Installation Instructions for ACID

(Analysis Console for Intrusion Detection)

By Guy Bruneau, GSEC, GCIA, GCUX

Version 1.0 – 1 October 2003

Requirements

This setup is built to get ACID working on Slackware 9. This document assumed you already have a Slackware Linux distribution running. These instructions should work on any Linux distribution with only minor (if any) modifications. Make sure you do not use the default zlib, mysql, mod_ssl and Apache packages from Slackware.

Remember the version for each of the packages below are being constantly updated and subject to changes. The files used for this installation are located on each of the following sites:

jpegsrc version 6b
http://www.ijg.org/files/

jpgraph version 1.13
http://www.aditus.nu/jpgraph/jpdownload.php

zlib version 1.1.4
http://www.gzip.org/zlib/

libpng version 1.2.5 (Download .tar.gz tarball)
http://www.libpng.org/pub/png/libpng.html

gd version 2.0.15
http://www.boutell.com/gd/http/

mysql version 4.0.15a (Source tarball version bottom of page)
http://www.mysql.com/downloads/mysql-4.0.html

openssl version 0.9.7c
http://www.openssl.org/source/

mod_ssl version 2.8.15-1.3.28 (Must match version of Apache)
http://www.modssl.org/source/

apache version 1.3.28
http://httpd.apache.org/dist/httpd/

php version 4.3.3
http://www.php.net/downloads.php

acid version 0.9.6b23
http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html

adodb version 39x
http://php.weblogs.com/adodb#downloads

snort version 2.0.2
http://www.snort.org/dl/

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

Important

In order to compile all of these packages, you are going to need to install at the minimum the following Slackware packages:

A, AP, D, L, N

Optional are the following packages if you want to run X-Windows on the same server:

Gnome or KDE, X, XAP

Note: Do not install from the N package apache, mod_ssl, php, openssl and mysql because they have to be compiled from source. Do not install from the L package zlib.

Getting Started

Note: It is recommended you copy all of the source files we require into a temp directory something like /tmp/acid

Before starting compiling the packages add the following to the console path:

vi /etc/profile and find the PATH and add to the following to the path:

PATH=”/usr/local/mysql/bin:/usr/local/apache/bin:/usr/local/bin:/usr/bin:/bin”

Log out and log in to enable the new environment

Install jpegsrc, zlib, libpng, gd

```
cd /tmp/acid
tar -zxvf jpegsrc*
cd jpegsrc*
./configure  &&  make  &&  make install

cd /tmp/acid
tar -zxvf zlib*
cd zlib*
./configure  &&   make  &&  make install

cd /tmp/acid
tar -zxvf libpng*
cd libpng*
cp  scripts/makefile.linux  ./Makefile
make  &&  make install

cd /tmp/acid
tar -zxvf gd*
cd gd*
,/configure && make  &&  make install
```

build and install mysql

```
cd /tmp/acid
tar -zxvf  mysql*
cd mysql*
```

```
./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          (Depending of your distribution, group/user might already be there)
useradd –g mysql mysql

chown –R root:mysql /usr/local/mysql
chown –R mysql:mysql /usr/local/mysql/var
cp support-files/my-medium.cnf   /etc/my.cnf (Use with 32 – 64 MB of RAM to DB)
cp support-files/my-huge.cnf /etc/my.cnf (Use with 1 –2 GB of RAM to DB)
cd  /usr/local/mysql
bin/mysqld_safe —-user=mysql &
bin/mysqladmin –u root password ‘your-new-password-for-sql_user-root’
```

build openssl

```
cd /tmp/acid
tar -zxvf openssl*
cd openssl*
sh config \ no-idea \ no-threads \ -fPIC && make && make install
```

build mod_ssl

Note: Make sure apache is already unpacked in /tmp/acid/

```
cd /tmp/acid
tar -zxvf mod_ssl*
cd mod_ssl*
./configure --with-apache=../apache<tab> --with-ssl=/usr/local/ssl  \
--prefix=/usr/local/apache --enable-shared=ssl --enable-module=ssl  \
--enable-rule=SSL_EXPERIMENTAL --enable-rule=SSL_VENDOR --enable-rule=EAPI
```

build and install apache

```
cd /tmp/acid
tar –zxvf apache*
cd apache*
make && make certificate && make install
```

Note: Important for the SSL Certificate:

Signature Algorithm: *Select RSA* (Default)
Enter certificate information pertaining to your site
Certificate version: *Select 3* (Default)
Encrypt private Key: *Select no* (If you select yes you will have to enter the password to start Apache in SSL)

build and install php

```
cd /tmp/acid
tar –zxvf php*
cd php*
./configure --prefix=/usr/local/apache/php --with-mysql=/usr/local/mysql \
--with-apxs=/usr/local/apache/bin/apxs --with-zlib-dir=/usr/local \
--enable-bcmath --with-gd --enable-sockets --enable-track-vars  \
&& make  &&  make install  &&  cp php.ini-dist  /usr/local/apache/php/php.ini
```

