTIFIED BY ‘make_a_password_for_user_dba’;
CREATE DATABASE snort;
GRANT INSERT,SELECT,DELETE ON snort.* TO snort@localhost \
IDENTIFIED BY ‘make_a_password_for_user_snort’;
\q
```

Note1: When entering the passwords for the sql_user dba & snort, ensure it gets enclosed in single quotes or you will get an error.

Note2: For users configuring a remote sensor, you must also add the following:

```
GRANT INSERT,SELECT,DELETE ON snort.* TO snort@remotehostname \
IDENTIFIED BY ‘make_a_password_for_remote_user_snort’;
```

- build openssl

```
cd /usr/local/acid_setup_files
tar –zxvf openssl*
rm openssl*.tar.gz
cd openssl*
sh config  \  no-idea  \  no-threads  \  -fPIC  && make && make install
```

- build mod_ssl **(Making sure apache is already untared in your temp directory)**

```
cd /usr/local/acid_setup_files
tar –zxvf mod_ssl*
rm mod_ssl*.tar.gz
cd mod_ssl*
./configure --with-apache=../apache<tab>  --with-ssl=../openssl<tab>  \
--prefix=/usr/local/apache  --enable-shared=ssl  --enable-module=ssl   \
--enable-rule=SSL_SDBM  --enable-rule=SSL_EXPERIMENTAL  \
--enable-rule=SSL_VENDOR  --enable-rule=EAPI
```

- build and install apache

```
cd ../apache<tab>
make && make certificate && make install
```

- You will be prompted during the making of certificates for information such as security levels and web server information. Use appropriate information for your server.

- Configure Apache and install ACID

Apache

- Remove all of the default files and directories from /usr/local/apahche/htdocs
- vi /usr/local/apache/conf/httpd.conf and search for, making sure the following is set:

```
MinSpareServers 1
MaxSpareServers 3
StartServers   2
MaxClients     5
Port 443
SSLRequireSSL (in <Directory “/usr/local/apache/htdocs”>)
ServerSignature Off
```

ACID

```
cd /usr/local/acid_setup_files
tar –zxvf acid*
rm acid*.tar
mv acid  /usr/local/apache/htdocs/acid
tar –zxvf adodb*
rm adodb*.tar.gz
mv adodb*  /usr/local/apache/htdocs/adodb
tar –zxvf phplot*
rm phplot*.tar.gz
mv phplot*  /usr/local/apache/htdocs/phplot

chmod 0755 /usr/local/apache/htdocs/acid
chmod 0644 /usr/local/apache/htdocs/acid/*

chmod 0755 /usr/local/apache/htdocs/adodb
chmod 0644 /usr/local/apache/htdocs/adodb/*

chmod 0755 /usr/local/apache/htdocs/phplot
chmod 0644 /usr/local/apache/htdocs/phplot/*

chown –R root:wheel /usr/local/apache/htdocs/acid/*
chown –R root:wheel /usr/local/apache/htdocs/phplot/*
chown –R root:wheel /usr/local/apache/htdocs/phplot/*
```

- Create the snort data directory and the databases

```
mkdir  /root/snort_log_storage                    (only an example... this is where snort.log and portscan.log will be stored)
mysql –u dba –p snort  <  /usr/local/snort*/contrib/create_mysql                               (sql-user dba password)
mysql –u dba –p snort  <  /usr/local/apache/htdocs/acid/create_acid_tbls_mysql.sql             (sql-user dba password)

zcat  /usr/local/acid_setup_files/snortdb-extra.gz  |  mysql  snort
```

- Configuring acid

vi /usr/local/apache/htdocs/acid/acid_conf.php and change for the following:

```
$DBlib_path=”/usr/local/apache/htdocs/adodb”
$ChartLib_path=”/usr/local/apache/htdocs/phplot”
```

$alert_dbname:	MySQL database name where the alerts are stored	***snort***
$alert_host:	host where the database is stored	***localhost***
$alert_port:	port where the database is stored	***3306***
$alert_user:	username into the database	***snort***
$alert_password:	password for username	***whatever_u_asassigned***

(using values you chose while creating the mysql database above)

- build and install php

```
./configure --with-mysql=/usr/local/mysql  --with-apxs=/usr/local/apache/bin/apxs \
--enable-bcmath  --with-gd  --enable-sockets  --enable-track-vars  && make  \
&&  make install  &&  cp php.ini-dist  /usr/local/lib/php.ini
```

Edit the /usr/local/apache/conf/httpd.conf file and make sure the PHP 4 mime type is there and uncommented. Something like this:

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

- Start up Apache

```
/usr/local/apache/bin/apachectl startssl  <enter the password>
```

- Configure and build Snort 1.8.1

```
cd /usr/local/acid_setup_files
tar –zxvf snort*
rm snort-1.*.tar.gz
```

```
cd snort*
./configure --with-mysql=/usr/local/mysql  --with-openssl=/usr/local/ssl  \
&&  make  &&  make install
mkdir /usr/local/snort
groupadd snort  && useradd –g snort snort  &&  passwd –l snort  &&  \
chmod 700 –R /usr/local/snort  &&  chown –R snort.snort  /usr/local/snort
```

- Configure snort for your site

```
mv /usr/local/acid_setup_files/snortrules*  /usr/local/snort
cd /usr/local/snort
tar –zxvf snortrules*
rm snortrules.tar  &&  cd rules
vi snort.conf and edit to your requirements
```

we must configure the following values in particular:
(Additionally setting up the values for your particular network settings)

The best source for documentation on setting up snort is available at:
http://www.snort.org/documentation.html

snort.conf

If you want snort to log to syslog: (optional)