Setting up the database and its users

At the bash shell, do :

```
mysql –p                                                    (root password set earlier)
\u mysql                                                    (User 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                                                          (Quit mysql)
```

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

Use this entry to configure a remote sensor only

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

Configure Apache and install ACID

Apache

vi /usr/local/apache/conf/httpd.conf and search for, making sure the following is set:

```
MinSpareServers 5
MaxSpareServers 10
```

```
StartServers     5
MaxClients      10
Port 443                   (instead of Port 80)
ServerSignature Off
```

Delete Listen 80   (We don’t want the server to listen on port 80 just 443)

Add the following PHP 4 mime type in the document. Add them after

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
AddType image/x-icon .ico
```

JPGraph

```
cp jpgraph* /usr/local/apache/htdocs
tar –zxvf jpgraph*
mv jpgraph* jpgraph
cd jpgraph
rm README
rm QPL.txt
```

Configure ACID

```
cd /tmp/acid
tar -zxvf acid*
mv acid  /usr/local/apache/htdocs/acid
chmod 0755 /usr/local/apache/htdocs/acid
chmod 0644 /usr/local/apache/htdocs/acid/*

cd /tmp/acid
tar -zxvf adodb*
mv adodb*  /usr/local/apache/htdocs/adodb
chown –R root:wheel /usr/local/apache/htdocs/adodb
```

Configure and build Snort 2.x

```
cd /tmp/acid
tar -zxvf snort*
cd snort*
./configure --with-mysql=/usr/local/mysql  &&  make && make install
```

Note: Use this configuration only if Snort sensor is collocated with the mysql database.

I recommend using the prebuilt Snort sensor package on the Shadow/Snort sensor CD located at www.whitehats.ca

Create the Snort database tables

<u>Note</u>: Use the dba password for all of these mysql commands.

The following two scripts (create_mysql and snort-extra.gz) are located in the Snort tarball

```
mysql –u dba –p snort  <  snort_tarball/contrib/create_mysql
gunzip snortdb-extra.gz
mysql –u dba –p snort < snort_tarball/contrib/snortdb-extra
```

This script is located in the Apache ACID directory

```
mysql –u dba –p snort < /usr/local/apache/htdocs/acid/create_acid_tbls_mysql.sql
```

Verify mysql tables

Login into mysql to verify the db was created correctly

```
mysql –p   (root password)
mysql> SHOW DATABASES;
```

You should see a database called mysql, snort and test at this point

```
mysql > use snort;
mysql > SHOW TABLES;
```

You should see 23 tables listed for this table

```
\q
```

Configuring acid

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

```
$DBlib_path=”/usr/local/apache/htdocs/adodb”;
$Dbtype=”mysql”;
$ChartLib_path=”/usr/local/apache/htdocs/jpgraph/src”;
```

$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	***root***
$alert_password:	password for username	***whatever_u_asassigned***

$archive_dbname:	***snort***
$archive_host:	***localhost***
$archive_port:	***3306***
$archive_user:	***root***
$archive_password:	***whatever_u_asassigned***

Note: You must use the values you chose while creating the mysql database above

Start up Apache

```
/usr/local/apache/bin/apachectl startssl  <enter the password if you set one up on the certificate>
```

Configure snort for your site

```
vi /usr/local/snort/etc/snort.*.conf file
```

This is optional

If you want to send the logs/alarms to other places as well, uncomment any of these lines:

```
output alert_syslog: LOG_AUTH  LOG_ALERT     (Send alarms to a syslog server)
output alert_full: alert.full                (Output all the data information)
output alert_smb: workstation.list           (Sending alerts to a workstation)
```

Local Sensor/Database (All on one line)**:**

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

Remote Sensor/Database (All on one line)**:**

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

- Starting Snort

```
/etc/rc.d/rc.snort stop
/etc/rc.d/rc.snort start
```

Final Configurations

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

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

Testing the final installation

From a workstation using a web browser enter, http://theipaddress/acid/acid_db_setup.php and 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.

Setup Snort on a remote sensor

Note: mysql libraries are required on the sensor, or snort will not run. The sensor will forward all of the data to a remote host specified in the snort.conf file.

Build mysql client only

Note: At this stage, you the sensor requires the mysql libraries, you might want to choose to compile the libraries on another workstation and copy them to /usr/local/mysql/lib/mysql on the sensor. **This mysql step only applies for a remote sensor**.

```
./configure --without-server --prefix=/usr/local/mysql && make && make install
tar zcf mysql.tgz /usr/local/mysql/lib/mysql
copy the mysql.tgz libraries to sensor
Unpack the mysql.tgz in /
echo /usr/local/mysql/lib/mysql >> /etc/ld.so.conf  &&  ldconfig
```

Compile snort with mysql logging enabled

Note: On the same workstation you just compiled the mysql libraries, compile the snort sensor.

```
./configure --with-mysql=/usr/local/mysql && make && make install
```