```
output alert_syslog: LOG_AUTH  LOG_ALERT
```

If you want snort to output the full data to a file: (optional)

```
output alert_full: alert.full
```

As we want snort to log to a mysql database, we require the following:

```
output database: alert, mysql, dbname=snort user=snort host=localhost  \
password=usersnortpassword  sensor_name=meaningful_name_for_host
```

Following is for a Remote Sensor

```
output database: alert, mysql, dbname=snort user=snort host=remotehostname  \
password=usersnortpassword  sensor_name=meaningful_name_for_host
```

- Test our snort config

```
/usr/local/snort/snort –c /usr/local/snort/rules/snort.conf  \
–b –l /root/snort_log_storage  -Nv –t /usr/local/snort
```

This command will start up snort in sniffer mode, dumping the packets to the screen, and testing our snort.conf file for errors, and we turned off logging for this test. We will be running snort in a chrooted environment (hence the –t option)

If all goes well, great… if you get any errors, you need to troubleshoot your config a little more before moving on the next step.

- Final Configurations

You will want to make some entries in /etc/rc.d/rc.local for the following to start on bootup:

```
echo "Starting up mysql… "
/usr/local/mysql/bin/safe_mysqld  –-user=mysql &

echo "Starting up snort… "
/usr/local/snort/snort –c /usr/local/snort/rules/snort.conf –u snort –g snort  \
–b –l /root/snort_log_storage –t /usr/local/snort
```

It would also be nice to have a line with "/usr/local/apache/bin/apachectl startssl" so that apache could start with ssl support on every bootup but you get prompted to enter the passphrase you chose during the make certificates part of the apache installation, so this could be an issue for some setups.

- Test it out

From another computer, surf to http://theipaddress/acid/acid_db_setup.php
Acid will tell you if it needs to modify the database in any way before it is usable.

After that, http://theipaddress/acid/index.html will show you any data you are getting.

Shadow IDS v1.5 Users

This section only applies to users using the Shadow IDS v1.5 package powered by Slackware Linux 8.0 put together by Guy Bruneau. Available here

You require the following additional packages to complete this acid installation.

bison
http://carroll.cac.psu.edu/pub/linux/distributions/slackware/slackware-8.0/slakware/d1/bison.tgz

flex
http://carroll.cac.psu.edu/pub/linux/distributions/slackware/slackware-8.0/slakware/d1/flex.tgz

gcc
http://carroll.cac.psu.edu/pub/linux/distributions/slackware/slackware-8.0/slakware/d1/gcc.tgz

binutils
http://carroll.cac.psu.edu/pub/linux/distributions/slackware/slackware-8.0/slakware/d1/binutils.tgz

gmake
http://carroll.cac.psu.edu/pub/linux/distributions/slackware/slackware-8.0/slakware/d1/gmake.tgz

glibc
http://carroll.cac.psu.edu/pub/linux/distributions/slackware/slackware-8.0/slakware/d1/glibc.tgz

linuxinc
http://carroll.cac.psu.edu/pub/linux/distributions/slackware/slackware-8.0/slakware/d1/linuxinc.tgz

You can just download each file you require, and (as root) install like:

installpkg filename <enter>

For the gd package that we will compile later, (which is the Image manipulation library providing JPEG/PNG/GIF support for creating charts), we will also have to download/compile/install the following packages.

jpegsrc
ftp://ftp.uu.net/graphics/jpeg/jpegsrc.v6b.tar.gz

zlib
http://www.info-zip.org/pub/infozip/zlib/zlib.tar.gz

libpng-1.0.11
http://www.libpng.org/pub/png/src/libpng-1.0.11.tar.gz

Setup on a remote sensor

Note: mysql is required on the sensor, or snort will not run.
The sensor will forward all of its data to a remote host that you specy in the snort.conf file.

- Install and compile openssl

```
sh config \ no-idea \ no-threads \ -fPIC && make && make install
```

- Install and compile openssh

```
./configure && make && make install
```

- Install mysql client only

```
./configure --without-server --prefix=/usr/local/mysql && make && make install  \
echo /usr/local/mysql/lib/mysql >> /etc/ld.so.conf  &&  ldconfig
```

- Compile snort with mysql logging enabled

```
./configure --with-mysql=/usr/local/mysql –with-openssl=/usr/local/ssl \
&& make && make install
```

- Setup sensor logging directory

- mkdir –p /usr/local/snort/var/log/snort
- copy the snort configuration files to /usr/local/snort
- configure the snort.conf file located in the /usr/local/snort directory as per the snort instructions earlier. (Click here)
- cp /usr/local/bin/snort /usr/local/snort
- groupadd snort
- useradd –g snort snort
- passwd –l snort
- chmod –R 700 /usr/local/snort
- chown –R snort.snort /usr/local/snort
- add the following to the local.rules file to ignore ssh connections to the $HOME_NET host.
    - pass tcp $HOME_NET 22 <> $HOME_NET any

- Test the snort remote logging the following way:

```
/usr/local/snort/snort –c snort.conf –dvo –t /usr/local/snort –g snort –u snort
```

If snort starts, the sensor is ready to go.

- Start the local sensor with the following options to run in a chrooted environment:

```
/usr/local/snort/snort –c snort.conf –doD –t /usr/local/snort –g snort –u snort
```

Thanks:

To Jamie French and Guy Bruneau for their assistance and all of the testing…

Copyright Notice: